Blockchain and Its Applications

이흥노 교수

한국은행 광주전남본부 강의

2018. 2. 20

강의자료

- 파일을 변형 없이 그대로 배포해도 좋습니다.
  - 배포 시 저에게 문자 주시면 고맙겠습니다.

- 내용을 인용할 때에는

  이흥노, "Blockchain and its Application," 한국은행광주전남본부 초청 강의 자료, 2018년 2월 20일.

  를 Reference에 넣고 Acknowledge 해 주십시오.

- GIST는 영어로 강의 합니다.
- 영어를 많이 사용하고 있는 점 양해 바랍니다.

강의 방향

- 4차 산업시대 mega trends
  - 공유경제, Unbundling of Centralized Authorities, 분권, Decentralized
  - Zero-marginal cost society, 소량 맞춤 형 생산, Prosumers 시대

- But we have to be discriminating!
  - A lot of hypes are out there as well!
  - Note unproven or immature ideas!

- Bitcoin에 기반한 블록체인
- Ethereum에 기반한 smart contracts
- 그 외 새로운 움직임 동향파악

Blockchain Technology and Cryptoeconomic Policy

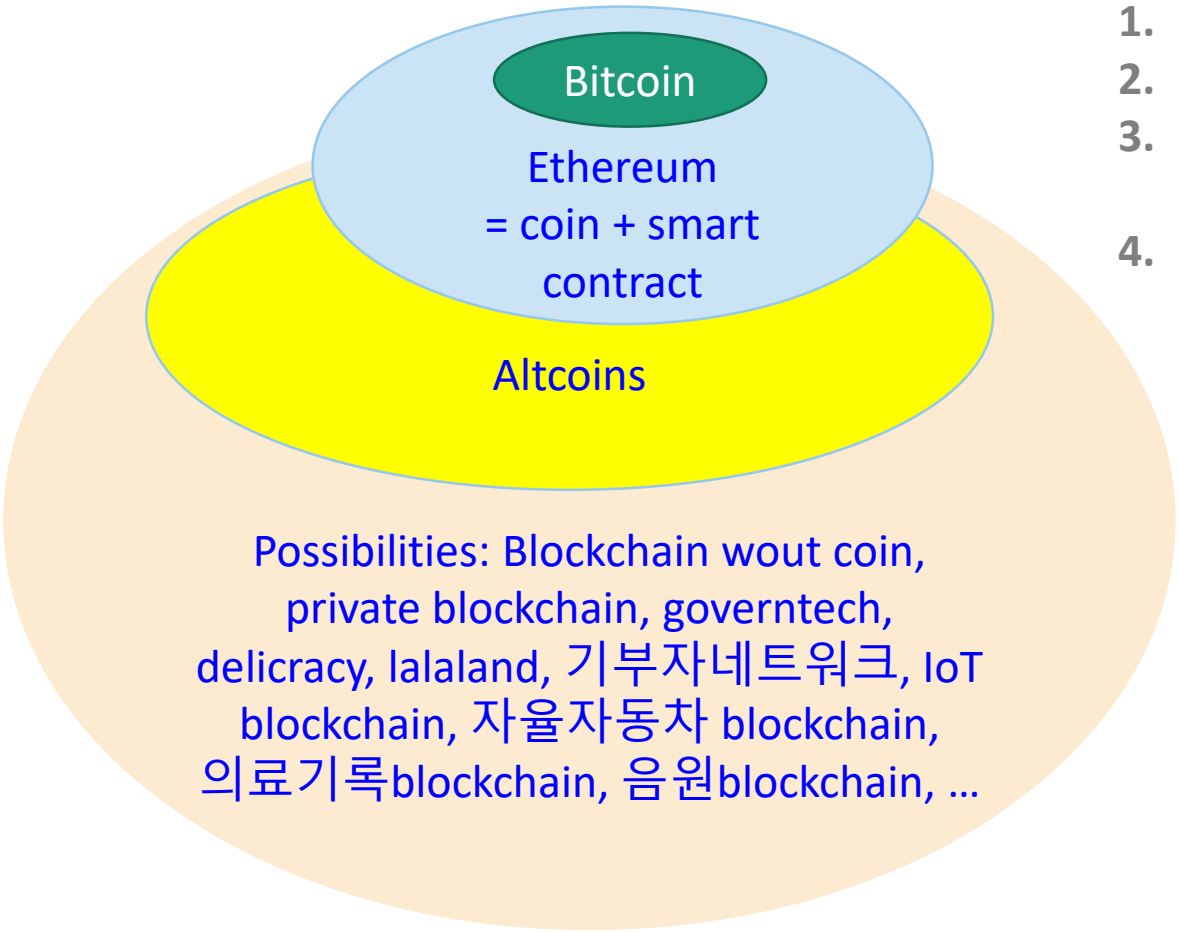
- Abstract -- Bitcoin is a peer-to-peer electronic cash transfer system without a bank in the middle. The e-cash can be sent to anyone in the internet as if it was an in-person transfer of money. To meet such an end, Bitcoin introduces a novel idea, blockchain. Blockchain maintains a group of “cryptographically chained” digital documents, a ledger. Cryptographic chain is required to record in an unforgeable way transactions such as coin transfers from one to the other. The ledger is published and left open in the internet. The open chained ledger makes electronic transfer of money possible over the internet without the authority in the middle. Since 2009 Bitcoin was introduced, it has made tremendous strides. Market value has been created, capitalization surpassing more than 20 Billion USD in 2017. Thousands of follow-up systems have been created. World Economic Forum has forecasted that 10% of global GDP will be stored in blockchains by 2025. In this tutorial, we aim to review Bitcoin and Ethereum for their program architectures and operations. Ethereum is believed to have made the e-cash system to the next level by inclusion of “smart contracts” in its function. Smart contracts enable formation of contractual relations between two or more parties and the terms specified in the contract are executed automatically when prescribed conditions are met. In this tutorial, we also aim to shed light on technical sides of blockchain technology such as privacy, security and autonomy which are sensitive to regulations and policies. Many initial coin offerings has been made amassing a large amount of crowd funding. While it is a revolutionary invention, blockchain and cryptocurrency systems are at its infancy stage. In order to foster continued healthy development, it is imperative for us to see the core of the technology and be able to evaluate the short and long term impacts of this technology based on scientific facts. This shall help us avoid any unwanted act of fear and road blocks to development. Regulations should be kept at its minimal. There are obvious ones: price manipulation practices and fraudulent investment operations should be prevented and punished heavily when caught. But more importance should be developing a policy to fostering researches, startups and funding to help uncover new opportunities. Blockchain can be useful in many future applications such as transfer of lands and houses, bank accounts to people in underdeveloped nations, and low cost maintenance of valuable records such as patents and copyrights. If some of them are indeed realizable, blockchain is sure to make the society clearer and more expectable. Protection of rights for underprivileged people can be improved; disputes and conflicts in the society lessened; transaction costs reduced and healthy interaction among people encouraged. Who knows that it shall lead us a step closer to the society of genuine trust!

My priority we shall spend time on

Let us set priority in the following order

1. Market proven ideas
2. Good ideas proven by investment funding : ICOs, VC funding start ups
3. Published scientific papers
4. Official decisions, court orders
5. Advisory notes by visionary figures
6. New articles

