Blockchain, Bitcoin, and Future

Heung-No Lee

May 2nd 2018

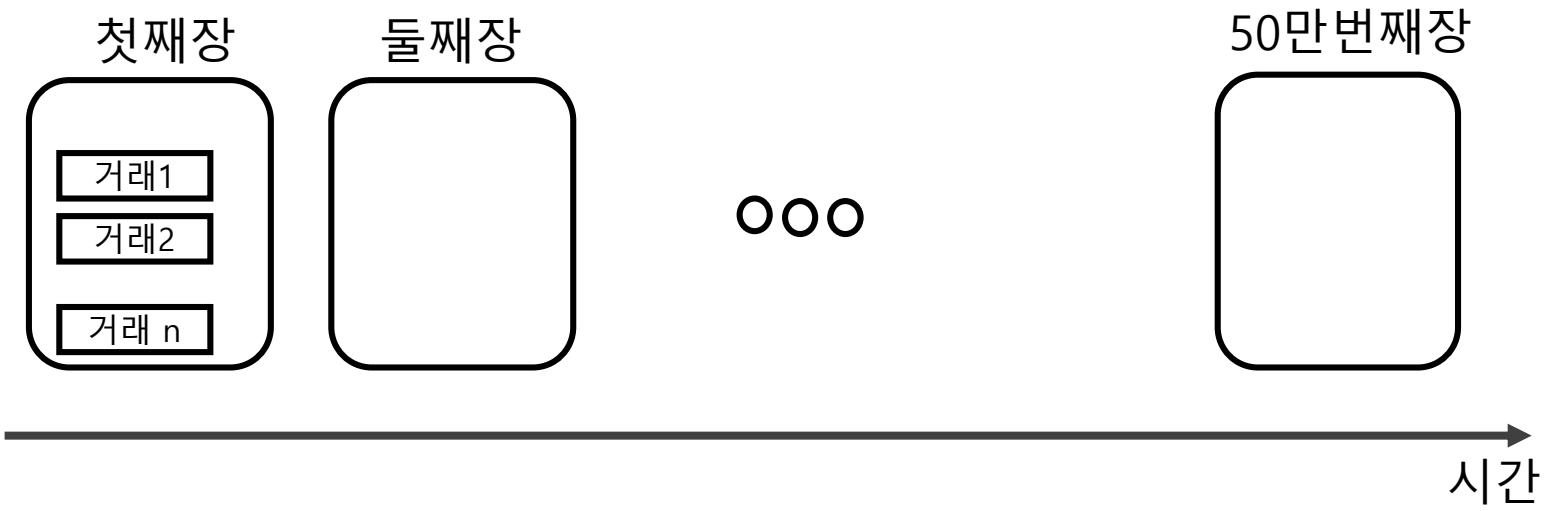
JCCI 특별프로그램1

제목: Blockchain, Bitcoin and Future
연사: **이흥노 교수** (GIST)
좌장: **신요안 교수** (숭실대)
일시: 5월 2일 (수) 14:40-15:50

블록체인은 2009년에 백서와 SW가 공개되었던 암호화폐 Bitcoin을 통해 세상에 알려졌습니다. 시간의 순으로 발생하는 모든 거래 내역을 순서대로 그때 그때 바로 바로 기록한 것을 블록체인 원장이라고 정의할 수 있습니다. 이 원장을 인터넷에 공개해 놓고 거래내역을 누구나 들여다 볼 수 있게 했습니다. 거래기록 작성은 특정인이나 단체 혹은 국가가 독점하지 못 하도록 하였습니다. 오히려 누구든지 거래원장 기록에 참여할 수 있도록 열어 놓은 분산 형 원장 작성 기술입니다. 누구나 작성에 참여하고 인터넷에 공개된 파일임에도 불구하고 어떤 것이 원본인지를 구분할 수 있도록 전혀 새로운 방식의 원장 동의 프로토콜을 만들었습니다. 또한 암호학적 설계로 원장에 기록된 내용을 임의로 바꿀 수 없습니다. 이 분산원장을 블록체인이라고 칭합니다. 누구나 작성에 참여할 수 있게 열려있고 한 번 입력된 기록은 위변조의 위험 없이 보존되기 때문에 거래에 참여하는 모두에게 신뢰를 얻습니다. 즉 블록체인에 기록된 내용은 발생한 시간과 내용이 순전 무결하게 그대로 기록되었고 보존되었다는 것을 믿을 수 있다는 것입니다. Bitcoin은 블록체인을 은행이나 국가의 개입이 필요 없는 암호화폐를 만드는데 사용했습니다. 즉 인터넷에서 코인을 주고 받을 수 있게 만든 것입니다. 마치 실물세계에서 화폐를 건네는 사람과 받는 사람이 대면 거래를 하듯이, 인터넷 상에서 거래당사자가 전자서명과 블록체인을 통해 코인의 소유권을 주고받을 수 있게 하였습니다. 현재까지 약 일천오백여 개의 새로운 암호화폐가 탄생했습니다. 블록체인이 확보해주는 데이터 무결성을 통한 신뢰의 가치는 매우 큽니다. 그로인해 스마트계약, 부동산거래, 전자투표, 보험 및 기부 네트워크관리, 토지관리 등 새로운 응용 분야가 속속 개발되고 있습니다. 세계적인 미래학자 돈 탭스콧은 인터넷이 지난 30년을 지배해온 것처럼 앞으로는 블록체인 혁명이 30년 이상 지배할 것이며 세상의 모든 것을 변화시킬 것이라고 언급하였습니다. 본 특강에서는 어떻게 Bitcoin과 블록체인이 이런 혁신을 이루어 내는지 그 핵심 기술들을 설명하도록 하겠습니다.

What is blockchain?

- Blockchain의 정의:
- 시간의 순으로 발생하는 모든 거래 내역을 순서대로 그때 그때 바로 바로 기록한 것을 블록체인 원장이라고 정의할 수 있습니다.



What is blockchain?

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

전세계 노드 모두 똑 같은 원장을 공유

미국에 있는 원장

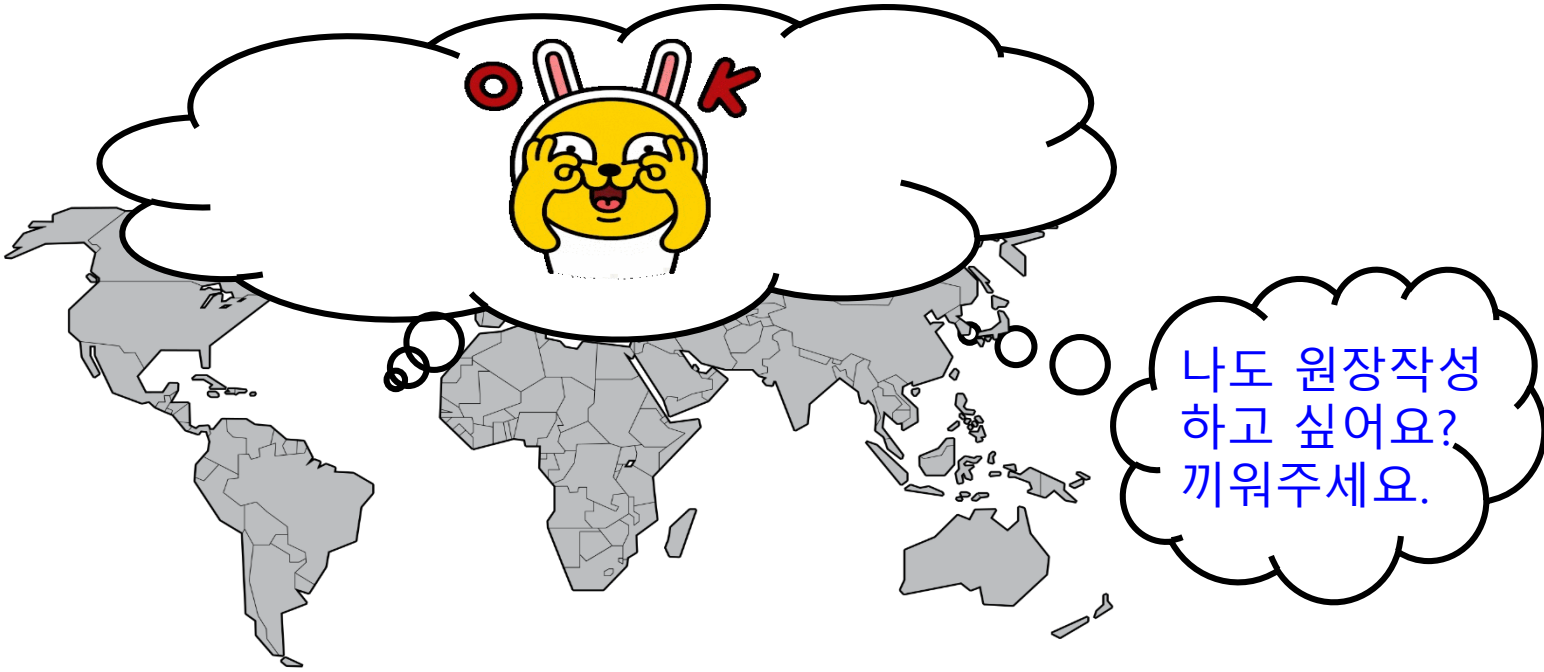
한국에 있는 원장

What is blockchain?

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

What is blockchain?

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

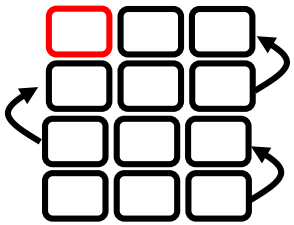


What is blockchain?

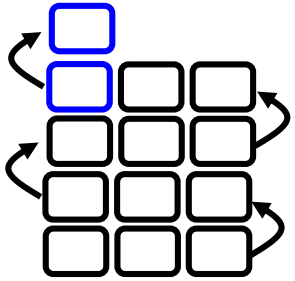
- 누구나 작성에 참여하고 인터넷에 공개된 파일임에도 불구하고 어떤 것이 원본인지 구분할 수 있도록 전혀 새로운 방식의 원장 동의 프로토콜을 만들었습니다.

동시에 2개의 다른 체인이 공표될 때
어떤 체인이 원장이 되나?

100번째장 작성
성공! 야호!



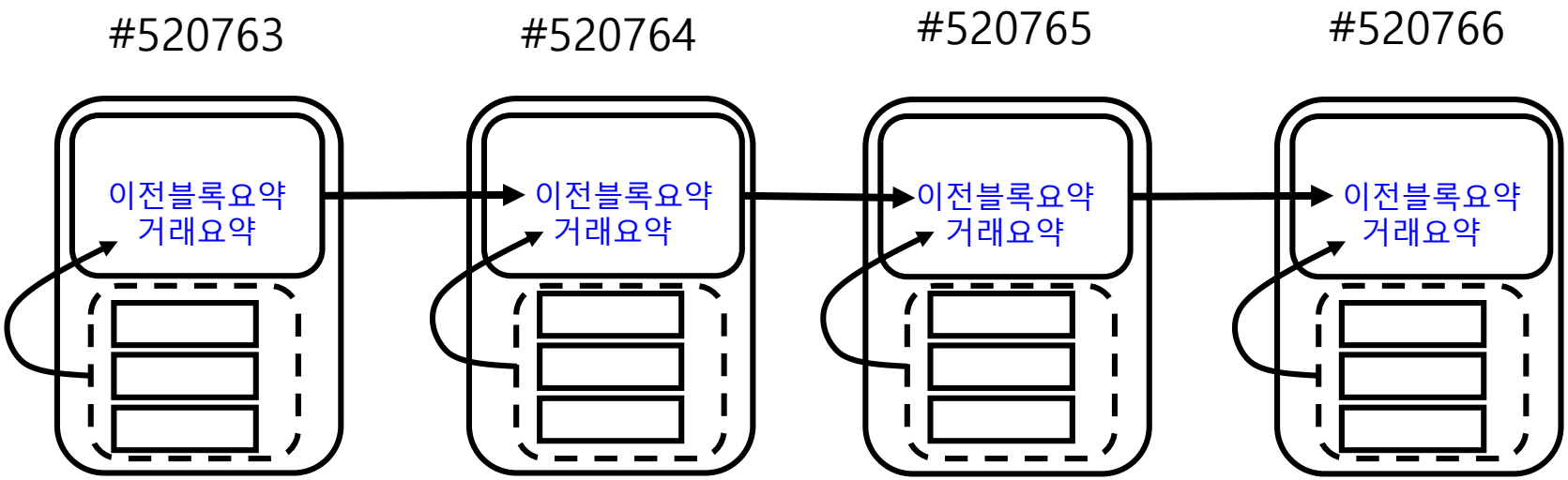
101번째장 작성
성공! 야호!



긴 체인이 승리!

Cryptographic Chain

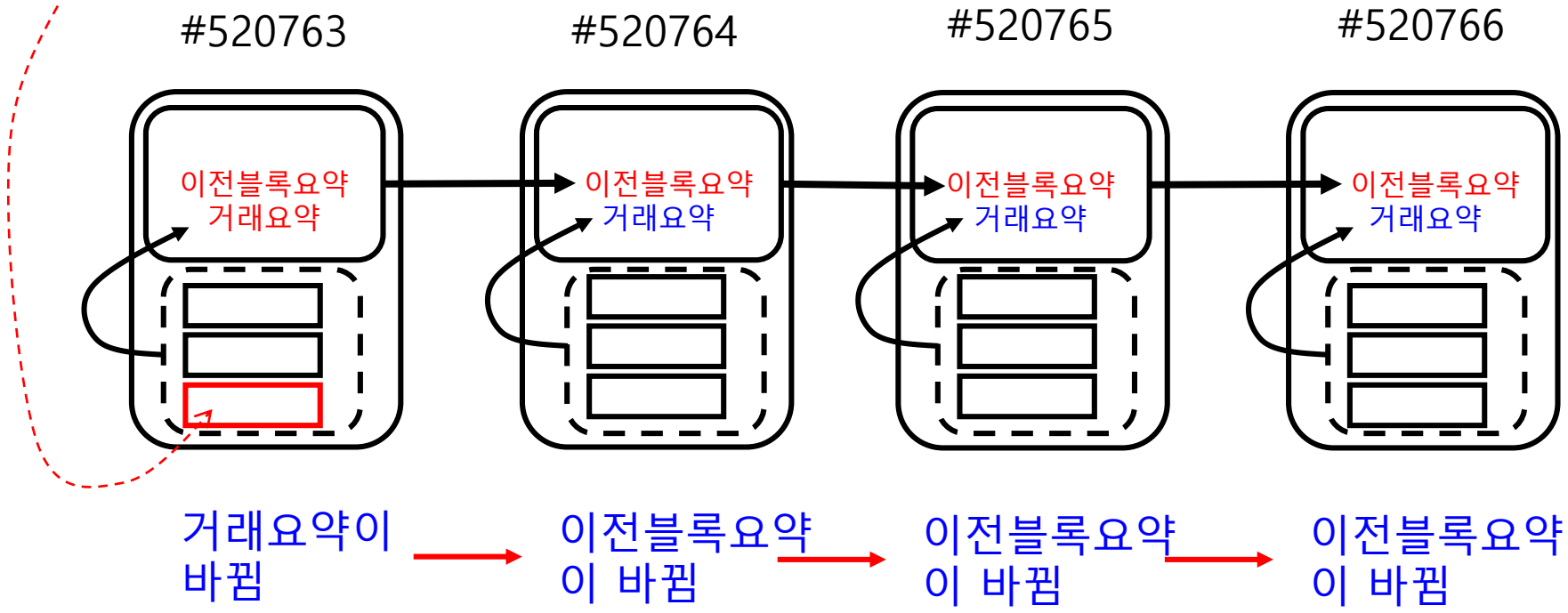
- 또한 암호학적 설계로 원장에 기록된 내용을 임의로 바꿀 수 없습니다. 이 분산원장을 블록체인이라고 칭합니다.