Hypes vs Revolutionary ideas

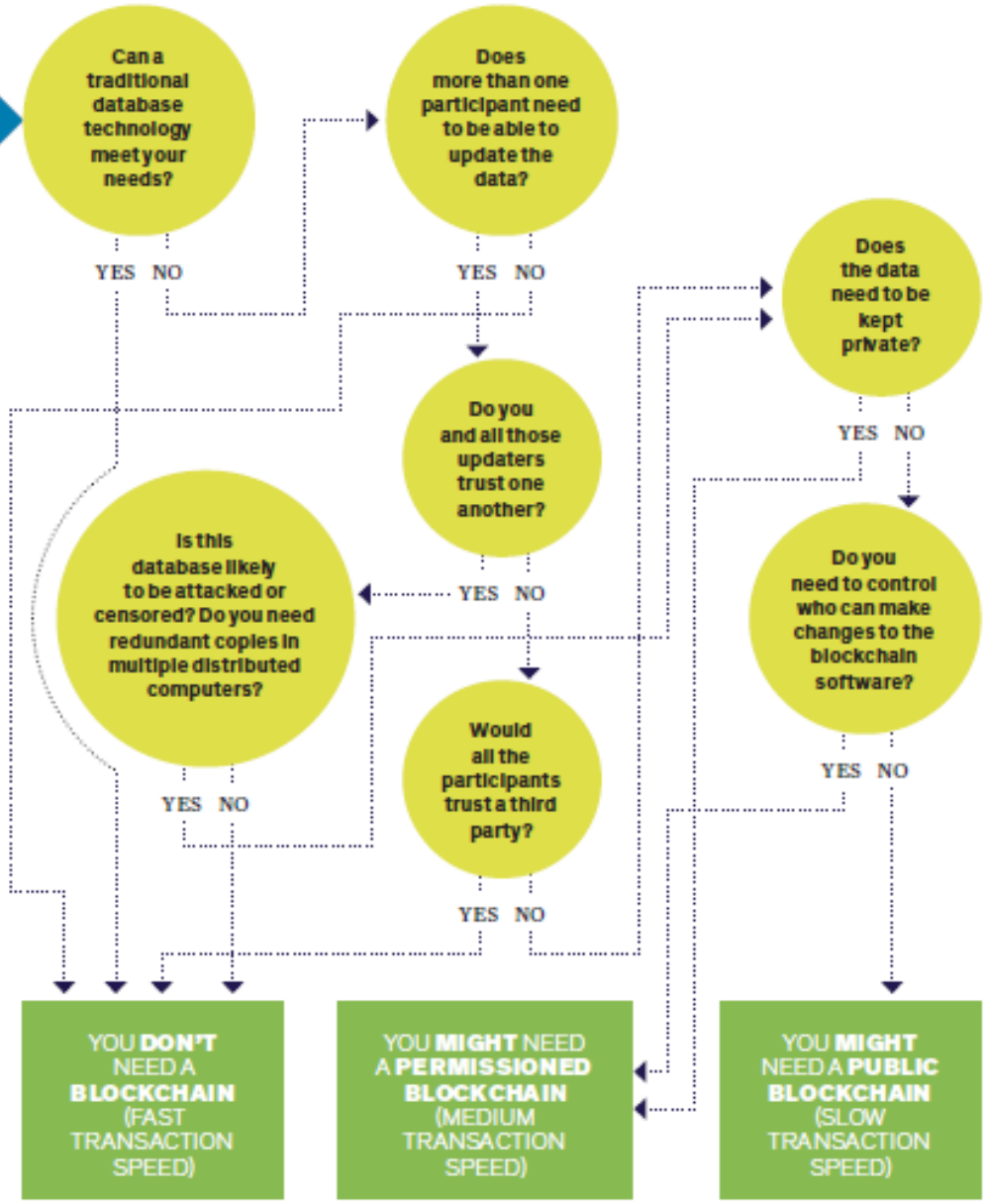


Questions to ask

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?**

I Want a Block-chain!

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



Many Different Types of Blockchains						
Principle	**Bitcoin**	**Ethereum**	**Stellar**	**IPFS**	**Blockstack**	**Hashgraph**
Confidentiality	None	None	None	Hash-based content addresses	None	None
Information availability	Block mirroring	Block mirroring	Ledger mirroring	Graph and file mirroring	Block mirroring/ DHT mirroring	Hashgraph/ mirroring; Optional Event History
Integrity	Multiple block verifications	Multiple block verifications	Latest block verification	Hash-based content addressing	Multiple block verifications	Consensus with probability one
Non repudiation	Digital signatures	Digital signatures	Digital signatures	Digital signatures	Digital signatures	Digital signatures
Provenance	Transaction inputs/outputs	Ethereum state machine and transition functions	Digitaly signed ledger transition instructions	Digital signatures and versioning	Transaction inputs & outputs and virtual chain references	Hashgraph/ mirroring; Optional Event History
Pseudonymity	Public keys	Public keys and contract addresses	Public keys	Public keys	Public keys, but public information encouraged	Not supported; could be layered
Selective disclosure	None	None	None	None	Selective access to encrypted storage	Not supported; could be layered

FIGURE 1. Blockchain information security principle analysis.

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-win 하는 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.

- MyBit is solving by connecting those interested in implementing solar projects with investors who are willing to fund such revenue generating assets.

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

Unbundling of Big Companies

- Fortune지. “SNR, Big data, IoT, AI로 무장한 벤처의 전통 대기업 모델 분해, Unbundling, 탈 중앙화, Decentralization”
- Unbundling Media, European Bank, Honeywell, FedEx …
- 1차 기계생산, 2차 전기_컨베이어벨트 분업, 3차 자동화
- 4차 산업은 Cyber-Physical System과 맞춤형 생산, Decentralized Autonomous Organization(DAO)
- Disruptive unbundling, Dis-intermediation, Decentralized Autonomous Networked Organization(DANO), DANSociety

Unbundling

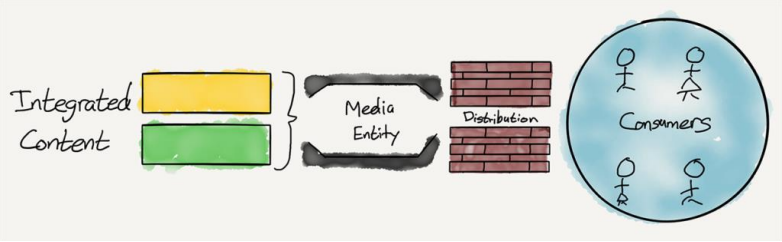
From Wikipedia, the free encyclopedia

- **Unbundling** is a neologism to describe how the ubiquity of mobile devices, Internet connectivity, consumer webtechnologies, social media and information access[1] in the 21st century is affecting older institutions (education, broadcasting, newspapers, games, shopping, etc.) by "break[ing] up the packages they once offered (possibly even for free),[2] providing particular parts of them at a scale and cost unmatchable by the old order."[3] Unbundling has been called "the great disruptor".[4]

The Great Unbundling

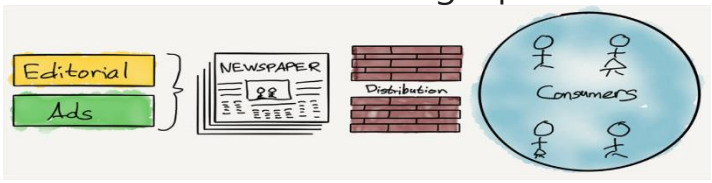
Ben Thompson

- https://stratechery.com/2017/the-great-unbundling/

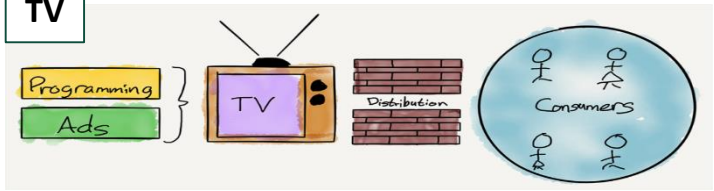


THE OLD MEDIA MODEL
Nearly all media in the pre-Internet era functioned under the same general model:
Note that there are two parts in this model when it comes to making money — distribution and then integration — and the order matters. Distribution required massive up-front investment, whether that be printing presses, radio airplay and physical media, or broadcast licenses and cable wires; the payoff was that those that owned distribution could create money-making integrations:

Print: Newspapers and magazines primarily made money by integrating editorial and advertisements into a single publication:



TV



Music

The Economics of Bundling
Chris Dixon

- What price should the cable company charge to maximize revenues?
- Suppose price set at 10% lower than W2P.
- Company revenue
  - $18 non-bundle
  - $23.40 bundle, charging each customer $11.70 (10%off $13)
- Consumers save
  - $2 non-bundle vs. $2.60 bundle.
- Both buyers and sellers benefit from bundling.

Cable TV buyers' willingness-to-pay

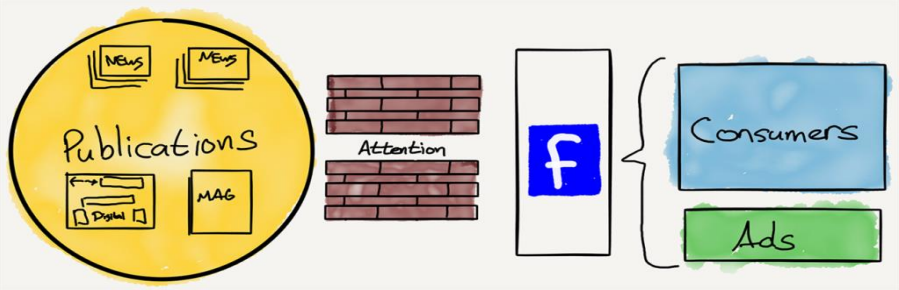
	ESPN	History channel
Sports lover	$10	$3
History lover	$3	$10

Lesson: if customers like more than one thing, then both content creators and customers gain from a bundle

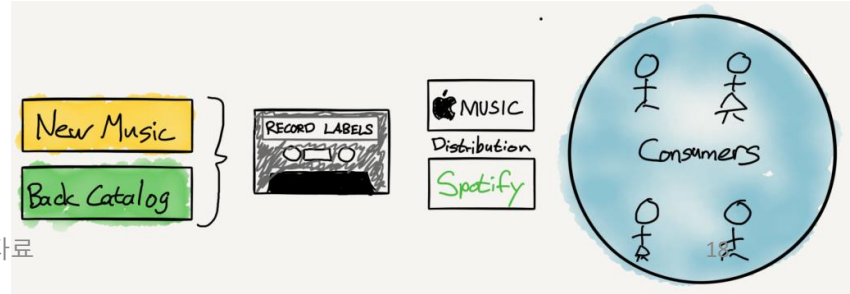
What happens, when distribution cost goes zero…

- The most obvious casualty has been text-based publications, and the reason should be clear: once newspapers and magazines lost their distribution-based monopoly on customer attention **the integration of editorial and advertising fell apart**. Advertisers could go directly to end users, first via ad networks and increasingly via Google and Facebook exclusively, while end users could avail themselves of any publication on the planet.

Print integration of editorial and ads fell apart!



Music: Streaming (bundling) services popular



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)

Crypto currency market capitalization

March 2017

- Bitcoin 20B USD
- Ethereum 3B
- Dash 0.66B
- Monero 0.31B
- Ripple 0.24B
- Litecoin 0.21B
- Ethereum Classic 0.18B
- Augur 0.10B

현금 없는 사회와 블록체인

- 스웨덴 (대중교통 요금 현금 결제 제한), 덴마크(의류판매 식당 등 소매업체 현금 수납 거부 가능 법안 발의), 이스라엘(현금없는 사회 추진위 설립), 중국(인민은행, 디지털화폐 발행 추진 중), 한국 (20’ 목표, 동전없는 사회 추진 중)

- “독일, 영국에 이어 일본도 암호화폐를 화폐로 인정” 신문보도 인용 하며, 일본정부가 암호화폐를 공적 결제수단으로 이용할 수 있도록 하는 법 규제안 각의 결정.

Bitcoin이 뭔가요?

The first paper

Bitcoin: A Peer-to-Peer Electronic Cash System

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

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

Satoshi Nakamoto

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

Bitcoin

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 신뢰하는 것입니다.**
- **갖고 있으면 언제든지 필요한 서비스 및 제품을 제공 받을 수 있다는 신뢰에 기반합니다.**

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.

Brief history on bitcoin markets

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

~2010 : M. value created, Pizza Day

- **October 2009**
- Bitcoin receives an equivalent value in traditional currencies. The New Liberty Standard established the value of a Bitcoin at $1 = 1,309 BTC. The equation was derived so as to include the cost of electricity to run the computer that created the Bitcoins in the first place.
- **February 2010**
- The world's first Bitcoin market is established by the now defunct dwdollar.
- **May 2010**
- A programmer living in Florida named Laslo Hanyecz sends 10,000BTC to a volunteer in England, who spent about $25 to order Hanyecz a pizza from Papa John's. Today that pizza is valued at £1,961,034 and stands as a major milestone in Bitcoin's history.
- **November 2010**
- Bitcoin reaches $1 million. Based on the number of Bitcoins in circulation at the time, the valuation leads to a surge in Bitcoin value to $0.50/BTC.

2013: Regulation started, “Bitcoin is money”

- **February 2011**
- Bitcoin reaches parity with the US dollar for the first time. By June each Bitcoin is worth $31 giving the currency a market cap of $206 million.
- **March 2013**
- The US Financial Crimes Enforcement Network (FINCEN) issues some of the world’s first bitcoin regulation in the form of a guidance report for persons administering, exchanging or using virtual currency. This marked the beginning of an ongoing debate on how best to regulate bitcoin.
- **March 2013**
- Bitcoin market capitalisation reaches $1bn.
- **August 2013**
- Federal Judge Mazzant claims: “It is clear that Bitcoin can be used as money” and “It can be used to purchase goods or services” in a case against Trendon Shavers, the so-called ‘Bernie Madoff of bitcoin’. Bloomberg begins testing bitcoin data on its terminal. Although alternative tickers exist, endorsement from Bloomberg gives bitcoin more institutional legitimacy.
- **December 2013**
- China’s central bank bars financial institutions from handling bitcoin transactions. This ban was issued after the People’s Bank of China said bitcoin is not a currency with “real meaning” and does not have the same legal status as fiat currency. The ban reflects the risk bitcoin poses to China’s capital controls and financial stability. Today China remains the world’s biggest bitcoin trader, with 80% of global bitcoin transactions being processed in China.

2014 : Taxation, Regulations, Funds

- **January 2014**
- Bitcoin custodians Elliptic launch the world's first insured bitcoin storage service for institutional clients. All deposits are comprehensively insured by a Fortune 100 insurer and held in full reserve. This means Elliptic never re-invests client assets; instead they secure them in deep cold storage. Overstock.com becomes the first major online retailer to embrace bitcoin, accepting payments in the US. Overstock was the first in what is now an expeditiously growing list of large businesses that accept bitcoin.
- **February 2014**
- HMRC classifies bitcoin as assets or private money, meaning that no VAT will be charged on the mining or exchange of bitcoin. This is important as it is the world's first and most progressive treatment of bitcoin, positioning the UK government as the most forward thinking and comprehensive with regard to bitcoin taxation.
- **July 2014**
- The 'Bit Licence' edges towards reality as the New York State Department of Financial Services releases the first draft of the agency's proposed rules for regulating virtual currencies. The European Banking Authority publishes its opinion on 'virtual currencies'. Their analytical report recommends that EU legislators consider declaring virtual currency exchanges as 'obliged entities' must comply with anti-money laundering (AML) and counter-terrorist financing requirements.
- The EBA report is important as it acts as a catalyst to launch bitcoin into the financial mainstream by highlighting the fact that virtual currencies require a regulatory approach to strive for an international coordination to achieve a successful regulatory regime.
- Also that month GABI (Global Advisors Bitcoin Investment Fund) launches the world's first regulated Bitcoin Investment fund. This is important to the bitcoin ecosystem as the launch of this investment vehicle adds further legitimacy to bitcoin in addition to allowing regulated investors a way to invest in bitcoin.

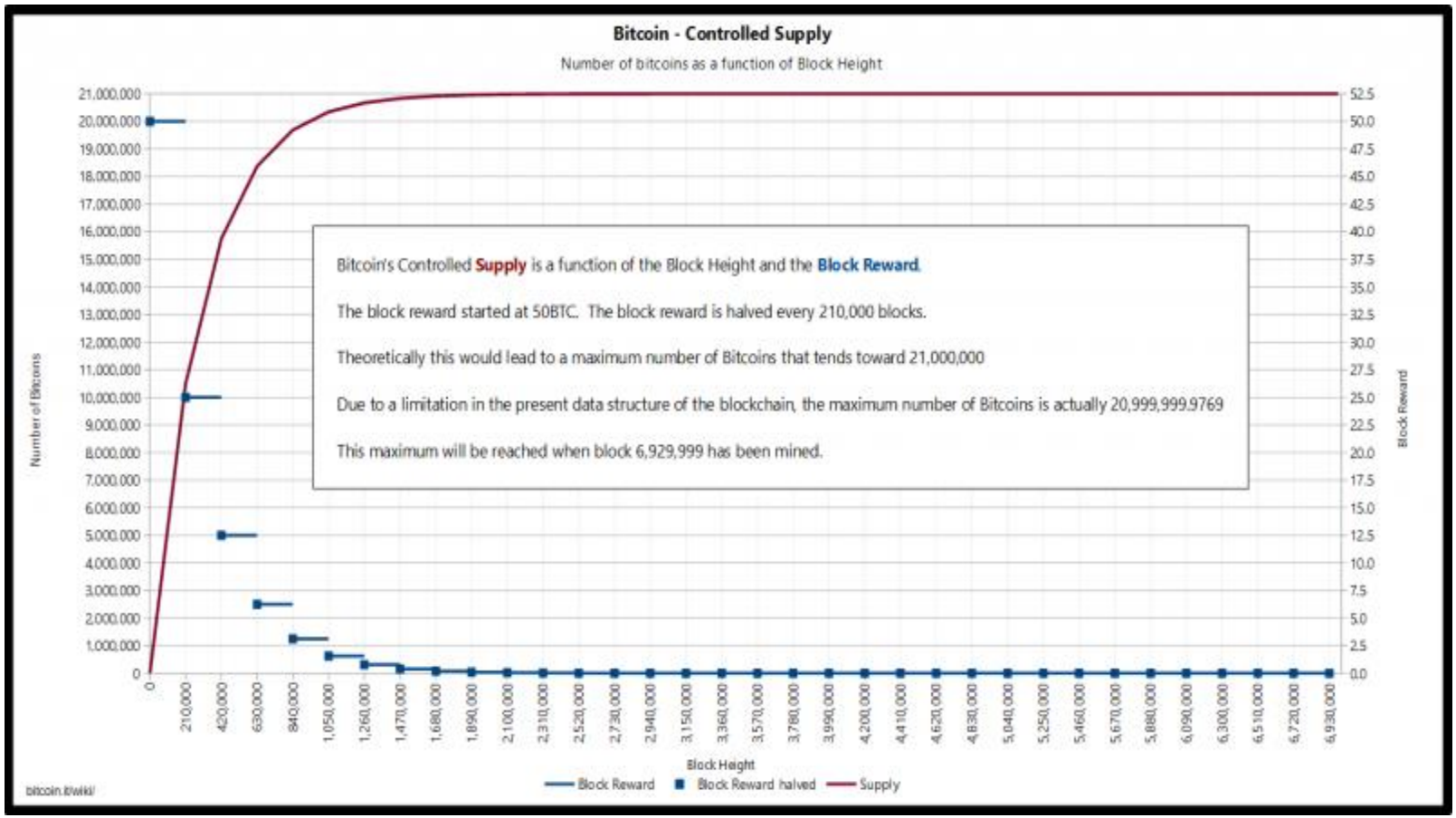
2015: Derivatives, Assets, Payments

- **August 2014**
- The Chancellor of the Exchequer, George Osborne, demonstrates his and HM Treasury's positive outlook on bitcoin when he purchases £20 worth of bitcoin and announces HM Treasury's Call for Information on digital currencies, offering digital currency businesses the chance to comment on the risks and benefits and potentially influence future government policy.
- **October 2014**
- TeraExchange announces that the first bitcoin derivative transaction was executed on a regulated exchange, adding a new hedging instrument to bitcoin and instilling credibility and institutional confidence in the entire bitcoin community.
- **December 2014**
- Tech giant Microsoft begins accepting bitcoin payments.
- **January 2015**
- The New York Stock Exchange is a minority investor in Coinbase's $75M funding round. The NYSE aims to tap into the new asset class by bringing transparency, security and confidence to bitcoin.
- **March 2015**
- The results of the UK Treasury's call for information on digital currency are announced.