디지털 파일인데 왜 못 바꿔?

위조나 변조 시 바로 들통!

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



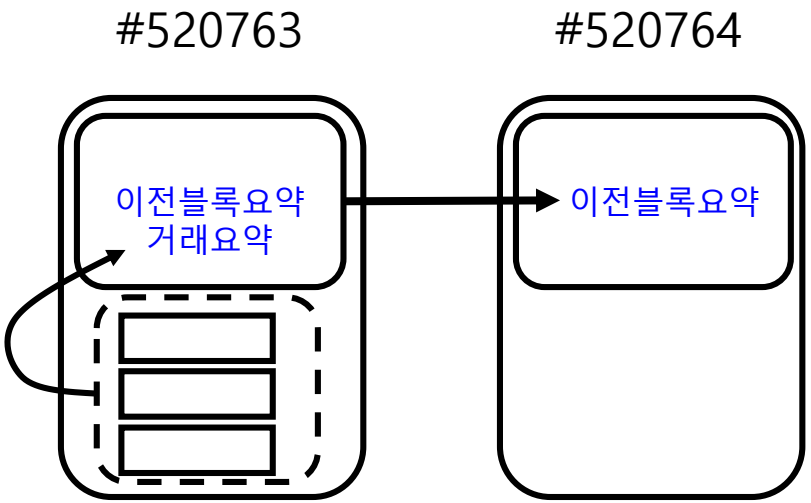
들통나지 않고 변조하려면?

해당 블록 및 그 후 요약을 모두 다시 찾아서 기록하면 됨

이런 짓을 못하게 하기 위해 작업증명이란 것을 하게 함.

Proof-of-Work (작업증명)

- 이전블록요약을 찾는 것을 매우 어렵게 만듬 (시간 소요).
- 가령 하나의 컴퓨터가 좋은 요약을 찾으려면 매우 오랜 시간이 소요 되도록 설계.
- 반면에 여러 대의 컴퓨터가 동시에 찾을 때, 그 중 한대가 단위시간 안에 답을 찾도록 작업증명 문제를 설계함.
- 블록마다 좋은 이전블록요약을 붙이도록 하므로, 전세계 모든 컴퓨터들이 협력하였음을 증명 하도록 함.



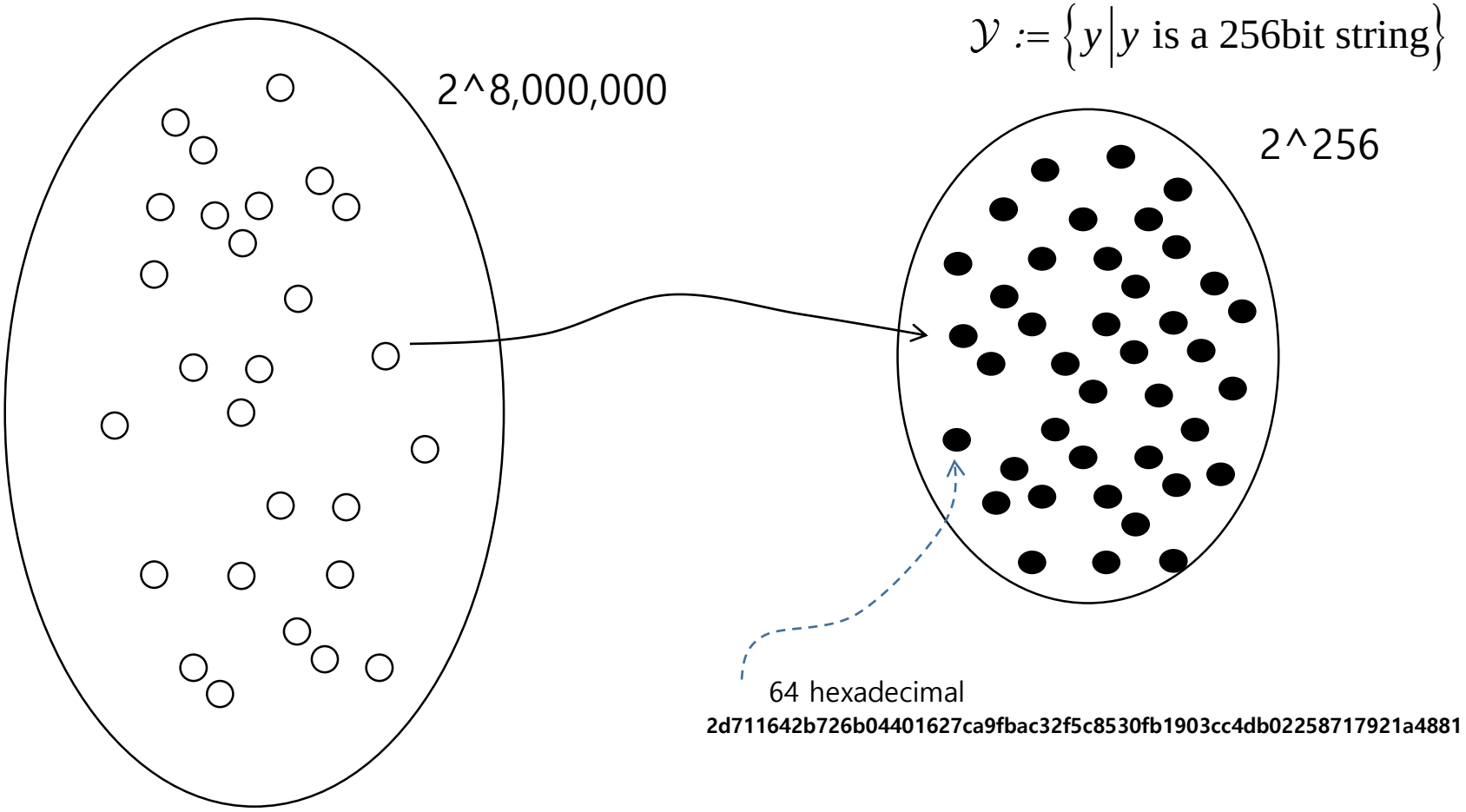
What is Hash Function?

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

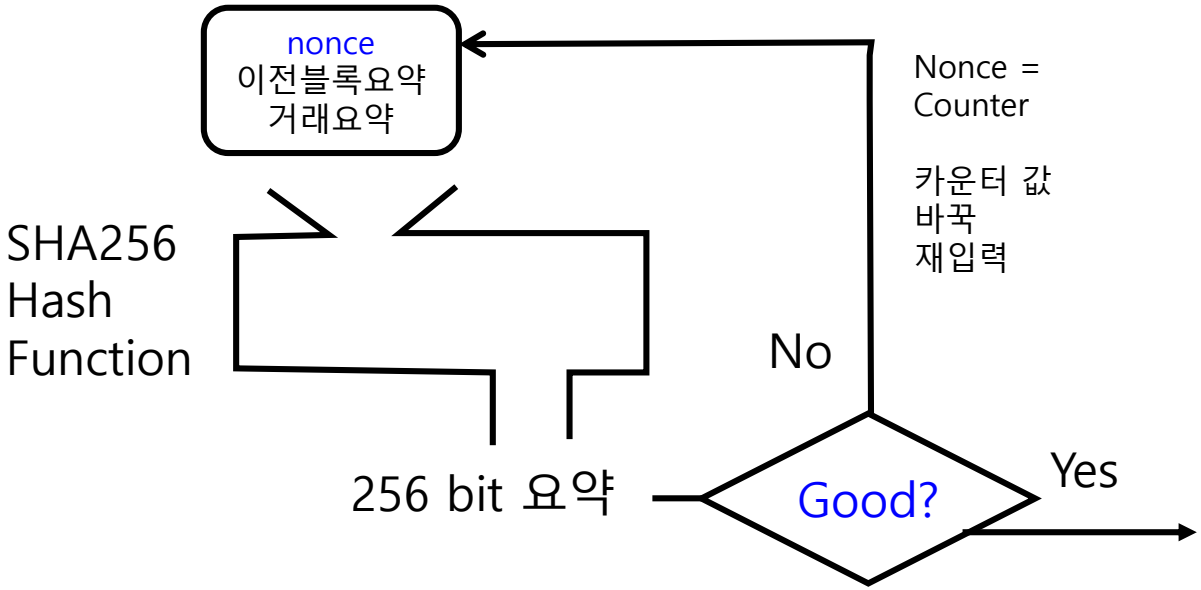
SHA256, F(x) = y

$\mathcal{X} := \{x \mid x \text{ is a message up to 1 Mbyte in size}\}$

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



Proof-of-Work (작업증명)



보통 hash 값
2d711642b726b04401627ca9fbac32f5c8530fb1903cc4db02258717921a4881

만족하는 해쉬 값
0000f727854b50bb95c054b39c1fe5c92e5ebcfa4bcb5dc279f56aa96a365e5a
→ 해당 Nonce값 기록 → 작업즉명

- 작업증명 문제
- 문제 난이도 조절: 앞의 16 개 bit가 모두 0 일것.
- 좋은 요약 즉, 만족하는 hash값을 찾을 때까지 Nonce 값을 바꾸어 가면서 해시함수에 입출력을 반복해 보는 것.
- 좋은 요약을 찾은 노드는 찾은 Nonce값을 blockheader에 기록해 놓음으로 해당 블록의 작업증명을 마친다.

채굴과 보상

- 좋은 블록요약을 찾을 때까지 전세계에서 참여하는 모든 노드들은 각자 컴퓨팅 자원을 동원하여, Hash function에 입출력을 반복한다.
  - 채굴 위해 엄청난 전기세 비용이 발생.

- Proof-of-work에 성공한 노드에게 일정량의 BTC을 주어 노력에 대한 보상을 한다.

- 이런 노드들을 채굴자라고 한다.

블록체인 데이터 무결성 확보

- 하나의 블록에 작업증명을 붙이는데 걸리는 시간은?
  - 채굴기 하나로 하면 평균 16년 정도 걸린다.
  - 그러나, 8백만개의 채굴기가 10분간 동시에 채굴 문제를 풀때, 그 중에 문제를 푸는데 성공한 채굴기가 평균적으로 한 대 나온다.
- 즉 각 블록에 기록된 Nonce값은 8백만대의 채굴기가 모두 동시에 Work를 했다는 증거다.
- 이런 Proof-of-work를 혼자 하려고 하면?
  - 한 블록도 혼자 하기는 어렵다. 16년.
- 그러므로 블록체인 안에 기록된 내용은 안 들키며 바꾸지 못 한다. 공격자는 소수라는 가정 하에.

참여자 신뢰 확보

- 누구나 작성에 참여할 수 있게 열려있고 한 번 입력된 기록은 위변조의 위험없이 보존되기 때문에 거래에 참여하는 모두에게 신뢰를 얻습니다.

- 즉 블록체인에 기록된 내용은 발생한 시간과 내용이 순전무결하게 그대로 기록되었고 보존되었다는 것을 거래에 참여하는 모두가 신뢰할 수 있다는 것입니다.

Bitcoin

- Bitcoin은 블록체인을 은행이나 국가의 개입이 필요 없는 암호화폐를 만드는데 사용했습니다.

- 즉 인터넷에서 코인을 주고 받을 수 있게 만든 것입니다.

- 마치 실물세계에서 화폐를 건네는 사람과 받는 사람이 대면 거래를 하듯이, 인터넷 상에서 거래당사자가 전자서명과 블록체인을 통해 코인의 소유권을 주고받을 수 있게 하였습니다.

신뢰하고 쓰면 화폐다!

PLANET MONEY

The Island Of Stone Money

Listen · 4:24 Queue Download Transcript

December 10, 2010 · 4:28 AM ET
Heard on Morning Edition

JACOB GOLDSTEIN DAVID KESTENBAUM

There's a tiny island called Yap out in the Pacific Ocean. Economists love it because it helps answer this really basic question: What is money?

Bitcoin

Bitcoin은 디지털 화폐입니다.

화폐는 신뢰에 기반 한 가치교환 수단입니다.

- 요즘에는, 화폐는 계좌에 찍혀진 숫자에 불과합니다. 그저 출금계좌에서 입금계좌로 숫자가 이동 할 뿐이지요.

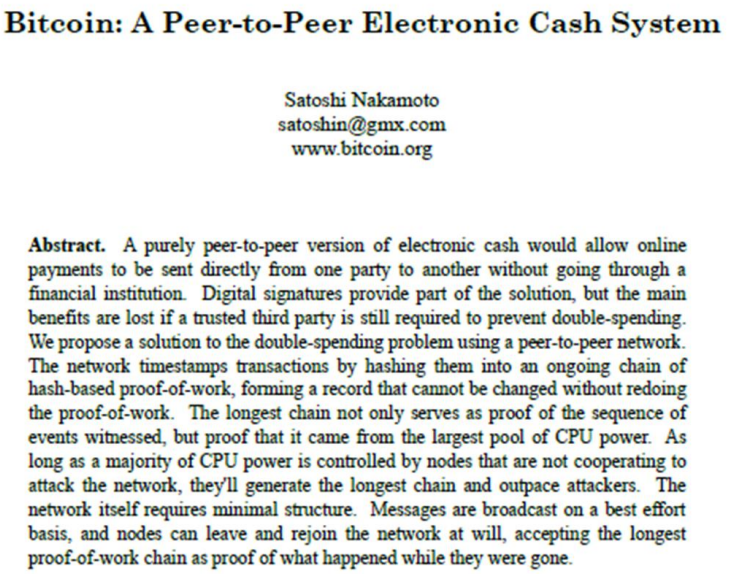
화폐의 시장가치는 화폐를 발행한 국가의 존재에 있습니다.

- 불법적 화폐 발행과 유통을 적발하고 엄단하는 **공권력을 행사하는 국가를 신뢰.**
- **갖고 있으면 언제든지 필요한 서비스 및 제품을 제공 받을 수 있다는 신뢰에 기반.**

신뢰도가 높고 수요가 많은 화폐는 높은 값어치를 갖게 되는 것입니다.

Bitcoin은 인터넷상에서 거래되는 디지털화폐를 생산하고, 유통하며, 거래를 관리하는 컴퓨터 알고리즘.
2009년에 알고리즘과 논문이 공개되었지요.

Bitcoin은 국가의 개입이 없었음에도 불구하고, 화폐로써의 지위를 확보하고,
수요에 기반 한 시장가치를 창출하는데 성공한 것 인류 첫 번째 가상 화폐입니다.



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

채굴자들이 각 거래를 인증하고, 인증된 거래는 장부에 기록하고, 장부에 기록된 거래는 절대 수정하지 못하게 하는 것.

첫 째 소유권 확인
둘 째 이중거래 방지
셋 째 블록체인 (위변조 불가능한 디지털 거래 장부)에 거래 기록

How?

- 거래 장부는 인터넷에 실시간으로 공개
  소유권 검증과 이중거래 방지 문제는 방지될 것으로 생각됩니다.
- 기록된 거래를 어떻게 임의로 수정하지 못하게 보관하고 관리할 것인가의 문제는 블록체인 기술로 해결

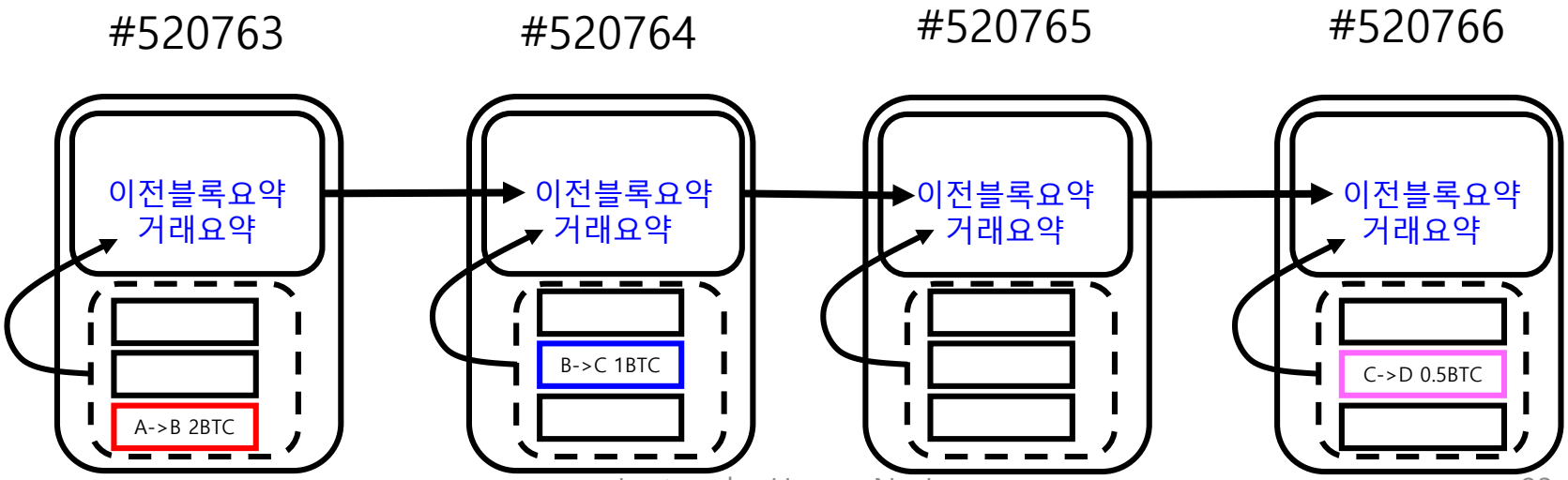
블록체인 : 디지털 파일에 들어간 내용을 위변조 할 수 없게 기록하는 기술

Bitcoin기술은 국가의 개입이 없어도, 인터넷 상 거래를
실시간으로 관리 추적할 수 있고, 동시에 보안과 신뢰성을 크게 높일 수 있음을 보여주었습니다.

Blockchain

- **시간 1: A가 B에게 코인 두 개를 지불합니다. A의 싸인.**
- **시간 2: B가 C에게 코인1개를 지불합니다. B의 싸인.**
- **시간 3: C가 D에게 코인 0.5개를 지불합니다. C의 싸인.**

- 와 같은 코인거래내용이 체인 안에 시간과 함께 모두 기록되도록 합니다.
- 이 체인을 들여다보면 누가 언제 누구에게 얼마만큼의 코인 소유권을 이전하였는지 알 수 있습니다.
- 이 거래장부는 누구나 언제든지 볼 수 있도록 인터넷에 공개됩니다.
- 장부를 열람해 보면, 어떤 코인이 누구에게 속해 있는 지, 소유권의 상태를 곧 바로 파악할 수 있습니다.



Blockchain

누구나 열람할 수 있는 거래 장부는 사실 암호화 되어 있습니다.
누가 해당 동전의 소유권을 갖고 있는지 확인 할 수는 있으나,
소유권자가 아니면 그 권한을 행사 할 수는 없게 만들어 졌습니다.

앞의 예시에서
A → A의 공개키
B → B의 공개키
C → C의 공개키

시간 2의 거래에서 코인을 받는 C는 B가 1BTC를 소유하고 있음을 어떻게 확인 하나?

답: 블록체인을 검색하여 거래 "A→ B 2BTC" 즉 B가 수취인으로 된 거래기록이 있는 지 찾아서 확인해 본다.

시간2의 거래내역을 정말 B가 보낸 것인지 어떻게 확인하나?

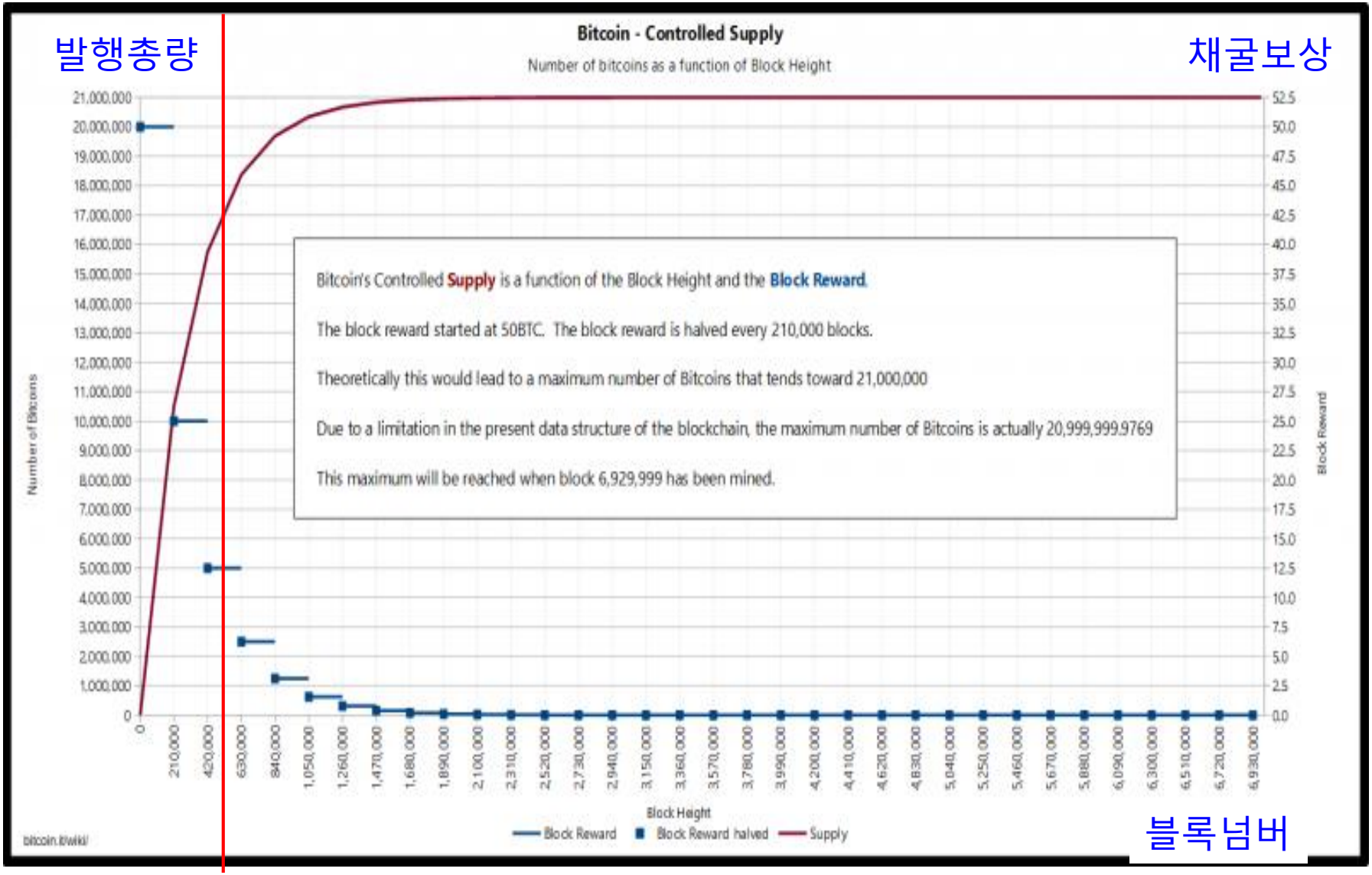
답: 거래내역을 B가 개인키로 싸인한 디지털싸인을 B의 공개키로 Decryption해 보므로 안다.

이중거래 방지

- 이중거래를 의심해봐야 하는 사람은 코인을 받는 사람
- 코인을 건네는 사람이 동 시간대 혹은 그 이전에 다른 이에게 이미 양도하지 않았는가 확인 필요
- 블록체인에 각 거래가 시간의 순으로 time-stamp가 찍혀 있고 공개 되어 있으므로 쉽게 확인 가능 (컴퓨터가 함, 채굴기)

Bitcoin은 화폐를 발행합니다!

Bitcoin Issuance Schedule



2018년 현재

Bitcoin Issuance Plan by the Year

Date reached	Block	Reward Era	BTC/block	Year (estimate)	Start BTC	BTC Added	End BTC	BTC Increase	End BTC % of Limit
2009-01-03	0	1	50.00	2009	0	2625000	2625000	infinite	12.500%
2010-04-22	52500	1	50.00	2010	2625000	2625000	5250000	100.00%	25.000%
2011-01-28	105000	1	50.00	2011*	5250000	2625000	7875000	50.00%	37.500%
2011-12-14	157500	1	50.00	2012	7875000	2625000	10500000	33.33%	50.000%
2012-11-28	210000	2	25.00	2013	10500000	1312500	11812500	12.50%	56.250%
2013-10-09	262500	2	25.00	2014	11812500	1312500	13125000	11.11%	62.500%
2014-08-11	315000	2	25.00	2015	13125000	1312500	14437500	10.00%	68.750%
2015-07-29	367500	2	25.00	2016	14437500	1312500	15750000	9.09%	75.000%
2016-07-09	420000	3	12.50	2016	15750000	656250	16406250	4.17%	78.125%
2017-06-23	472500	3	12.50	2018	16406250	656250	17062500	4.00%	81.250%
	525000	3	12.50	2019	17062500	656250	17718750	3.85%	84.375%
	577500	3	12.50	2020	17718750	656250	18375000	3.70%	87.500%
	630000	4	6.25	2021	18375000	328125	18703125	1.79%	89.063%
	682500	4	6.25	2022	18703125	328125	19031250	1.75%	90.625%
	735000	4	6.25	2023	19031250	328125	19359375	1.72%	92.188%
	787500	4	6.25	2024	19359375	328125	19687500	1.69%	93.750%

Seigniorage Effect

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

Seigniorage and the Federal Reserve

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

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

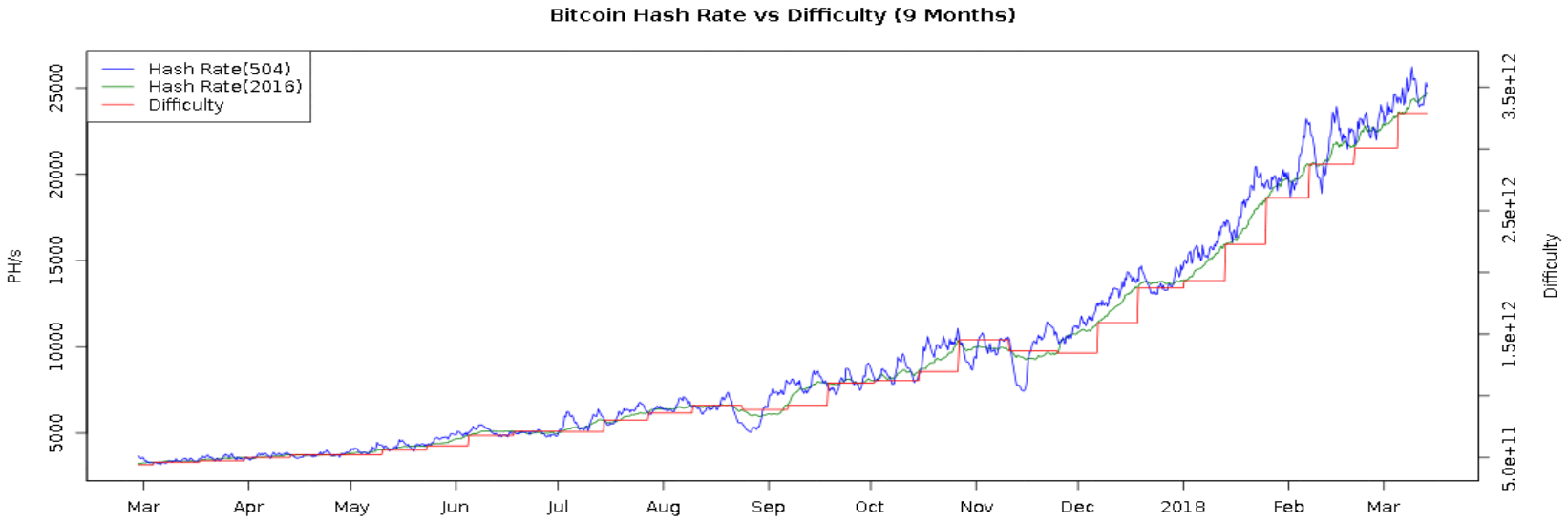
Bitcoin은 전기를 엄청나게 씁니다

Ebit E10, mining **SHA-256 algorithm** with hashrate of **18Th/s** and power consumption of **1650W. 개당 3000불 수준.**

Bitcoin 네트워크의 총 Hashrate이 계속 급증하고 있으며, 현재는 약 30EH/s 정도입니다.