Future predictions

- There are several possible ways Bitcoin can go at this point, all of which point to a legitimate, widespread adoption by large institutions through tighter regulation. Recently, New York's BitLicense became the world's first digital currency-specific regulatory regime. It has been through a couple of rounds of consultations and is expected to come into force in a couple of weeks.
- The European Central Bank and European Banking authority have both released detailed reports on digital currencies, and suggested regulation of the industry by the EU to further control price fluctuations. The Winklevoss brothers, they of Facebook fame, are on the verge of launching their own exchange-traded fund holding Bitcoins.
- Bitcoin's journey into the financial mainstream has already begun, with HM Treasury's report on digital currencies marking encouraging progress toward the predictions in this infographic. The report introduces anti-money laundering, consumer protection and technical standardisation for digital currency companies in the UK, which will encourage traditional financial services to engage more with digital currency businesses and accelerate the integration of blockchain technology within financial services.

화폐 발행 Schedule



연도 별 화폐 발행 량

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%

Bitcoin

이 알고리즘은 Bitcoin 네트워크에 속한 모든 컴퓨터가
거래 검증 및 기록을 하도록 상호 협력하도록 디자인 되었으며,

거래기록의 위조 및 이중거래를 차단하도록 설계되어 있습니다.

이 알고리즘은, "A가 B에게 코인 한 개를 지불 합니다" 같은
평범한 문자 메세지가 수정 불가능하도록 기록될 때,

A가 B를 직접 만나서 동전 한 개를 건네주는 것과 똑같은 수준의
지불수단의 역할을 할 수 있음을 보여 주었습니다.

국가나 은행과 같은 신뢰받는 제3자의 중개가 없어도,
누구나 안심하고 인터넷 상에서 신뢰거래를 할 수 있게 된 것이죠.

도대체 어떻게 설계된 알고리즘이기에 그런 게 가능해진 것 일까요?

해답은 의외로 너무나 간단한 것이었습니다.

즉, 거래의 내용과 시간이 수정 불가능한 방식으로 기록되고,
또 기록된 거래장부를 인터넷에 실시간으로 공개하여
누구나 열람 가능하도록 한 것 입니다.

Bitcoin

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 파일 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 영원히 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.

이 기술혁신에 전 세계가 주목하고 있습니다.
화폐 이외에 다른 문제에도 적용하여 효과를 크게 보고 있습니다.

Blockchain 기술

한 개의 파일(1Mbyte)을 블록이라고 칭합니다.
이 파일 안에 거래 내용과 시간을 담습니다.
이런 파일들을 시간의 순서대로 연결한 것을 블록체인이라 부릅니다.

즉 블록체인은 연결된 디지털거래장부입니다.

시간 1: A가 B에게 코인 두 개를 지불합니다
시간 2: B가 C에게 코인1개를 지불합니다
시간 3: C가 D에게 코인 0.5개를 지불합니다

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.

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.

시간 2의 거래 예시) B의 소유권 확인은 어떻게 하나?

답: 시간 1의 거래에 "B의 공개키에게 코인을 두개 지불합니다" 라고 기록 되는 것.

시간2의 거래내역을 정말로 B가 보낸것을 어떻게 아나?

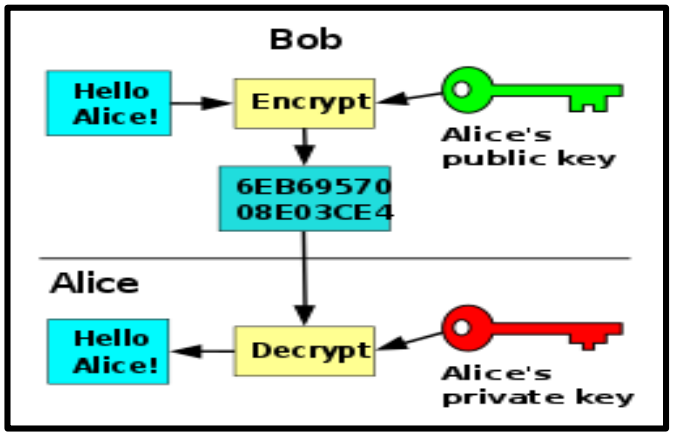
답: 거래내역을 B가 개인키로 싸인을 보태서 기록하는 것.

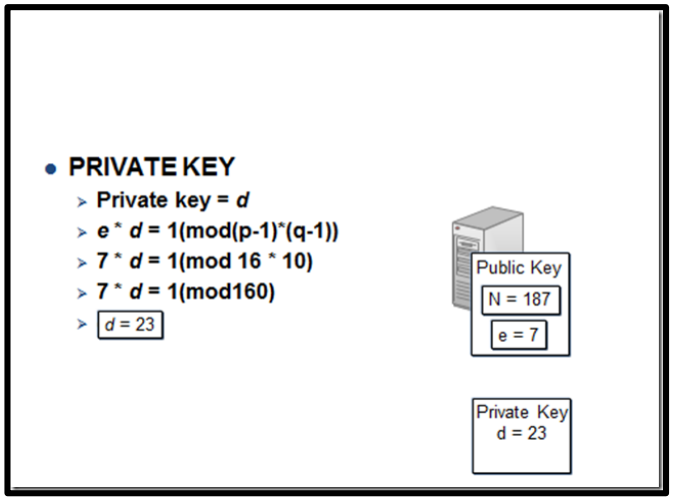
How to do Digital Signature (RSA example)

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

  $y = ENC(m, Pub\_a)$
- *Alice receives y and decrypts it using its private key.*

  $message = DEC(y, Pri\_a)$
- *ENC* and *DEC* are given and known functions.





Google pictures

RSA 디지털 싸인

Q.1. Let *e*, *m* and *n* be *known* positive integers.
Is it easy to find *d?*

$$\left(m^e\right)^d = m \bmod n \quad \text{-- (1)}$$

Once d known, it is easy to check

$$\left(m^d\right)^e = m \bmod n \quad \text{-- (2)}$$

Let d be pri-key and e public-key.

Pri-key: 개인키
Pub-key: 공개키

Ex 1) *Bob can send a private message m to Alice.*
Bob uses public key e of Alice, send c = m^e to Alice.
Only Alice can recover original message m, using d in (1).

Note: bitcoin에서는 RCA를 사용하지 않고 SHA를 사용함.

그러나 잘 알려진 RCA를 활용하여 디지털싸인 기능을 설명하고자 함

Ex 2) *Bob can append his signature h(m)^d to his message m sent to Alice.*
Bob uses his pri-key d to generate h(m)^d.
Using Bob's pub-key e, Alice recovers h(m) via (2).
Using Bob's message m recovered from Ex1), Alice generates h(m).
Alice checks if the two hash values match.

Blockchain 기술

블록체인은 공개된 디지털 파일묶음입니다.

디지털 파일?
그 안에 들어있는 거래기록은 위조 및 변조되기 쉽지 않은가?

전혀 새로운 방식으로 위조 및 변조 문제의 해결책을 제시하였습니다.

- 새로운 블록을 생성하는 단위 시간마다, 해당 블록의 블록요약을 붙여야 한다.
- 요약은 허가된 수준을 만족해야 하며, 좋은 블록요약이 기록된 블록은 체인에 연결합니다.

천재적 발상.
- 한 대의 컴퓨터로는 정해진 시간 내에 만족하는 좋은 블록요약을 찾을 수 없음.
- 무수히 많은 컴퓨터가 참여할 때, 비로서 그들 중 한 대가 Good 블록요약 결과를 낼 수 있음.
- Good요약에 성공한 한 대의 컴퓨터에게 코인보상을 함으로써, 지속 참여 유도.