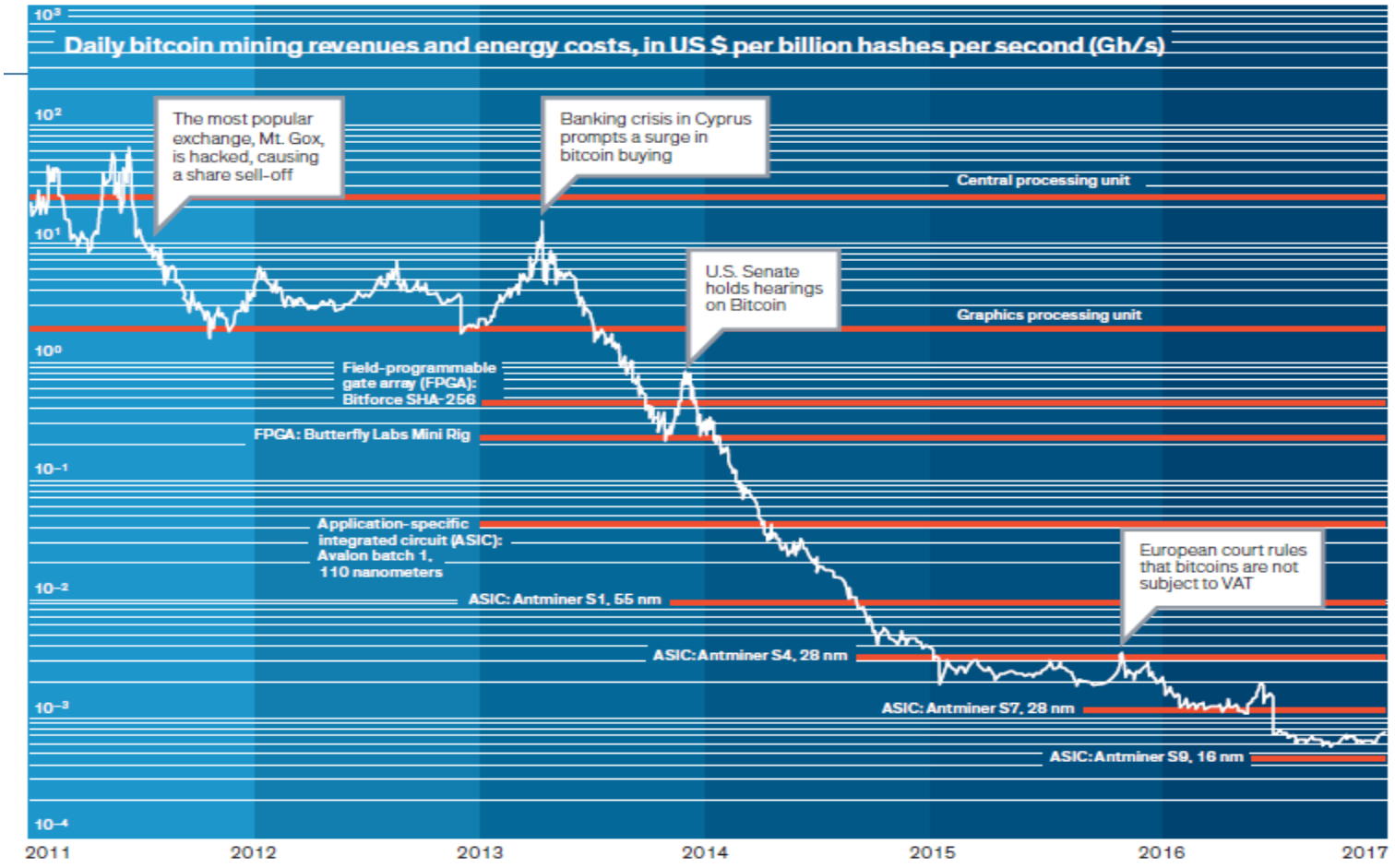
Difficulty(73bit leading zeros)를 증가시켜 매 10분마다 1블록이 채굴되도록 조절합니다.

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



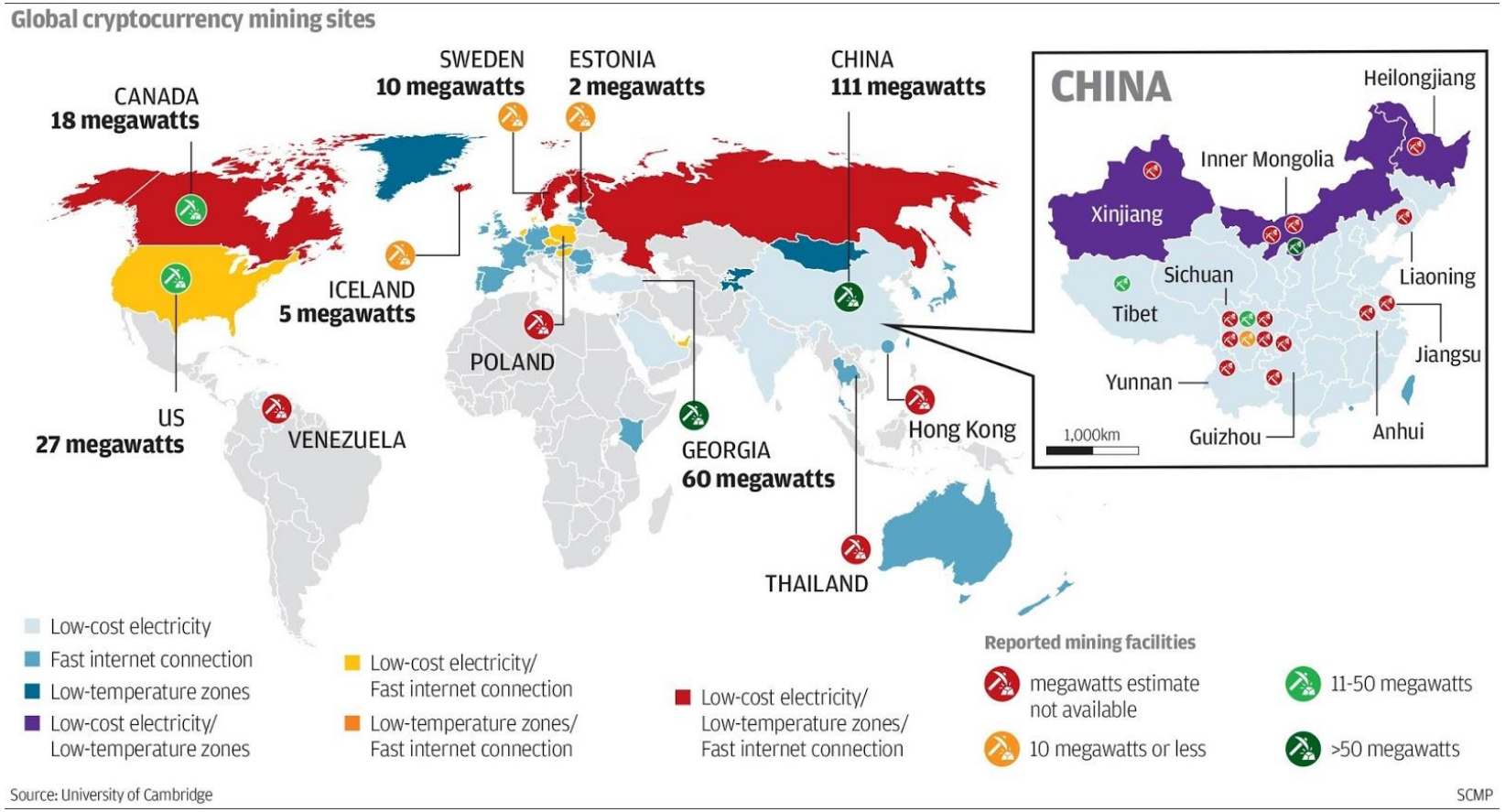
https://bitcoinwisdom.com/bitcoin/difficulty

Revenue from Mining vs. Energy Cost



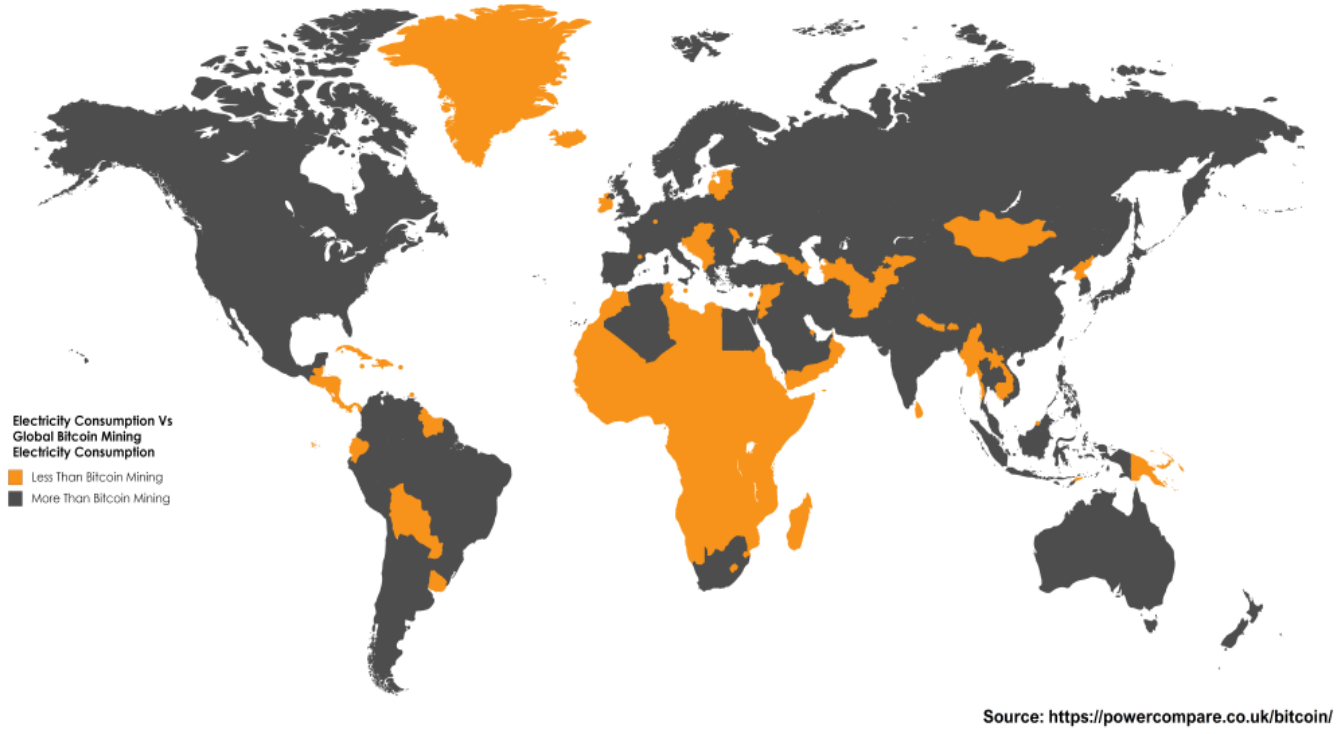
Sisyphean Slide: Daily revenues for mining bitcoins [white], in US dollars per unit of computational power, are generally somewhat higher than the daily energy costs [red] of running the computers.

PoW, 전기에너지 소모, Monopolized



Energy spending for bitcoin mining exceeds energy consumption of a country

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



Bitcoin

- 블록체인 무결성을 코인거래 원장으로 썼음
- PoW라는 Computation Intensive 방법으로 데이터 무결성 확보
- 채굴 보상, 채굴자 Incentivising, 시스템 유지
- 2009년 부터 지난 9년 간 큰 문제없이 한 순간의 멈춤도 없이 작동해온 살아 숨쉬는 화폐 시스템.
- 국경이 없는 Global 디지털 화폐.
- Bank와 국가에 대한 신뢰가 엷어지던 2008년 경에 탄생하였음.
  - Decentralization
  - Reforming Wall Street
  - Unbundling big corporations
  - Sharing economy

ISSUES
Reforming Wall Street

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

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

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

The Evolution of Trust

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

Natalie Smolenski

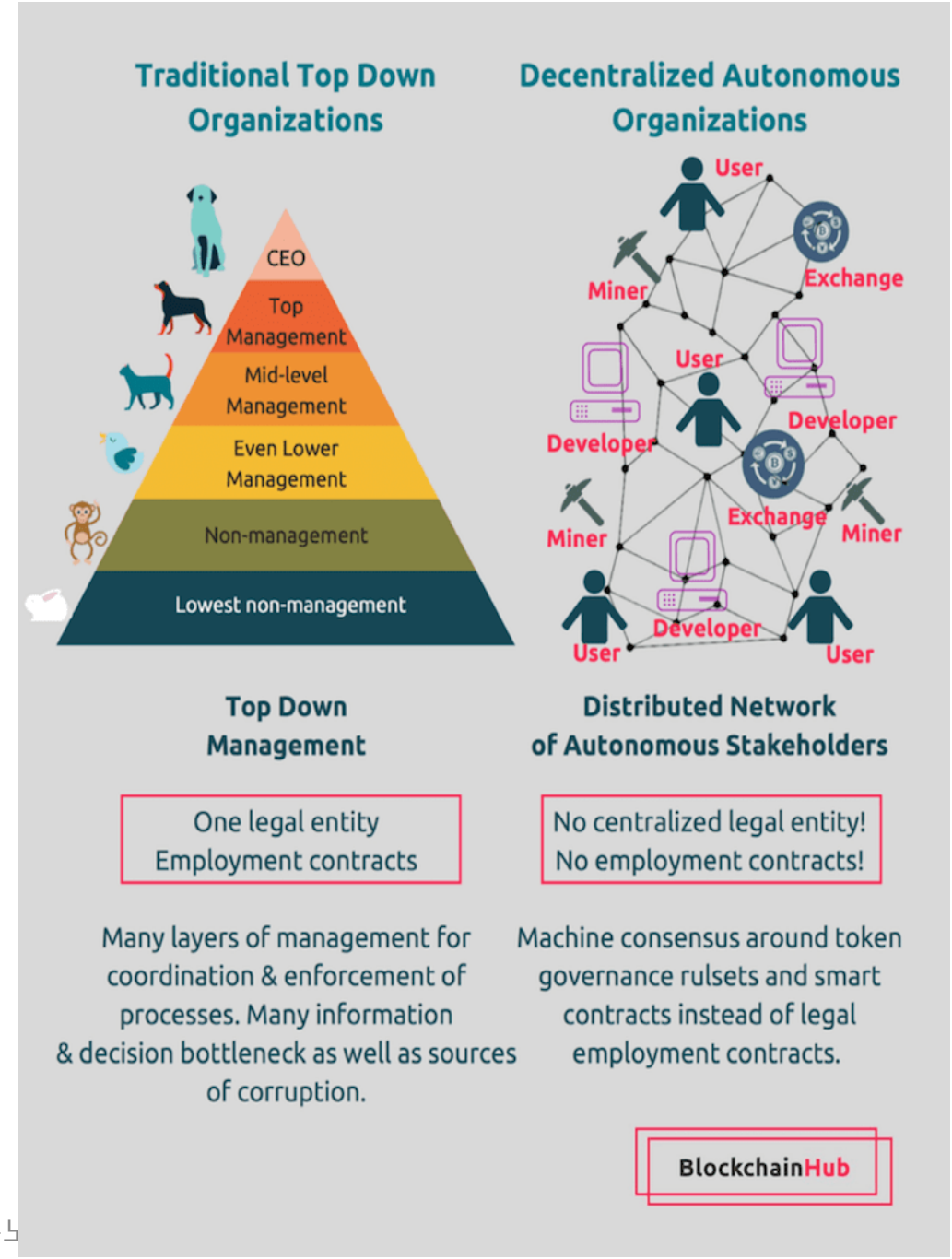
- Banks and governments have in many ways failed to broker trust for the global economy, especially in the past few decades. Ordinary people have grown wary of centralized power and are seeking alternatives.
- Bitcoin—and blockchain technology in general—allows the brokering of trust to be shifted toward 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.

Bitcoin Economy

- 설계자
  - 연간코인 발행 량, 거래 및 처리 속도, 인센티브, 블록 체인에 담을 내용 등 master plan 설계,
- 개발자 pool
  - 버그 및 문제점 개선
  - 시스템 유지 및 보수
- 사용자 pool
  - 송금, 소매, 도매, 은행
- Miner pool

의도치 않았지만 생겨난

- Exchange
- 투자자
- Crowd funding



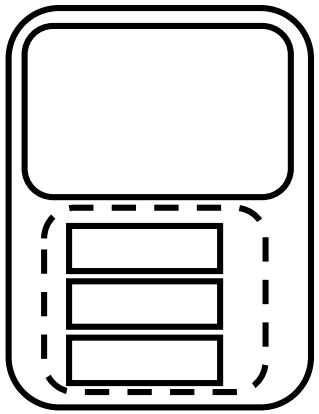
Ethereum

- Vitalik Buterin had worked in the Bitcoin community.
- In 2013, Vitalik published the Ethereum white paper, containing technical design for protocol and smart contracts.
- In January 2014, Ethereum was announced by Vitalik, The North American Bitcoin Conference, Miami, Florida, USA.
- Then, Vitalik also started working with Dr. Gavin Wood and co-founded Ethereum.
- The Ethereum client has been implemented by following the Yellow Paper in seven programming languages including C++, Go, Python, Java, JavaScript.
- Source: http://ethdocs.org/en/latest/introduction/history-of-ethereum.html

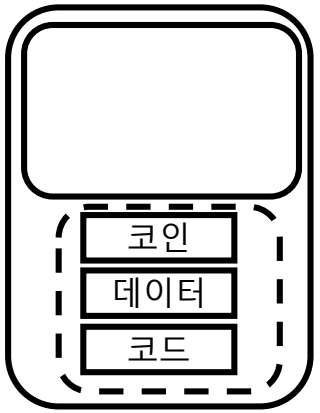
Ethereum

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

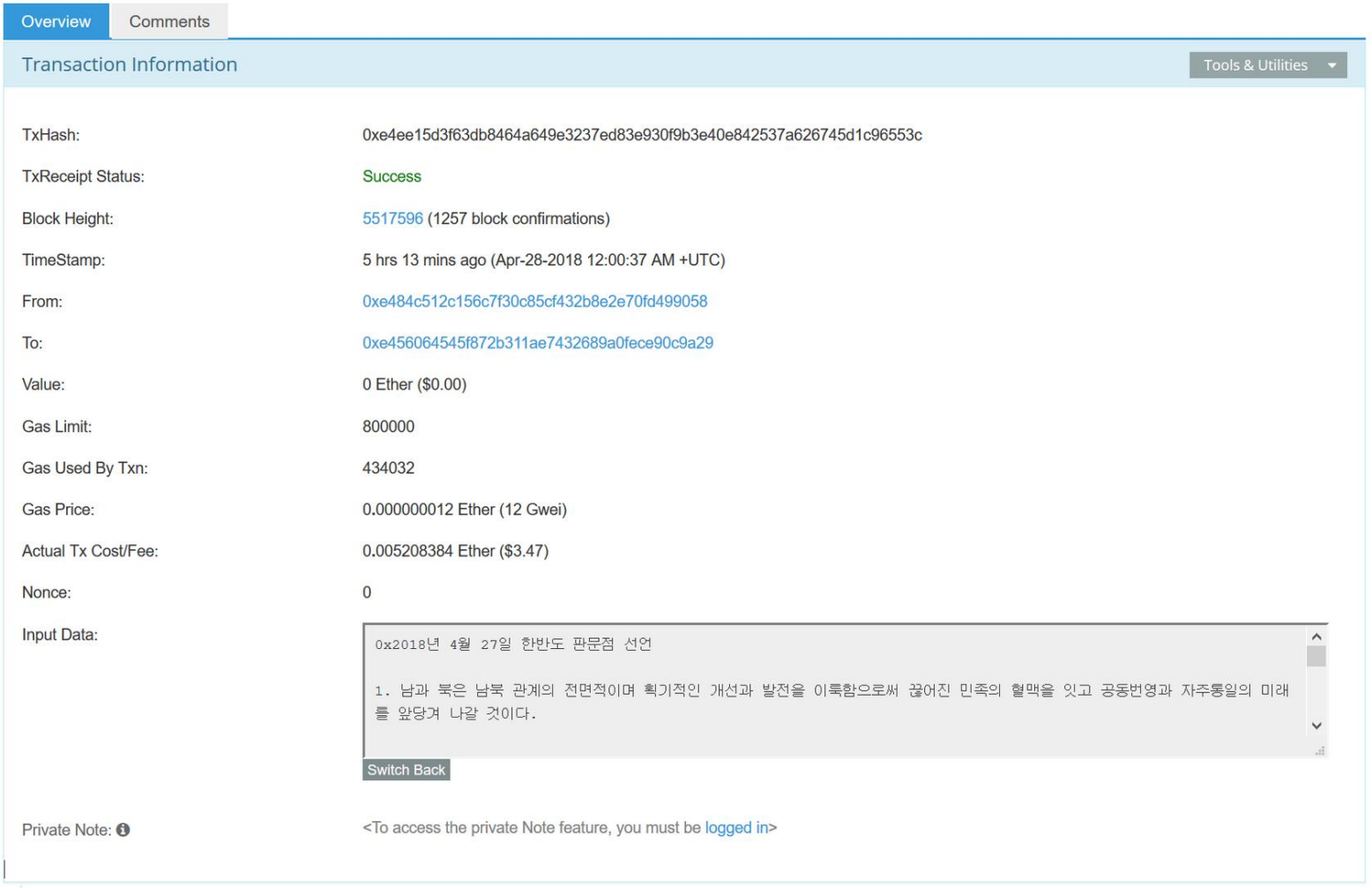
Bitcoin 블록
은 코인거래만
담는 반면



Ethereum블록,
컴퓨터코드도 넣고
데이터도 넣자

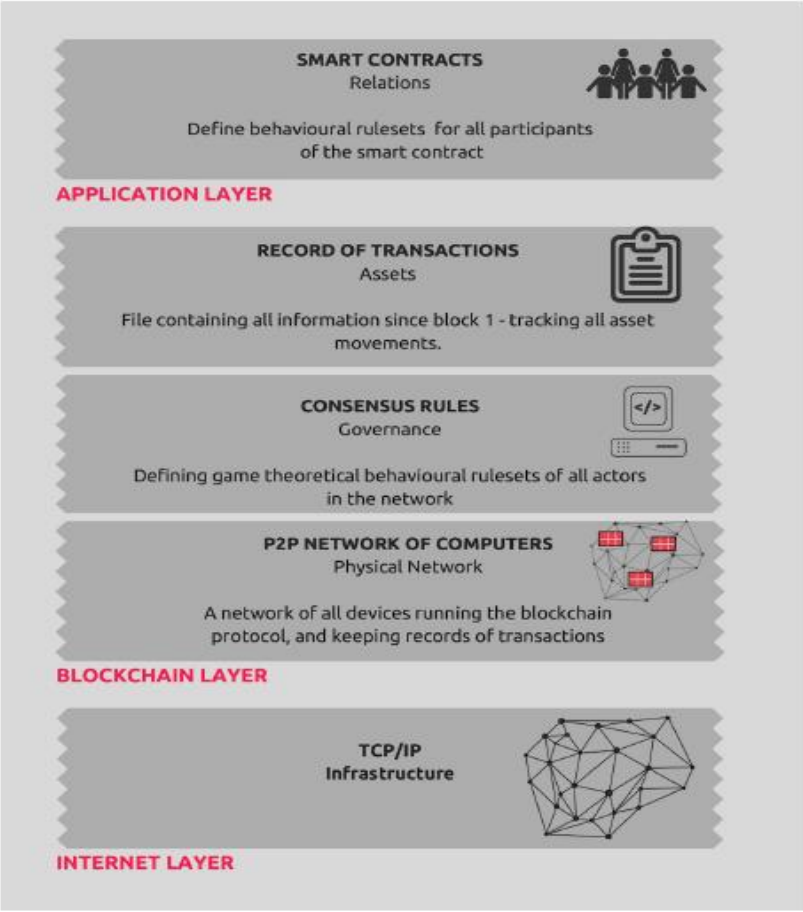


Ethereum 블록에 들어간 판문점 선언문



Smart Contracts

- By decoupling the smart contract layer from the blockchain layer, blockchains like Ethereum aim to provide a more flexible development environment than the Bitcoin blockchain.
- These smart contracts are a piece of code running on top of a blockchain network, where digital assets are controlled by that piece of code implementing arbitrary rules.
- If and when all parties to the smart contract fulfill the pre-defined arbitrary rules, the smart contract will auto execute the transaction.
- Smart contracts can be used for simple economic transactions like sending money from A to B.
- Registering any kind of ownership and property rights like land registries and intellectual property, or managing smart access control for the sharing economy, just to name a few.



Blockchain Technology Stack: Ethereum & similar Blockchains
Inspired by Florian Glatz: Source

③ 계약의 스마트화

■ 블록체인의 보안성을 활용한 스마트 계약(Smart contract)*을 통해 기존 계약 체결 및 이행에 소요되던 비용과 시간을 절감하고 강제 계약 실행으로 거래미이행 위험을 낮춤

* 프로그래밍된 조건부 계약 실행 시스템으로, 일정 조건을 충족하는 경우 약속한 계약을 강제적으로 또는 자동화하여 실행하는 것을 의미

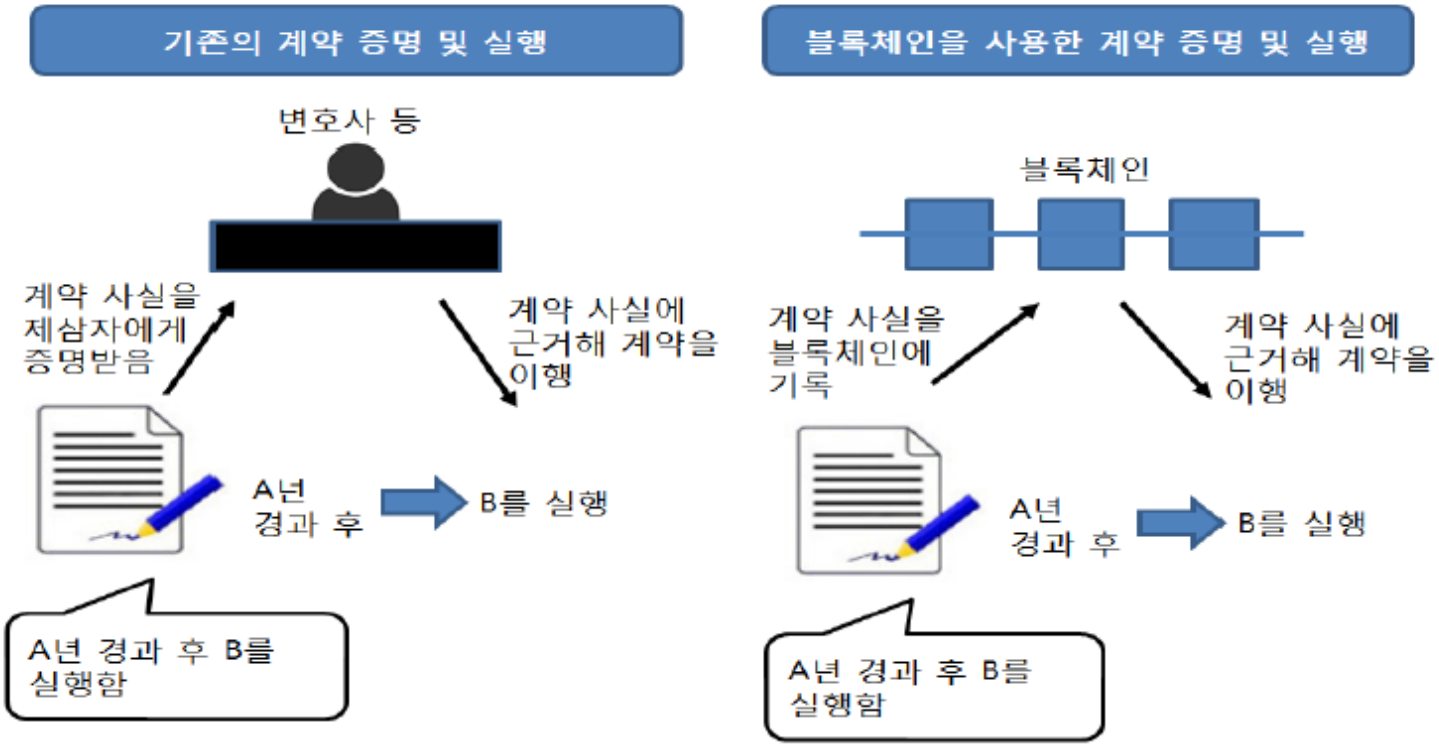
● 이더리움(Ethereum) 등 스마트 계약에 특화된 블록체인이 등장하면서 중개자를 통하지 않는 다양한 형태의 계약 실행 자동화가 가능