Bitcoin Blockchain

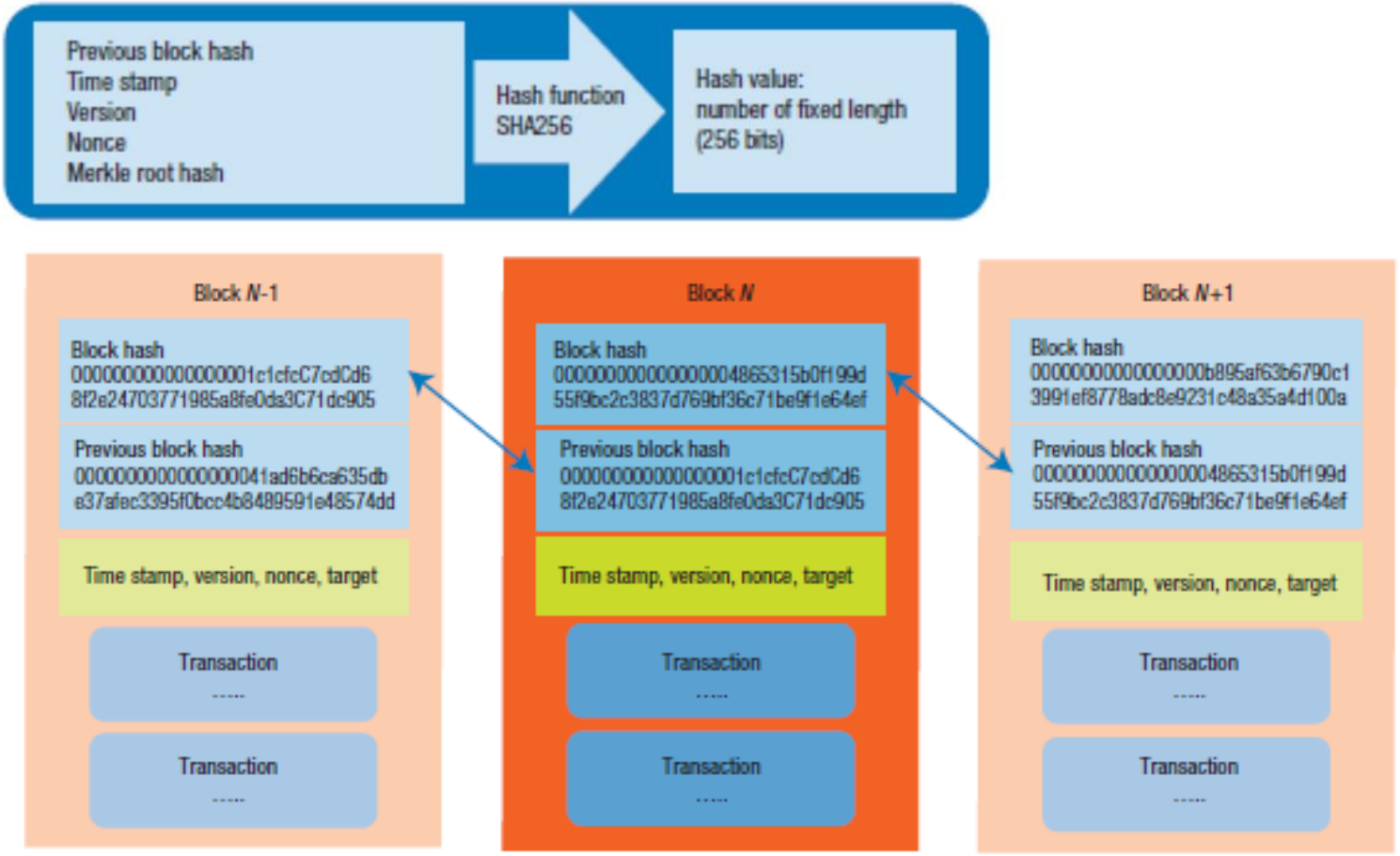
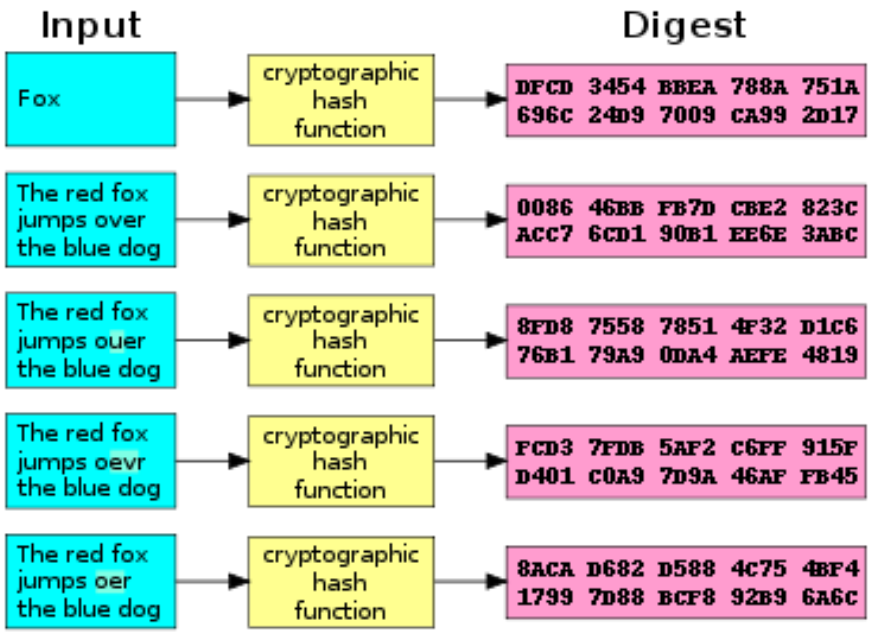
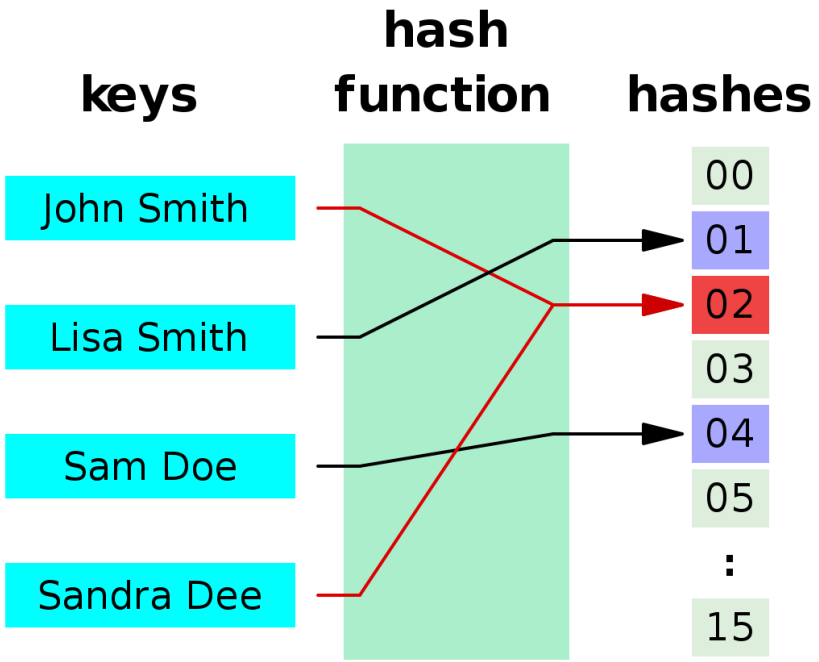


FIGURE 2. Bitcoin blockchain. The blockchain consists of text blocks containing records of transactions that are linked through consecutive hash numbers generated from the content of the previous block plus a random part.

Secure Hash Function I/O





Pictures from google image

Bitcoin uses SHA-256

SHA-256(M):
(* Let M be the message to be hashed *)
for each 512-bit block B in M **do**
$W = f_{exp}(B)$;
(* Initialize the registers with the constants. *)
$a = H_0$; $b = H_1$; $c = H_2$; $d = H_3$; $e = H_4$; $f = H_5$; $g = H_6$; $h = H_7$;
for $i = 0$ **to** 63 **do**
(* Apply the 64 rounds of mixing. *)
$T_1 = h + \Sigma_1(e) + f_{if}(e, f, g) + K_i + W_i$;
$T_2 = \Sigma_0(a) + f_{maj}(a, b, c)$;
$h = g$; $g = f$; $f = e$; $e = d + T_1$; $d = c$; $c = b$; $b = a$; $a = T_1 + T_2$;
(* After all the rounds, save the values in preparation of the next data block. *)
$H_0 = a + H_0$; $H_1 = b + H_1$; $H_2 = c + H_2$; $H_3 = d + H_3$;
$H_4 = e + H_4$; $H_5 = e + H_5$; $H_6 = e + H_6$; $H_7 = e + H_7$;
(* After all 512-bit blocks have been processed, return the hash. *)
return concat(H_0, H_1, H_2, H_3, H_4, H_5, H_6, H_7);

Algorithm 1.3: THE SHA-256 ALGORITHM.

SHA-2

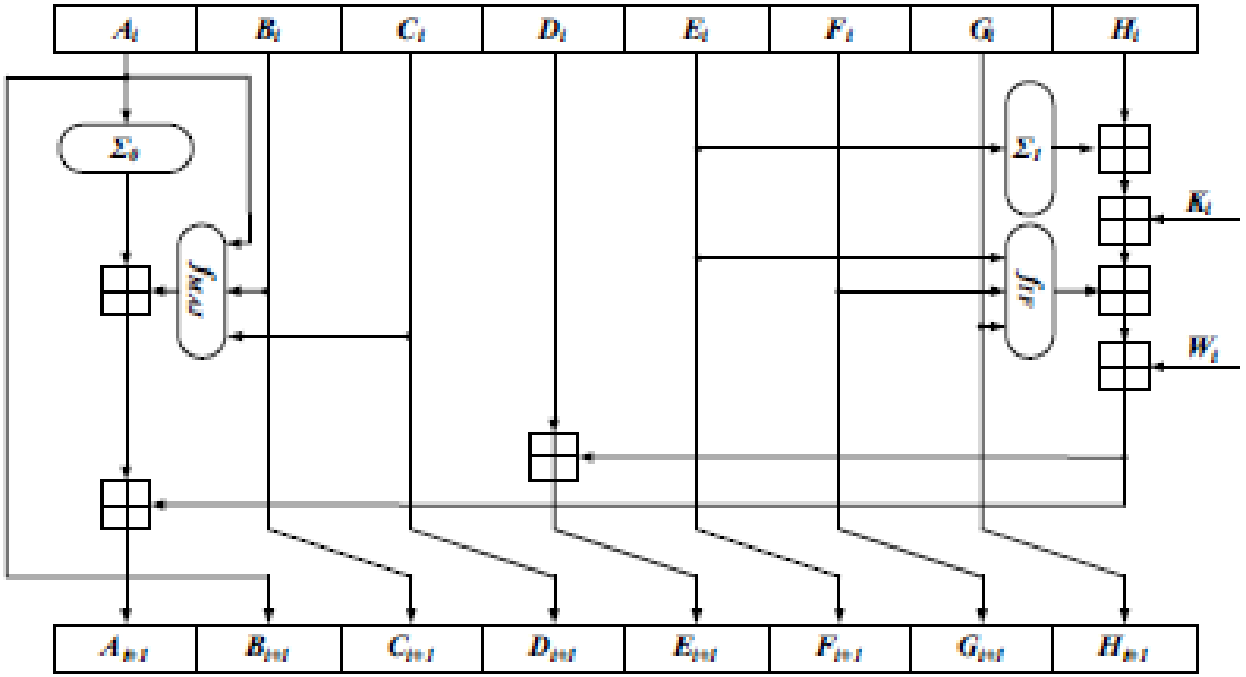


Figure 1.4: Schematic oveview of a 0 SHA-2 round. Note the added non-linear functions in comparison with SHA-1.