– 이해 당사자 간 공유된 블록체인을 통해 변호사, 중재자 등 없이도 계약 체결이 가능하며 계약의 결과에 대한 신뢰를 보장할 수 있음

* 주식거래시 체결과 동시에 정산이 가능해지며, 과다한 거래비용으로 활성화되지 못한 글로벌 소액결제도 활성화될 수 있음

스마트계약 vs 기존계약

<기존 계약관리와 블록체인 기반 계약관리(스마트 계약) 비교>



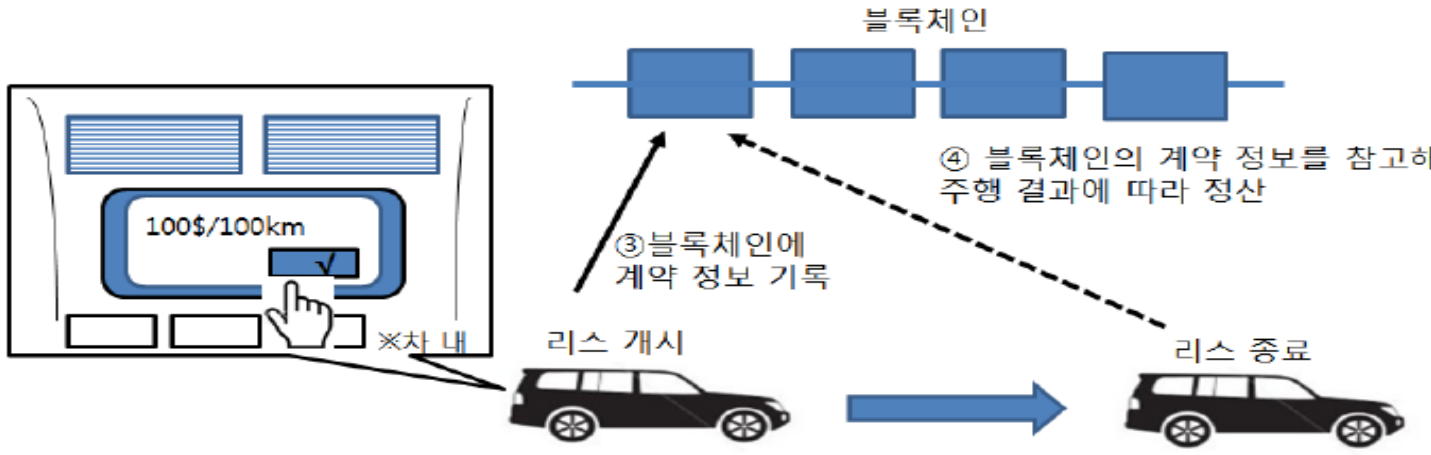
자료 : 블록체인 구조와 이론, 2017

무역협회자료

금융분야 적용사례

<금융 분야 블록체인 적용 사례 – 자동차 리스 및 보험>

- 글로벌 결제 서비스 기업 비자(VISA)는 2015년 디지털 서명 관리기업 다큐사인(Docusign)과 진행한 자동차 리스 및 보험과 관련된 계약을 블록체인으로 관리하는 실증실험을 공개함
- 사용자가 차내의 터치패널형 단말기를 통해 자동차 리스 및 보험 계약을 종이 없이 완료하도록 함



① 차 내의 단말로부터 자동차 리스나 보험 계약을 선택
② 사용자는 터치 패널에 서명해 계약을 확정

자료 : 블록체인 구조와 이론, 2017

무역협회자료

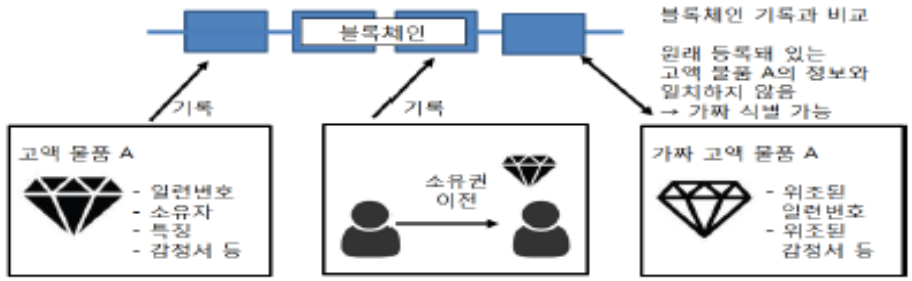
② 제조 · 유통 – 공급망 가시성 확보 및 신규 비즈니스 모델 발굴

■ 제조 · 유통업에서는 제조 및 유통 이력 통합관리, 원자재 정보 상시공유 등 공급망 가시성 제고 및 최적화에 가장 많이 활용

● 특히 IoT 기술과 결합할 경우 실시간 정보수집이 가능하기 때문에 식료품과 고가품의 이력추적 관련한 시범적용이 활발

<제조 · 유통분야 블록체인 적용 사례① – 이력추적>

- (중국 월마트) 2016년 IBM, 칭화대와 협력하여 돼지고기의 안전성 및 품질과 관련된 이력 추적 및 공급망 관리 전 과정에 블록체인을 시범 도입. 돼지고기 이력 및 유통정보는 공급망 참여자, 소비자와 실시간으로 공유되며 향후 구제역 등 문제발생시 신속한 유통과정 역추적이 가능
- (영국 프로베넨스) B2B 스프트웨어 스타트업인 프로베넨스(Provenance)는 2016년 일본 레스토랑에 공급되는 인도네시아산 참치의 공급망을 대상으로 블록체인을 시범 적용해 인증서의 중복 확인 비용 절감 및 식품 이력 추적의 투명성 확보 효과를 거둠
- (영국 에버렛저) 영국 스타트업 에버렛저(Everledger)는 다이아몬드 감정 정보 및 출처 기록을 블록체인으로 관리하여 감정서 위조 및 사기문제를 해결



자료 : 블록체인 구조와 이론, 2017

무역협회자료

국내외 제조기업 또한 자율주행차, 스마트 홈 등에 블록체인을 적용하여 고객 맞춤형의 신규 비즈니스 모델을 발굴 중

<제조 · 유통분야 블록체인 적용 사례 ② - 신규 비즈니스 발굴>

- (도요타) 완성차 사업에 블록체인을 도입하여 자율주행과 공유경제 등의 부문으로 확장을 준비

  - 미국 MIT 산하 미디어랩과 제휴하여 자율주행차 주행데이터 공유, 자동차와 차고의 공유 및 카풀 관리, 차량 사용정보 저장 등을 위한 블록체인 기술도입을 연구 중 (Fortune, 2017)

- (삼성전자) 2017년 IBM과 협력하여 블록체인 기술과 사물인터넷(IoT)이 적용된 ADEPT (Autonomous Decentralized Peer-to-Peer Telemetry) 플랫폼을 공개(2017)

  - ADEPT는 스마트 전자기기를 IoT에 연결하여 주변사물들과 소통을 통해 소모품 교체를 위한 주문, 자체 점검 시스템을 통한 유지 관리 등을 스스로 해결하는 솔루션

무역협회자료

③ 문화콘텐츠 – 저작권 보호

■ 블록체인 기반의 인증 서비스를 통해 저작권 등록 및 증명, 콘텐츠 이력 추적을 용이하게 함으로써 불법적인 복제와 유통을 방지하는데 활용

● 지적재산권의 소유자 이력을 포함한 모든 거래 내역을 활용해 향후 저작권료 지급 자동화와 같은 스마트 계약까지 적용영역이 확대될 것으로 예상

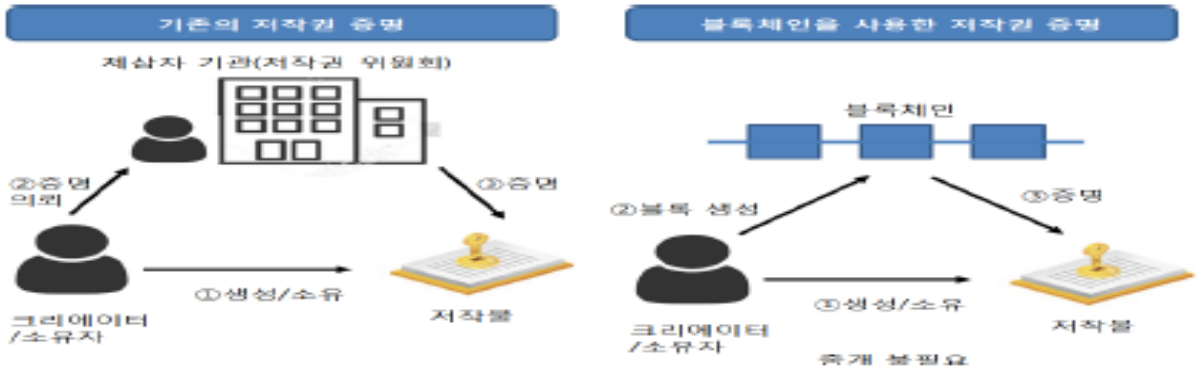
<문화콘텐츠 분야 블록체인 적용 사례 – 저작권 관리>

■ (디지털 음원유통–우조뮤직) 영국 음원유통 서비스 기업 우조뮤직은 블록체인을 활용해 음원 사용 시 각국의 저작권 징수기관 보고 및 수익금 배분을 자동화

– 사용자가 음원을 구매할 경우 프로듀서, 작사가, 엔지니어, 가수 등 음원제작에 참여한 구성원들은 중개자 없이 사용자에게 직접 저작권료를 징수할 수 있음

■ (예술품 저작권–블록아이(BLockai)) 미국 스타트업으로 블록체인 기술 기반 저작권 등록 서비스를 제공

– 예술가들이 저작권 협회를 거치지 않고도 자신의 작품에 대한 저작권을 저비용으로 인증받을 수 있도록 블록체인 기술을 활용해 저작권 데이터를 관리



자료 : 블록체인 구조와 이론, 2017

무역협회자료

④ 공공 – 투명성 강화

■ 토지 · 주택 · 차량관리, 선거 및 투표관리, 의료정보관리 등 관리투명성이 중요한 공공서비스를 중심으로 블록체인 도입을 검토 중

● 공공기록물 관리 및 예산 집행 시 투명성, 관리효율성 제고로 운영비와 같은 제반비용 절감 효과가 기대됨

<주요국의 공공 분야 블록체인 적용 현황 및 계획>

국가	활용현황 및 계획
영국	각종 공과금 및 과징금 징수, 납세, 여권발급, 토지등기 내역 관리 등 일선 공공업무와 기록 통합 관리에 도입 검토
미국	우편서비스, 의료정보 기록 및 공유 등의 분야에 활용 검토
우크라이나	투표 관리 및 운영 방안 활용 논의 중
에스토니아	'키 없는 전자서명 인프라(KSI)'를 도입해 현장업무에 활용
온두라스	국가 토지대장 관리를 기존의 단순 전산 데이터베이스 방식에서 블록체인 방식으로 전환하여 주택담보, 대출, 계약, 광물관리에 적용할 계획
한국	(외교부) 아포스티유(Apostille)[5] 인증서 발급 기록 시스템을 블록체인 기반으로 구축하는 계획 발표 (서울시) 개인정보제공에 동의만 하면 고용노동부와 국민건강보험공단의 서류 발급 과정 없이 각 시에서 관련 기관의 정보를 한 번에 조회해 청년수당을 지급할 계획 (선관위) 투표과정에 블록체인 기술을 활용하는 시범사업 추진 중 (조폐공사) 블록체인 기반 지불 인증 시스템을 구축해 모바일 신분증 및 모바일 상품권 시범사업을 실시할 예정

자료 : 블록체인 기술의 산업동향 및 특허동향(한국지식재산연구원) 재구성

무역협회자료

Blockchain and Sharing Economy

Sharing Economy 와 Blockchain

- 소유권자가 쓰지 않고 있는 유휴자원을 나눈다면?
- 자동차, 집, 주차장, cpu 시간 등 유휴 제품 및 서비스를 소유권자가 개방하고 공유할 때, 소유권자와 사용자가 둘 다 win-win하는 상황을 만들어낼 수 있음.
- 이때 예약과 사용료 정산이 중요
- Blockchain의 Smart Contract를 활용하여 예약하고, 암호화폐을 통하여 정산이 강제되도록 하면 신뢰에 기반한 공유경제 활성화를 이루어 낼 수 있음
  - Smart City 개념에 blockchain이 들어가 있는 이유!

Why Blockchain Is The Future Of The Sharing Economy (1)

- Omri Barzilary, Aug. 14th, 2017, Forbes.
- *Will Blockchain Ignite Fractional Ownership Market For Homes?*
- *Tezos $232 Million ICO May Just Be The Beginning*

These days, the sharing economy feels a bit past its prime. "The 'Sharing Economy' is Dead," Fast Company declared two years ago, summarizing a general sense of fatigue with what now feels like a wildly overhyped idea. But, according to many, the fusion of blockchain and the sharing economy may create a revolution that will transform our economy and share the wealth beyond certain companies and individuals.

Smart contracts help to unbundle ownership!

Blockchain can help energize and unlock the sharing economy by making it cheaper to create and operate an online platform. For example, transactions could be coordinated by self-executing smart contracts or performed at lower cost by other small competing providers. The next phase of the sharing economy can emphasize today's inequalities or ease them, depending on the purpose of the technology itself.

Why Blockchain Is The Future Of The Sharing Economy (2)

- MyBit, the blockchain powered platform connecting investors to future-proof projects, is a good example to a company that utilizes this idea. The company's vision is to democratize the ownership of machines and its resulting revenue streams instead of letting them fall into the control of centralized financial institutions. The platform will be applicable to drones, self-driving cars, smart homes, autonomous machinery, 3D printers and more.