Hash Function이란 무엇인가?

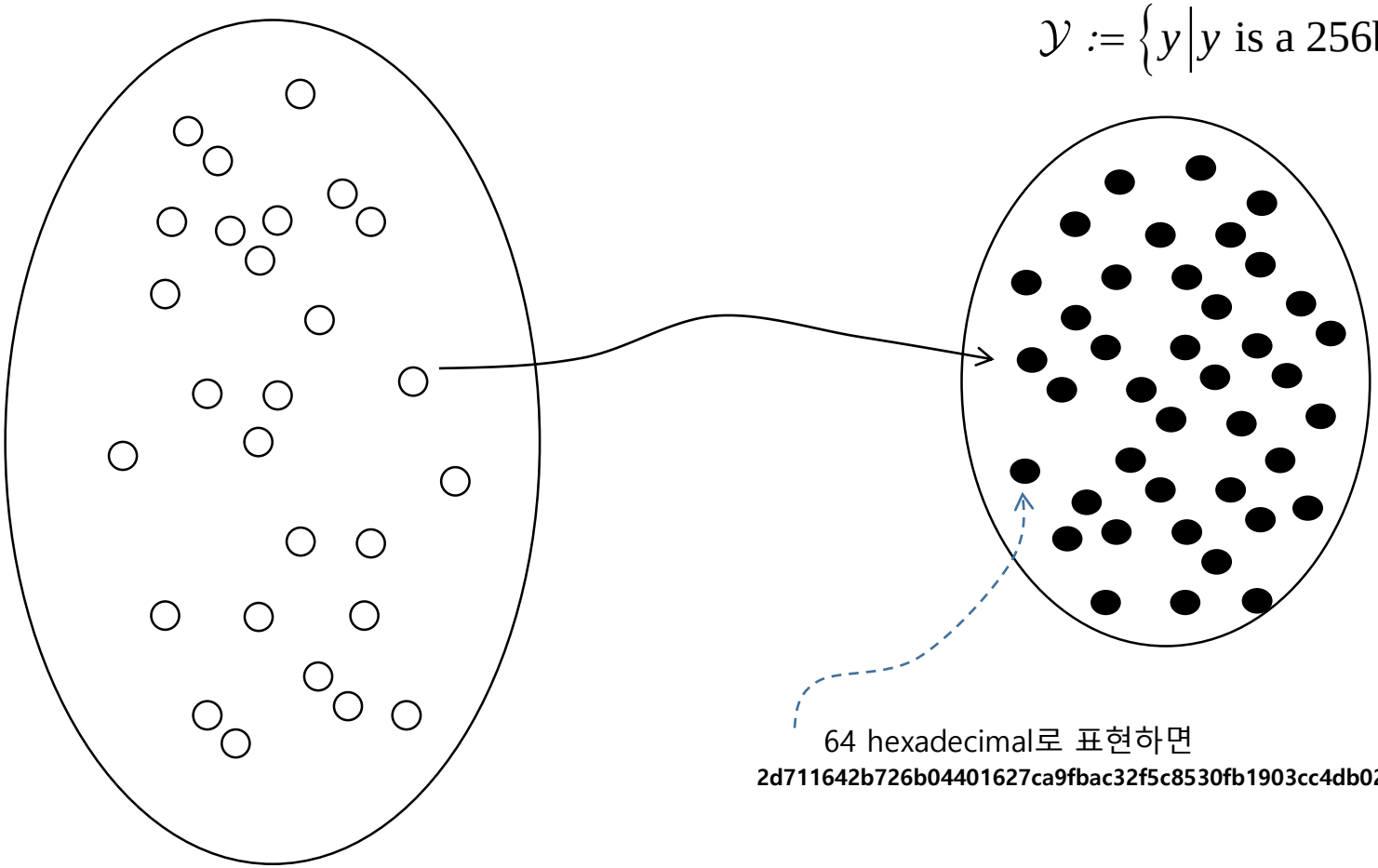
- Bitcoin은 SHA256 hash function을 사용 함.
- Hash function의 input은 text message 혹은 파일.
- Hash function의 output은 256 bit string.
- Hash Function의 조건
  - Input이 조금만 바뀌어도 output은 완전히 다르게 바뀜.
    - Input distance 는 output distance 와 아무런 관련이 없음.
  - Given y = H(x), finding x1 such that H(x1) = y shall be almost impossible!
  - Finding an input pair x and x1 which leads to H(x) = H(x1) shall be almost impossible!

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

SHA256 설명, F(x) = y

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

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



64 hexadecimal로 표현하면

2d711642b726b04401627ca9fbac32f5c8530fb1903cc4db02258717921a4881

만족하는 블록요약 찾기 예시

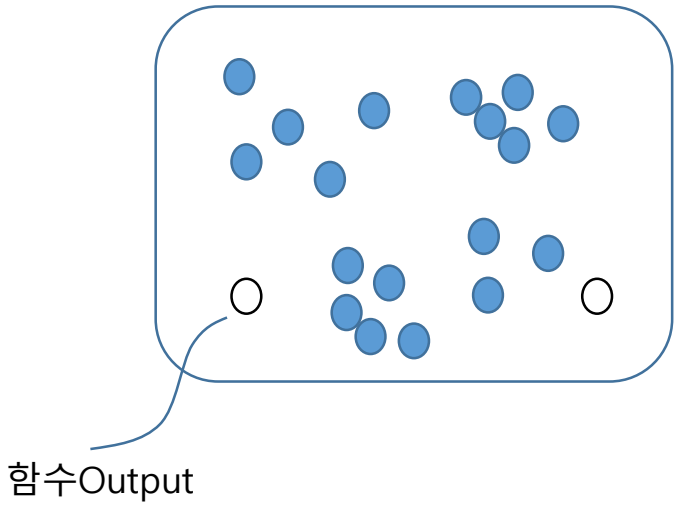
- 암호함수 F 사용
- 함수F 는 Input x 을 주면 Output y 를 내주는 것
- 함수의 Output을 F(Input) 라고 표현
- F(블록) = 블록요약
- 디지털 컴퓨터에서, 파일내용, 블록요약은 모두 디지털 숫자임
- 만족하는 블록요약 문제 제시는 다음과 같이 할 수 있음.

F(블록, 블록난수) < 지정된 특정 숫자

- 블록 난수를 바꾸어 가며, 함수 입출력을 계속해서 위 식을 만족하는 블록난수 하나를 찾는 것
- 찾은 블록 난수 하나를 찾아 블록에 기입하는 것

아래 상자에서 눈감고 공을 하나 뽑을 때

한 번에 흰색 공을 뽑을 확률은?



작업증명 군가혼불 문제 예시

======= 작업증명 군가혼불 증명 =======

입력값의 집합 C는 크게 둘로 나눌 수 있음.
원하는 출력값을 내는 입력 값의 집합 A.
A의 여집합 B.
각 집합의 크기를 a, b, c로.

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

이 cpu가 한 번 대입으로 PoW문제를 푸는데 성공할 확률은?

P1 = a/c
= 10^-6
= 0.000001

Cpu 1은 10초안에 함수 입출력을 100번 할수 있음.

Cpu1이 10초 안에 PoW문제풀이에 성공할 확률은?

P2 = a/c + (b/c)*a/c + (b/c)^2*a/c + …
~ 100*a/c
= 10^-4

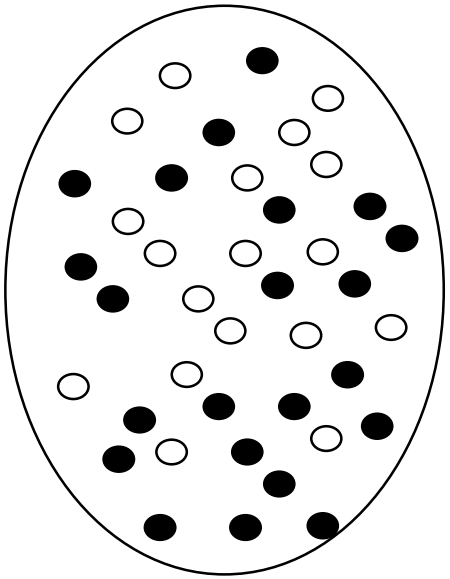
이런 cpu 1만 대가 참여하는 네트워크에서, 그 중 최소 한 대가 10초 안에 문제를 풀 확률은?

지금 guess한 그 정도면 됨.

==========군가혼불 증명 끝 ==========

문제: 앞에 0이 4개 붙은 작업증명값을, cpu가 단 한 번에 찾을 확률 P1은?

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



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

256 bit는 64 hexadecimal string

보통 해쉬 값
2d711642b726b04401627ca9fbac32f5c8530fb1903cc4db02258717921a4881

앞에 네 자리가 0이어야 한다는 조건을 통과하는 hash값
0000f727854b50bb95c054b39c1fe5c92e5ebcfa4bcb5dc279f56aa96a365e5a

c = 해쉬 집합의 크기 = 2^256
a = 원하는 해쉬 집합의 크기 = 2^(256 – 16) = 2^240

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

Proof of Work Analysis

- Proof of work(작업증명)는 miner들이 경쟁적으로 문제를 푸는 방식.
  제일 먼저 문제를 푼 miner가 코인보상을 받고 새로운 블록을 체인에 연결 하는 방식 임.
- 한 번 체인에 들어간 내용은 절대 수정 불가능함.
- 어떻게 그렇게 하는 것인지 궁금해짐.

- 답은 간단.
  군집 중 어느 하나는 시간내에 답을 찾지만, 혼자서는 시간내에 못 찾는 "군가혼불" 작업증명 문제를 만들고 각자 풀게 함.
- 작업증명문제?
  함수의 정의. 입력값을 함수에 넣으면 출력값이 나옴.
  어떤 암호함수를 지정함. 이 함수의 특징은 입력값과 출력값은 1대1 매칭. 출력값을 보고 입력값을 전혀 짐작 못 함.
  작업증명 문제는 암호함수의 출력값이 특정 숫자보다 작게나오게 하는 입력값을 찾는 문제임.
- 그러므로 작증문제를 푸는 방식은 대입법 뿐.
  즉, 원하는 출력값이 나올 때 까지, 입력값을 바꾸어 보는 것.
  찾은 입력값을 블록에 기록해 넣음으로 블록의 작업증명을 완결함.

위변조 원천 봉쇄 기술

- 혼자서는 시간 내에 못 푸는 문제를, 네트워크에 속한 수 많은 컴퓨터가 경쟁적으로 풀게 할 때, 특정 시간안에 풀릴 수 있도록 설계 한 것이 바로 작업증명 방식임.
- 이런 군가혼불 작업증명 방식으로 블록체인의 보안성을 확보 함.
  군가혼불이기에 소수가 다수를 기만할 수 없게 됨.
- 작업증명은 승인된 거래내역을 담은 블록의 내용과 일치하는 군가혼불 문제의 입력값을 찾아 블록안에 기입해 넣는 것.
- 한 번 블록체인안에 기록된 내용을 절 대 바꿀 수 없는 이유는 무엇인가?
  체인에 들어간 모든 블록은 군가혼불 입력값이 기입되어 있음.
  내용을 조금이라도 바꿀 경우 쉽게 알 수 있음.
- 특정블록안에 들어간 내용을 바꾸기는 쉬움.
  왜? 디지털파일이니까.
  그러나 블록내용이 바뀌면, 기입되어있는 군가혼불값과 블록내요은 서로 일치 하지 않게 됨.
  즉 암호함수의 입력과 출력값이 다르게 됨.
  암호함수입출력을 통해누구나
  쉽게 내용이 변조되었음을 누구나 알게 됨!
  변조된 블록체인은 폐기 함.
- 위변조하려는 공격자는
  그러므로 군가혼불 문제를, 바뀐 내용을 반영하며 다시 풀어야 함.
  왜?

그렇지 않으면 내용을 몰래 바꾼 것을 숨길 수 없기 때문에.
블락들은 체인으로 연결되어 있음. 즉, 어떤 한개의 블록내용의 위변조는 뒷 블록들의 연쇄적 내용 변화를초래.
내용이 변한 모든 블록의 군가혼불 문제를 정해진 시간내에 모두 풀어야 함.

한 두대의 컴퓨터로는 당연히 불가능.
체인에 깊숙히 자리잡은 거래기록은 매우 안전한 이유이기도 함.
네트워크에 속한 컴퓨터를 매우 높은 비율로 확보한 집단이
다른 참여자들을 기만하고
체인을 공격하는 것은 가능하나,
수 많은 다양하고 독립적인 참여자를 확보한 분산네트워크에서는 그런 연합이 생겨날 가능성은 거의 없는 것으로 치부 됨.

그러므로
비트코인네트워크의 안정적인 운영에는
수 많은 독립적인 miner 들의 참여가 필수적.

문제는 각miner들이 위에 설명한 군가혼불 문제를 풀기위해
많은 전기를 소모하며 대입법 문제를 풀고 있는 것.
비트코인 시스템의 보안성 확보를 위해 세계에서 각지에서 많은 전기에너지를 소모하고 있는 비효율이 만들어 지고 있는 것.

이제 걸음마를 떼고 있는 블록체인 기술이 더욱 성숙해지기 위해서 꼭 해결해야 할 문제 중 하나 임.

이 문제 해결을 위해 PoW대신 Proof of Stake로 하자는 제안이 주목받음!

Blockchain : 위변조가 불가능하게 공개파일에 기록하는 기술

블록 체인은 디지털 파일을 시간의 순으로 연결한 것.
목적은 공개되어 기록된 내용을 누구나 확인할 수 있으나, 내용의 위변조는 불가능하게 하는 것.

How?
체인으로 연결된 모든 블록은 그 다음 블록과 연계함.

- 현재 블록의 한 줄 요약을 그 다음 블록의 내용에 넣도록 설계되어 있음.
- 퀴즈) 특정 블록의 내용이 바꾸면 생기는 일은?

또한 그 블록 뒤에 붙은 블록의 내용과 작업증명들도 따라서 바뀌어야 하는 것 입니다.

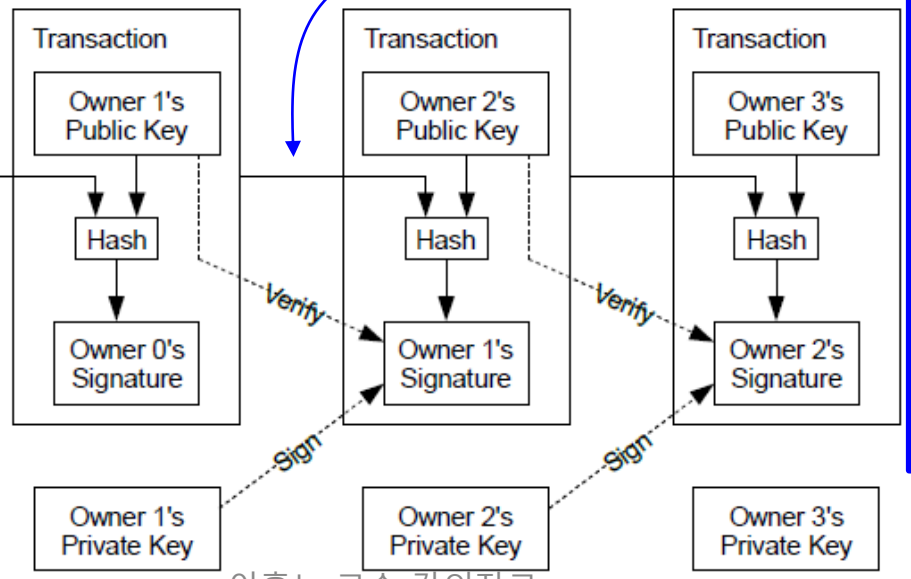
위변조는 블록체인 속에 기록된 거래 내용을 어떤 한 대 혹은 한 무리의 컴퓨터가 임의로 다른 구성원의 동의 없이 바꿀 수 있을 때 가능합니다.

일단 이런 기만적 행위가 가능하려면, 위변조에 필요한 작업증명을 모두 혼자서 감당할 수 있을 때입니다.
앞서 언급한데로, 공동노력에 의한 작업증명 설계는 이러한 소수의 공격을 무의미한 것으로 만듭니다.

Bitcoin

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

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



두 번째 Tx 상황
1. 첫번째 거래기록을 O2의 pubkey로 hash해서 저장.
2. 저장한 해쉬값을 Owner1이 PrivKey로 싸인해서, 거래기록2에 남김.
누구든지, Owner1의 Signature를 Owner1의 public key로 Decrypt 해서, Decrypt 값이 해쉬값과 일치하는지 확인할 수 있음.
그런데 chain of digital signatures가 코인이라면 hash값은 저장 안 되는 것인가?
Hash값이 없으면, 싸인과 일치하는지 확인할 수 없지!
그러니까, Hash는 싸인과 함께 저장되어 있어야 함!

2nd Tx = BTC1개를 Owner1이 Owner2로 보냄

위 Message를 Owner2와 PubKey 함께, Encrypt한게 해쉬 값

이 거래의 해쉬값을 Owner1이 싸인하므로 자신이 해당 코인의 소유권을 증명함과 동시에 그 소유권을 O2에게 넘기고 있음을 증명.

Double Spending Problem

- Mint가 심판으로 존재하는 경우, 모든 거래를 보고받고, 누가 먼저 거래를 완료했는지 확인 가능하며, Double spending문제를 원천 봉쇄 할 수 있음.
- 문제가 원천봉쇄 되었기 때문에, O2는 Double Spending을 시도 할 수 조차 없음.
- 제 삼자의 도움 없이, Double spending 문제를 푸는 방법은 없는가?
- 특히 P2P 네트워크에서 여러 노드들이 해결하는 방법은 없는가 연구.
- 여러 노드들이, 해당 코인의 거래를 기록한 장부를 단 하나만 만들고 유지하는 방법은 무엇인가?
- 즉 P2P네트워크에 거래원장을 만들고 유지할 수 없는가?

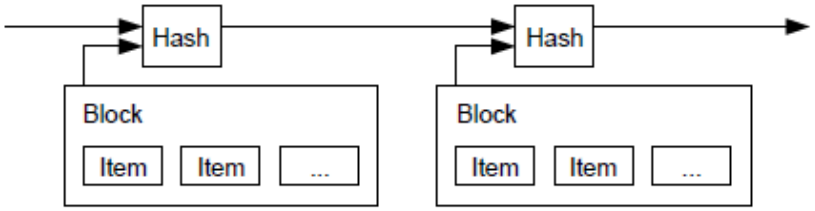
The problem of course is the payee can't verify that one of the owners did not double-spend the coin. A common solution is to introduce a trusted central authority, or mint, that checks every transaction for double spending. After each transaction, the coin must be returned to the mint to issue a new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

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

- 제 삼자의 도움 없이, P2P 네트워크에서 여러 노드들이 DS문제를 해결하는 방법 연구.
- 여러 노드 들이, 해당 코인의 거래를 기록한 장부를 단 하나만 만들고 유지하는 방법은 무엇인가? 즉 원장을 만들고 유지할 수는 없는가?
- 다음페이지에 나오는 Time-stamp 서버를 운영한다면 해결 가능한 가?