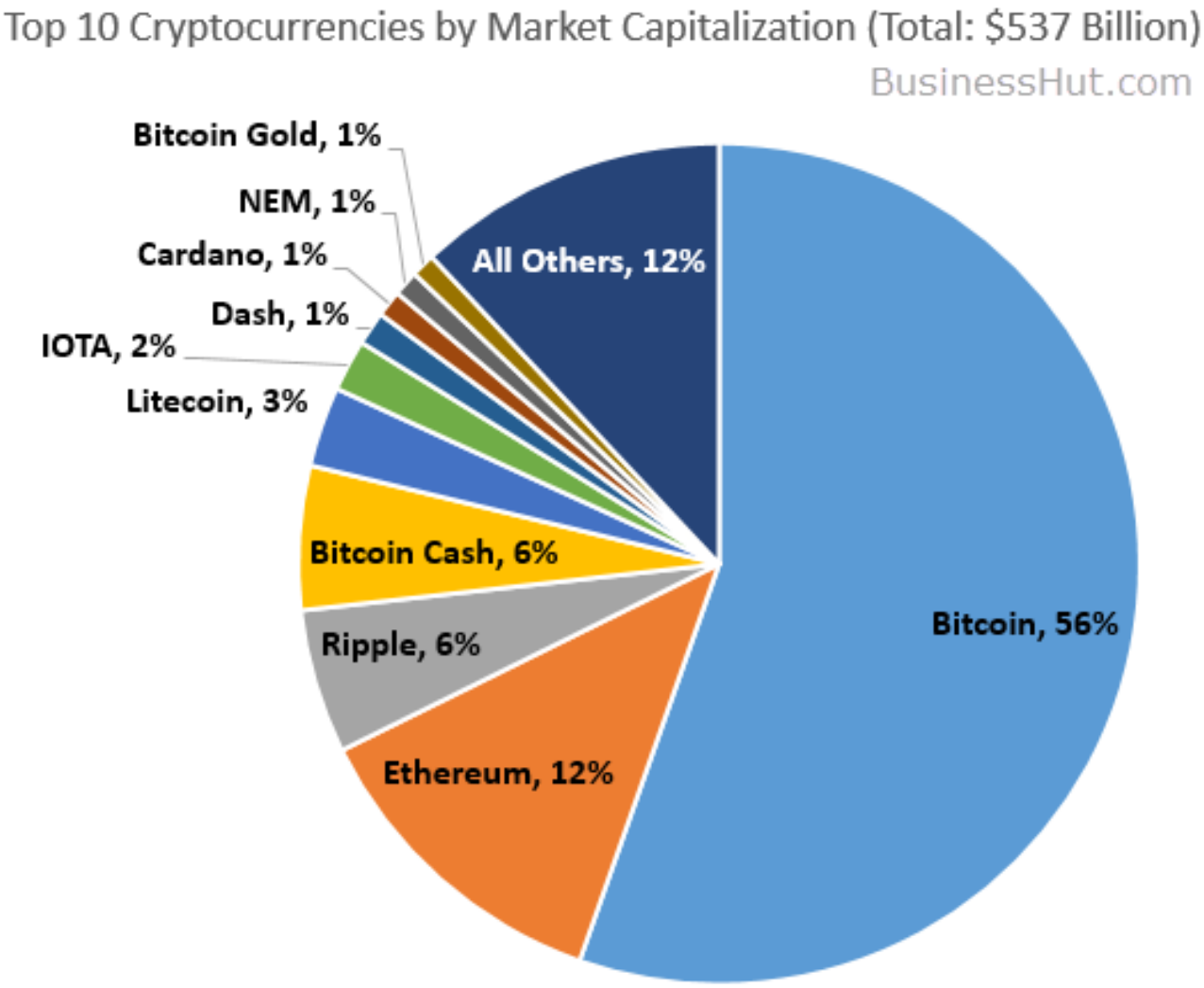
Tokens raised, worth 2.7 Million USD, ICO July 2017

Why Blockchain Is The Future Of The Sharing Economy (3)

- Slock.it, which recently secured $2M in seed funding, is another example of a company who is trying to shake up the sharing economy by enabling both companies and individuals to rent, sell or share any connected smart object. Since its inception in November 2015, Slock.it's mission has been to develop Universal Sharing Network, or "USN". Build on top of the public Ethereum Blockchain, the USN will provide users a set of mobile and desktop applications to find, locate, rent and control any object mediated by smart contracts, from anywhere in the world

각종 다양화 축과 변종코인

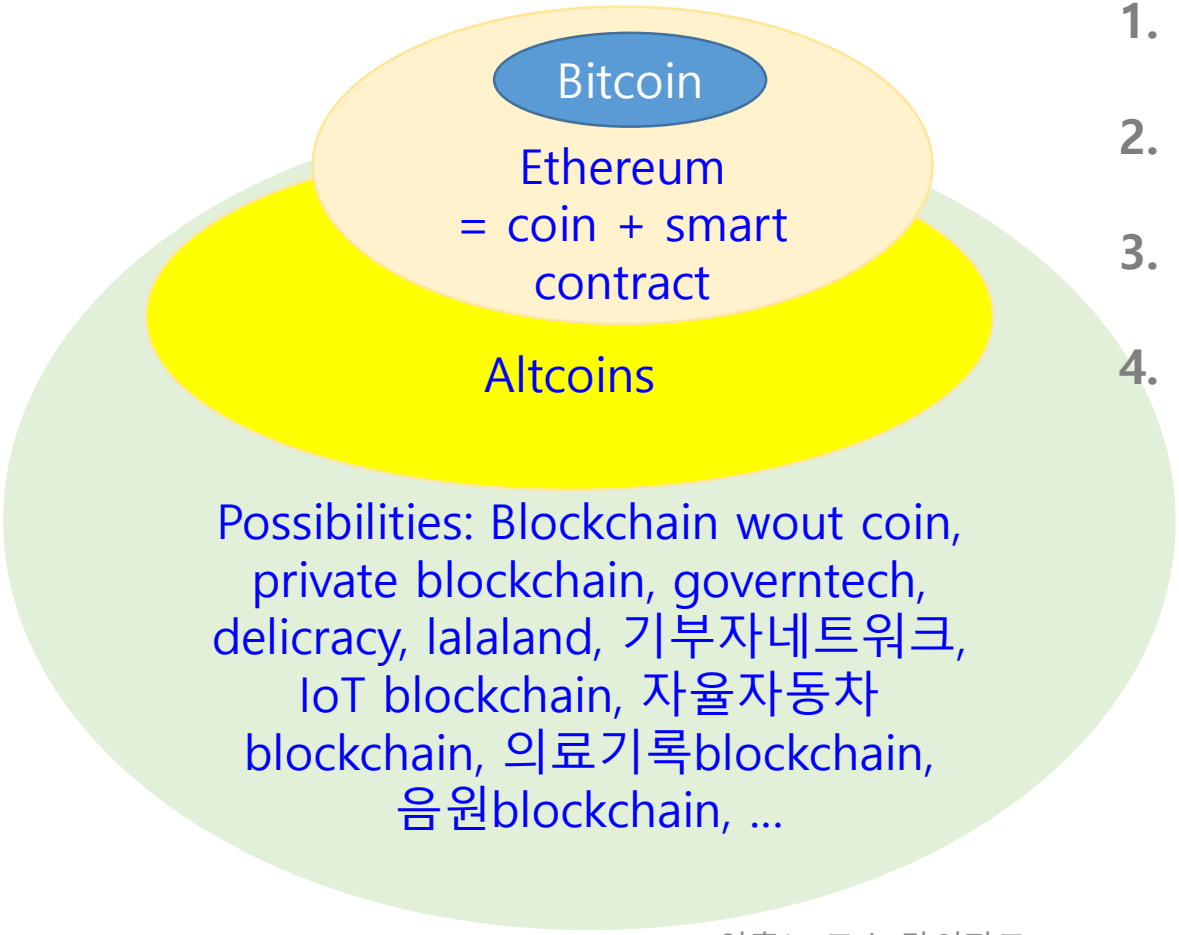
- 거래속도 다양화
  - 10min per block, 1min/block, 40초/block, …
- 채굴방식의 다양화
  - Proof-of-work, Proof-of-Stake, Proof-of-activity, …
- 블록체인 다변화
  - Bitcoin기반, Ethereum기반


Top 10 Cryptocurrencies by Market Capitalization (Total: $537 Billion)
BusinessHut.com
Bitcoin Gold, 1%
NEM, 1%
Cardano, 1%
Dash, 1%
IOTA, 2%
Litecoin, 3%
All Others, 12%
Bitcoin Cash, 6%
Ripple, 6%
Ethereum, 12%
Bitcoin, 56%

WEF 암호화폐 전망

- 1980 PC Windows
- 1995 Internet, Explorer
- 2005 Mobile, Android iOS
- 2015 WEF 5월 보고서 예측, “27’ 전세계 GDP 10% 암호화폐로 보관”, “23’ 국가가 세금을 암호화폐로 징수 시작”
- 2016 다보스포럼, 빅데이터와 블록체인이 승자
- Korea GDP 1,400B.USD 2015에서 1,800B 2027 전망
- World GDP 80,000B 2015에서 100,000B 2027 전망
- Cryptocurrency, 10B 2015, 10,000B 2027 전망
  (0.01% → 10%, 천배 성장)

Hypes vs Revolutionary ideas



Questions to ask

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

Initial Coin Offering

- ICO는 블록체인기업이 신규 암호화폐를 발행해 자금을 모으는 것을 의미.
- 기업이 자금을 유치하기 위해 기업공개(IPO)를 하는 것과 비슷.

ICO 유형

- 투자금 유치를 위해 블록체인기업은 백서를 쓴다.
- 블록체인과 암호화폐를 활용하여 어떤 새로운 제품과 서비스를 만들 것인지 밝힌다.
- 블록체인의 무결성과 시스템의 안정적 운용을 담보하기 위해서는 개발자와 관리자, 사용자 네트워크를 폭넓게 확보해야 한다.
- 시스템을 빠르게 구축하기 위한 인센티브 제공을 위하여 암호화폐를 발행한다.
- 신규 암호화폐가 거래소에 상장 될 때,
- 개발된 서비스가 폭넓게 사용 될 때,
- 발행한 암호화폐에 대한 교환가치가 상승한다.
- 이때 관리자, 사용자, 투자자들 모두가 투자했던 노력과 자금에 대한 보상을 받는다.

인간 상호 작용과 교류범위 확대 via token/coin 발행과 Incentivising!

문제는 이 혁신기술이 어떻게 세상을 더 이롭게 할 수 있을 것인지를 찾는 것입니다.

블록체인은 4차 산업시대에 정치, 경제, 사회, 문화 등 모든 영역에서 근본적인 변화를 이끌 것으로 기대 받고 있습니다.

4차 산업시대는 인터넷 속 가상세계가 현실세계와 일치하게 되는 시대입니다. 블록체인은 가상세계 속 거래를 현실 거래가 되도록 합니다.

블록체인은 핸드폰을 가진 개인은 누구나, 정치, 경제, 사회 등 인간의 주요 활동영역에서, 타인과 신뢰에 기반 한 상호작용을 원활하게 할 수 있도록 만들어 줍니다. 우리는 구성원 간 공정거래 및 계약이행을 위하여 사법시스템과 공권력을 만들고 운영하는 데 많은 사회적 인프라 비용을 지출합니다.

블록체인은 이러한 사회적 비용을 크게 낮추고, 개인 간 직거래와 상호작용을 크게 촉진 할 것으로 기대 받고 있습니다.

연결하는 것이 창의성입니다.

신뢰에 기반 한 인간 상호작용과 교류범위의 확대는, 사회 구성원 간 갈등은 낮추고, 생산성을 크게 높여줄 것입니다.

과학기술이 신뢰사회를 추동 하는 것입니다.

블록체인 기반 신뢰사회 구축!

세계최초 연예인 블록체인 탄생.
기부자 블록체인, 음원협회블록체인 등 계속해서 나올 듯 합니다.

저는 학회임원회의 때 앉아서 학회블록체인을 상상해 보았었습니다. 대한전자공학회 임원회의에 참석했었지요. 회원 수 감소, 신입생 감소 등 고민이 깊었습니다. 어떻게 학회를 다시 활성화 할 수 있을까요.

학회 운영진은 심각하게 고민합니다. 학회 발전을 위해 온갖 아이디어를 짜내고 노력하는데, 잘 안 됩니다. 기본적으로, 회원과의 거리를 좁히기 어렵습니다. 운영진의 새로운 시도는 대게는 회원들에게 잘 전달되지 못 합니다. 소통의 간극이 큽니다. 학회 발전에는 회원 구성원의 적극적인 참여가 필수적입니다. 그런데, 문제는 대다수 회원들의 입장에서는 운영진의 노력은 보이지 않습니다. 우선, 학회운영진이 매년 바뀝니다. 회원들은 리더들이 무엇을 하려고 하는지 모릅니다. 모르니 관심을 갖기 어렵습니다.

이런 상황에서, 학회가 코인을 발행하고, 회원들에게 회원활동의 보상으로 코인을 지급하면 어떻게 될까 생각해 보았던 것 입니다.

학회 발전에는 회원의 적극적인 참여가 필수적입니다. 가장 간단한 학회참석에서 시작해서, 논문 투고, 논문 심사, 세미나 강사, 심혈을 기울인 발표 등 끝이 없지요. 서로가 신경써서 이런 활동을 잘 하면 모임이 즐거워지고, 학문이 크게 발전하고, 학회도 따라 융성한다는 것은 모두가 압니다. 얻는 실익이 많으면, 참여자는 더 적극적이 되고, 참여자가 수가 증가하는 등 상승 작용이 일어난다는 것도 압니다. 그러나 이런 기본적인게 잘 안 됩니다.

이와 같은 상호작용을 일으키기 위해서, 적극적 회원활동에 대한 즉각적 보상으로, 코인을 지급해 보자는 게 제 아이디어 입이다.

논문 심사료, 강연료도 코인으로 주고, 학회장 질서유지 및 안내자 수고도 코인으로 보상해 줍니다. 블록체인유지를 위해 서버를 사용하게 해 주는 교수연구실에게도 코인을 지급합니다. 나중에는 학회 등록비도 코인으로 낼수 있고 학회에서 발표를 잘 한 학생에게 코인을 쏴 줄 수 있게도 해 줍니다. 적극적인 학회 활동을 돈 안드는 코인을 발행해서 지급하는 것 입니다. 점차로 더 많은 회원들에게 코인이 지급되고, 회원들이 적극적 참여로 코인 주고 받기를 잘 하면, 학회 활동이 촉진될 것 입니다. 어느덧 코인 사용자가 많아지게 되겠지요. 더 많은 회원이 학회활동에 적극적이 되고 서로 긍정적 영향을 주고 받게 됩니다.

학회는 내실을 갖게 됩니다. 수많은 회원이 사용하므로 학회가 발행해 쓰는 코인에도 변화가 일어납니다. 시장가치가 생겨나는 것이지요. 왕성하게 활동한 회원들은 금전적인 가치도 보상으로 받게 되는 것 입니다.

국내 암호화폐 규제현황

- 하태경 의원, 정부의 암호화폐 규제 정책 비판, 해운대에 '크립토 밸리' 조성 계획 밝혀,
- 고려대 김형중 교수, "암호화폐는 하늘이 文 정부에 준 큰 선물",
- 오정근 한국금융ICT융합학회장, "우리나라도 서둘러 ICO 특구를 지정해야 한다"
- 4월 30일 국회에서 있었던 "한국 크립토밸리 조성필요성과 조성 방안"
- 토론회 후 검색되는 기사들의 내용입니다.

- 국내에서는 작년 9월 암호화폐 거래 과열과 사기성 ICO를 이유로 정부가 전면 금지 조치를 내린 상태입니다.
- 청와대는 2월 14일 '암호화폐 규제 반대' 청원에 대한 답변에서

"가상통화 거래 불법행위와 불투명성은 막고, 블록체인 기술은 적극 육성해 나간다는 게 정부의 기본 방침이다"라고 밝혔습니다.

국내 암호화폐 규제현황

- 암호화폐는 규제하고, 블록체인은 장려한다는데, 과연 그게 무슨 말인가?
- 선뜻 이해가 안 가서, 연구를 좀 해 보았습니다.

- '암호화폐가 없는 블록체인'은 사실 쟁점이 아닙니다.
- 만약 누군가 암호화폐 발행 없이 혁신적인 블록체인사업아이이더를 제시한다면,
- 그건 그냥 진행해보게 놔두면 됩니다.
- 그런 게 성공할 수 있을지 의문입니다만 막을 이유는 없습니다.

- 문제는 신규 암호화폐 발행이 포함된 블록체인 사업입니다.
- Bitcoin이 만들어낸 혁신 때문에, 그런데서 성공하는 BM이 나오기 쉽기 때문입니다.
- 그러나 바로 그 신규 암호화폐 발행부분 때문에 적절한 규제가 필요한 것이기도 하지요.
- 먼저 문호를 개방하여 ICO가 성행하고 있는 나라를 살펴보았습니다.

- Singapore, 스위스, 캐이난아일랜즈 등이 삼대 성지로 나타납니다.
- 다 도시 수준 국가 입니다, "조세회피처"라는 단어도 생각납니다.
- 미국, 영국, 프랑스, 중국, 일본 등은 뭘 하고 있지?
- 의문이 들었고, 찾아보았습니다만 어느 나라에서도 ICO가 성행하고 있지 않습니다.

금융강국 미국의 규제현황

- Jay Clayton 증권거래위원회 의장이 쓴 공개서한을 찾을 수 있었습니다.

- Clayton은 현재 진행되고 있는 ICO를 다음과 같은 시선으로 바라보고 있습니다.
  - 투자금 유치를 위해 블록체인기업은 백서를 쓴다.
  - 블록체인과 암호화폐를 활용하여 어떤 새로운 제품과 서비스를 만들 것인지 밝힌다.
  - 블록체인의 무결성과 시스템의 안정적 운용을 담보하기 위해서는
  - 개발자와 관리자, 사용자 네트워크를 폭넓게 확보해야 한다.
  - 시스템을 빠르게 구축하기 위한 인센티브 제공을 위하여 암호화폐를 발행한다.
  - 신규 암호화폐가 거래소에 상장 될 때,
  - 개발된 서비스가 폭넓게 사용 될 때,
  - 발행한 암호화폐에 대한 교환가치가 상승한다.
  - 이때 관리자, 사용자, 투자자들 모두가 투자했던 노력과 자금에 대한 보상을 받는다.

- 이런류의 신규**코인이 바로 증권**이라고 Clayton은 선언합니다.
- 투자금 모집을 위해 발행하는 코인이 바로 증권이라는 것이다.
- 코인이 증권이 되면 기업의 입장에서는 매우 난감해집니다.
- 오랜 전통을 가진 증권법을 따라야하기 때문입니다.

금융강국 미국의 규제현황

- 증권법의 기본 개념은 투자자 보호, 거래질서유지, 시장 투명성 확보 입니다. 즉 증권을 판매하고자 하는 기업과 거래소는 까다로운 기업공개절차를 밟아야 합니다.
- 재정상태, 기술팀의 이력, 다년간의 회계기록 등과 같은 중요한 사항을 낱낱이 공개해야 합니다.
- 듣고 보니 참 당연한 얘기입니다.

- 잘 알고 투자할 수 있도록 기업에 관한 중요 정보를
- 공개하도록 하는 게 기본 아니겠습니까?

- 이렇다 보니, 현재 미국에서 ICO를 진행하고자 하는 기업은 많지 않습니다.

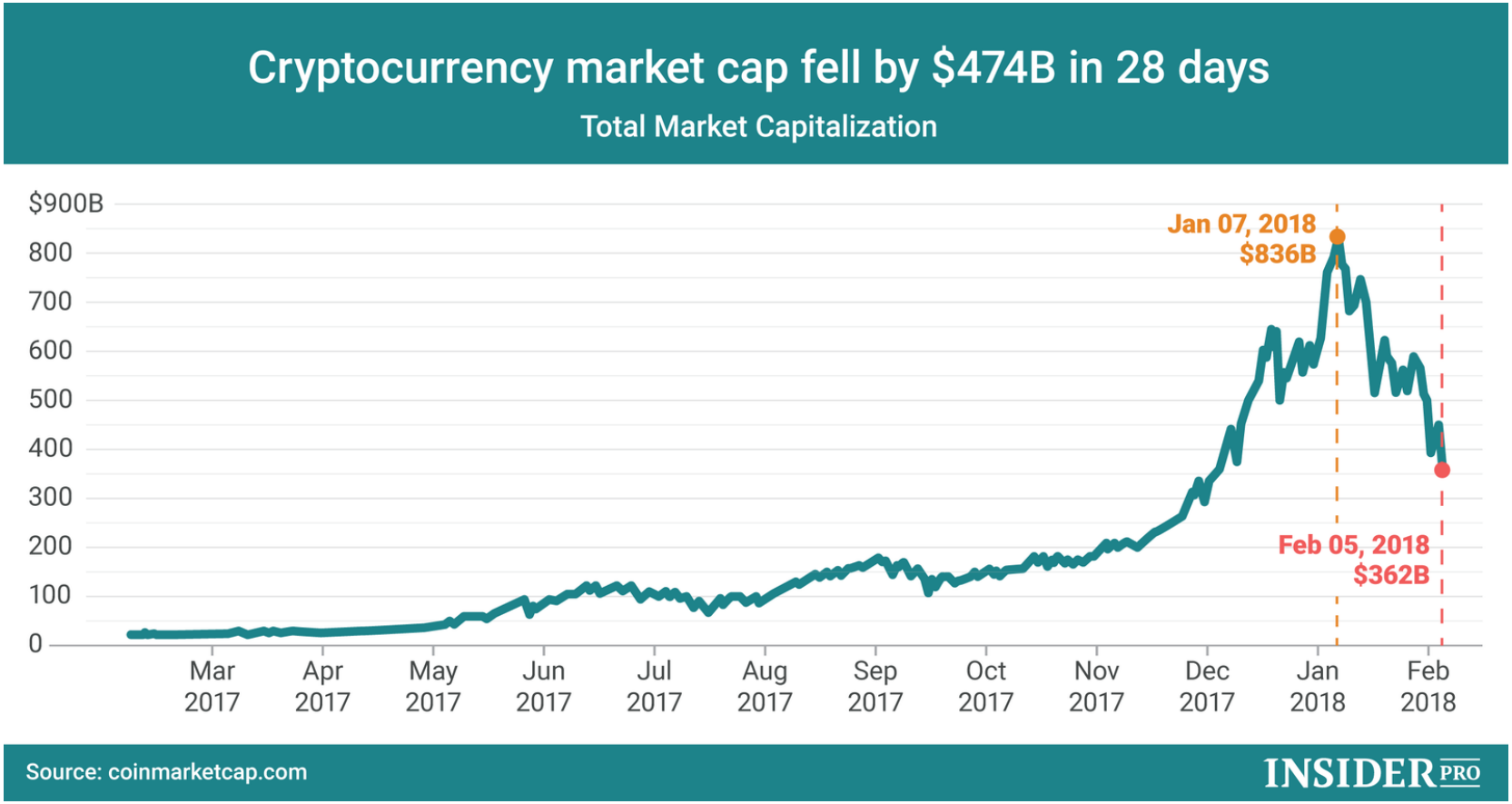
- 미국의 증권법 적용을 두려워한 나머지, ICO 기업이 스스로 미국인들의 참여를 막아놓는 것입니다.

규제 샌드박스

- 우리나라도 미국 수준의 규제를 적용해야 할까요?

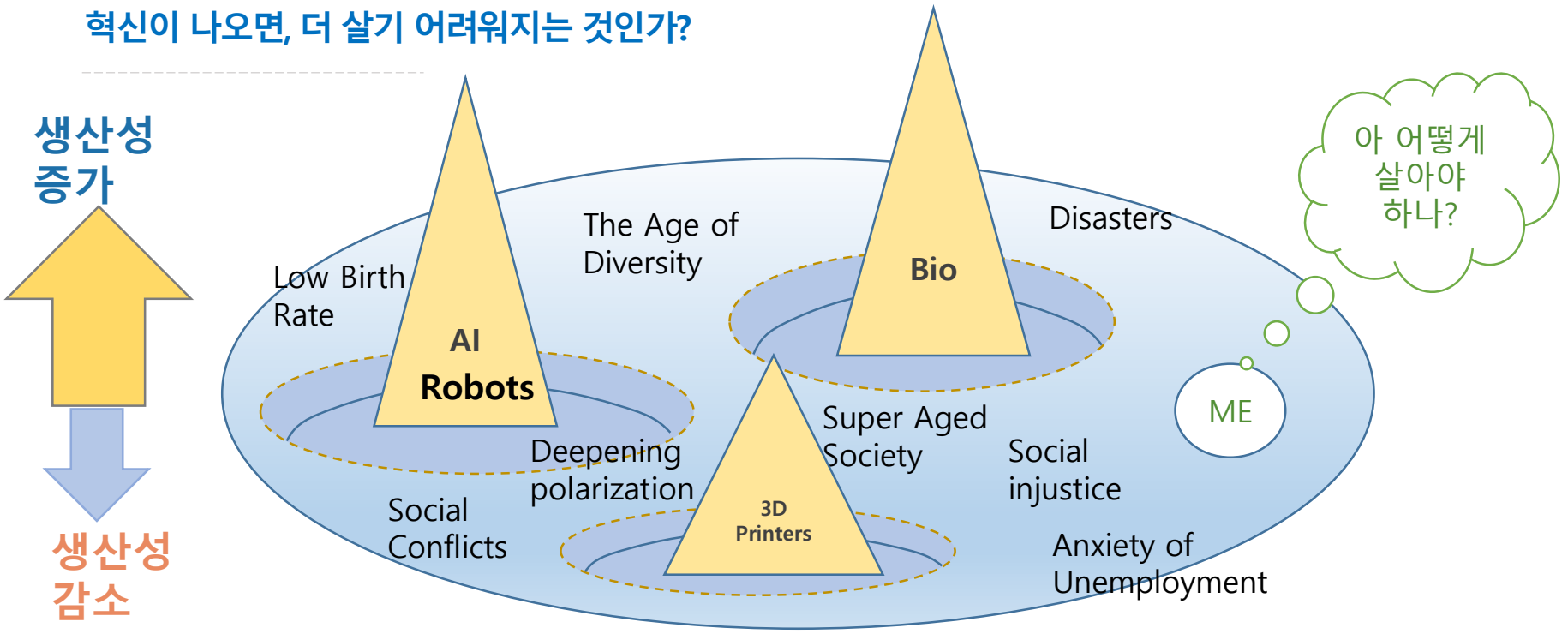
- 저는 블록체인 산업의 진흥을 위해 규제샌드박스를 적용해 보는 게 어떤가 생각합니다.
- 우선 제한적으로 곳곳에 있는 첨단산업특구에 먼저 적용해 보는 것은 어떨까요?

정점 이전과 이후


Cryptocurrency market cap fell by $474B in 28 days
Total Market Capitalization
$900B
800
700
600
500
400
300
200
100
0
Jan 07, 2018
$836B
Feb 05, 2018
$362B
Mar 2017
Apr 2017
May 2017
Jun 2017
Jul 2017
Aug 2017
Sep 2017
Oct 2017
Nov 2017
Dec 2017
Jan 2018
Feb 2018
Source: coinmarketcap.com
INSIDER PRO

파괴적 혁신의 문제~ W.T.A., 소득양극화, 일자리 소멸, 인구절벽

혁신이 나오면, 더 살기 어려워지는 것인가?



소수혁신가에겐 대박, 대중은 이득, 직장잃은자에게는 파멸!

블록체인에 개개인의 지재권(특허, 카피라잇, 성실한 업무 수행 등)과 평상 업무 시 노력의 증거물을 남길 수 있지 않을까?
암호화폐가 수평적 소통과, 나누고 협력하는 집단을 촉진할 수 있지 않을 까?

미래 변화 선도 혁신성장 전략

- **혁신성장**
  - 기업가 정신, 대학의 개방 통한 창업타운 구축, 혁신 기술 기반 창업, 유니콘 기업 배출
- **포용적 분배**
  - 사회안정망, 패인골 매우기, 일자리나누기
- 행복하고, 활기찬, 창의 혁신 국가로 도약!

Conclusion

- 블록체인 응용 무궁무진
- 새로운 사회/경제 시스템의 탄생
  - 분권, Decentralization (탈중앙화) 조직
  - Unbundling 큰 조직 분해해 나누기(같이 먹고 살자)
  - Incentivising 에 의한 노력과 투자에 대한 보상으로 대규모 협력 가능
  - Initial coin offering에 의한 startup fund raising
- 정치/경제/사회/문화/스포츠/물류/유통 모든 영역으로 확장중
  - 메디블록, 디지털거버넌스, 운동블록체인
  - 부동산거래, 토지거래, 무역, 보험
- 규제 와 투자자 보호
  - 규제 Sandbox 도입 필요