3. Timestamp Server

The solution we propose begins with a timestamp server. A timestamp server works by taking a hash of a block of items to be timestamped and widely publishing the hash, such as in a newspaper or Usenet post [2-5]. The timestamp proves that the data must have existed at the time, obviously, in order to get into the hash. Each timestamp includes the previous timestamp in its hash, forming a chain, with each additional timestamp reinforcing the ones before it.



- Timestamp server가 특정시간에 hash값이 존재했던 것을 알려주기만 하면, 거래를 기록하는 원장을 만들수 있는 가?
  - Hash값만 공표해도 된다면, block내용은 공표하지 않아도 된다면, Scalability문제 없음, 거래 당사자 외 타인은 거래내용을 알 수 없음으로 Privacy 도 보장!
  - 그런데, 뒤의 예에서 볼 수 있듯이, 블록내용도 공개되어야 함. 거래 검증 및 이중거래 방지 위해서 필요.
- 문제는, 과연 누가 Timestamp Server를 관리하게 할 것인가?
- 국가가 관리하면 private blockchain (사회학적으로는 public 즉 공적체인) 이 됨!
- 국가가 관리할 경우의 문제점은 무엇인가?

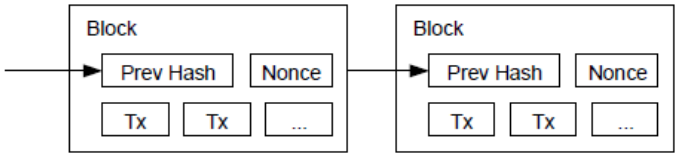
Blockchain & Proof-of-Work

- Timestamp Server를 P2P 네트워크로 구현하고자 함.
  - Why?
  - Central authority에 의존하지 않기 위해서.
  - Central authority는 은행 혹은 국가등
  - 국가 내에서는 국가가 관리하면 됨.
  - 국경을 넘나드는 거래를 가능하게 하기 위해서는, 국가간 P2P가 필요하게 됨
- Solution?
  - Distributed timestamp P2P network
  - Distributed됨으로, 데이터 무결성을 확보하기 힘들게 됨
  - Distributed system에서 데이터 무결성 확보 위해, PoW system같은 장치를 제안하게 됨.

4. Proof-of-Work

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

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



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

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

5. Network

Consensus Rule

The steps to run the network are as follows:

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

Nodes always consider the longest chain to be the correct one and will keep working on extending it. If two nodes broadcast different versions of the next block simultaneously, some nodes may receive one or the other first. In that case, they work on the first one they received, but save the other branch in case it becomes longer. The tie will be broken when the next proof-of-work is found and one branch becomes longer; the nodes that were working on the other branch will then switch to the longer one.

New transaction broadcasts do not necessarily need to reach all nodes. As long as they reach many nodes, they will get into a block before long. Block broadcasts are also tolerant of dropped messages. If a node does not receive a block, it will request it when it receives the next block and realizes it missed one.

- 모든 tx가 block에 들어간다는 보장이 어디 있지?
- 인센티브(tx fee)를 지급해서 넣으려고 하기는 할 테지만, 넘쳐나는 tx이 있는 경우라면, 다른 것들에 밀려 block에 못 들어갈 수도 있지않은가?
- Tx을 issue한 노드가 verify하는 방법은 무엇이지? 순서가 있는 것도 아닌데. 코인을 받아야 하는 사람 쪽에서, block announcement를 보고 계속 체크하거나, 코인을 지불하는 쪽에서도 물건을 빨리 받기 위해서 check를 할 수도 있기는 하지만. …
- 거래요청이 Block에 들어간다는 보장이 없음. 거래완료 보장 없음!

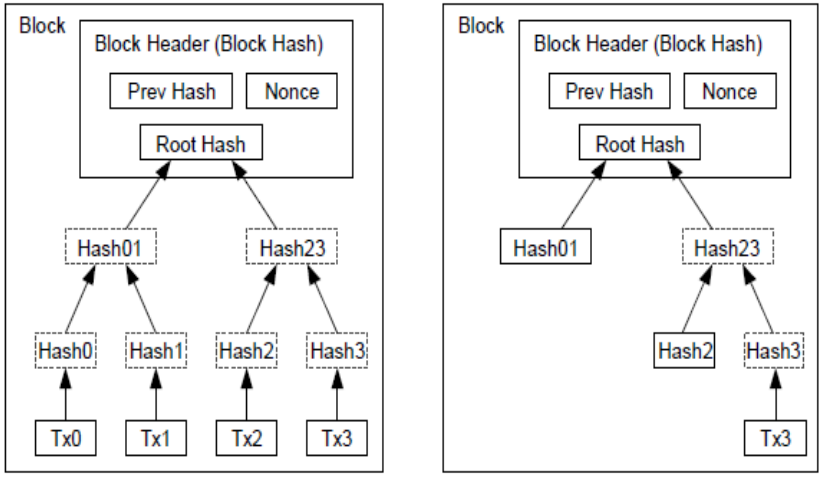
Blockchain Scalability

- Merkle tree활용, Diskspace 절약
- Blockhash를 헤더에 남기고 유지.
- 지나간 거래기록 내용이 있는 부분tree는 대표hash만 남기고, 지워 버림.
- 블록헤더 80 bytes

1. Block no.
2. Prev hash: 256 bit = 2^8 = 2^5*(2^3) = 2^5 Bytes = 32 Bytes
3. Roothash = 32 Bytes
4. Nonce = 4 Bytes = 32 bit
5. Blockhash = 32

7. Reclaiming Disk Space

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



Transactions Hashed in a Merkle Tree

After Pruning Tx0-2 from the Block

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

80 Byte Block Header

Bytes	Name	Data Type	Description
4	version	int32_t	The block version number indicates which set of block validation rules to follow. See the list of block versions below.
32	previous block header hash	char[32]	A SHA256(SHA256()) hash in internal byte orderof the previous block's header. This ensures no previous block can be changed without also changing this block's header.
32	merkle roothash	char[32]	A SHA256(SHA256()) hash in internal byte order. The merkle root is derived from the hashes of all transactions included in this block, ensuring that none of those transactions can be modified without modifying the header. See the merkle trees section below.
4	time	uint32_t	The block time is a Unix epoch time when the miner started hashing the header (according to the miner). Must be strictly greater than the median time of the previous 11 blocks. Full nodeswill not accept blocks with headers more than two hours in the future according to their clock.
4	nBits	uint32_t	An encoded version of the target threshold this block's header hash must be less than or equal to. See the nBits format described below.
4	nonce	uint32_t	An arbitrary number miners change to modify the header hash in order to produce a hash less than or equal to the target threshold. If all 32-bit values are tested, the time can be updated or the coinbase transaction can be changed and the merkle root updated.

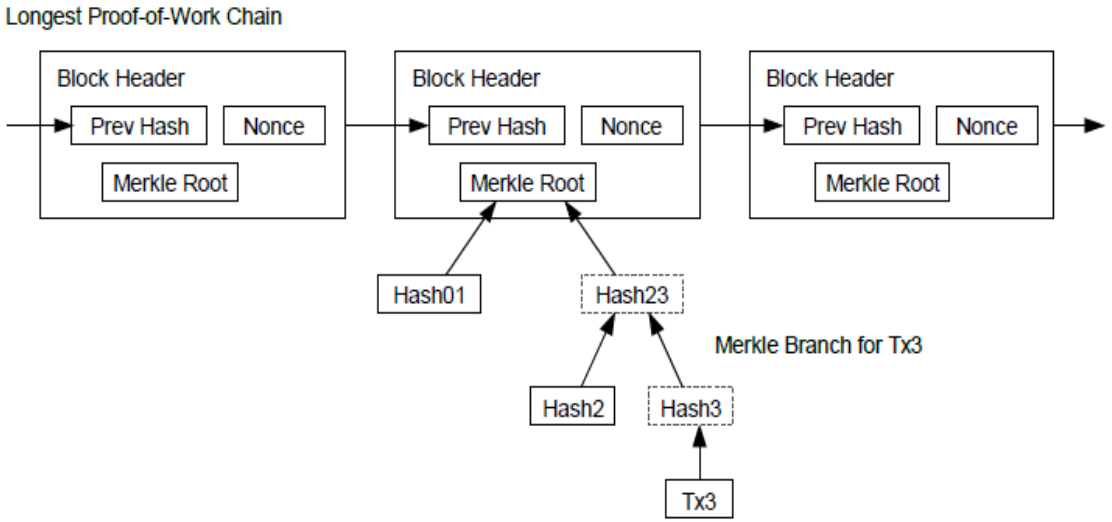
Source : https://bitcoin.org/en/developer-reference#block-headers

Longest Chain is Trusted, Why?

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

8. Simplified Payment Verification

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



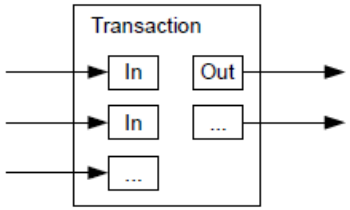
As such, the verification is reliable as long as honest nodes control the network, but is more vulnerable if the network is overpowered by an attacker. While network nodes can verify transactions for themselves, the simplified method can be fooled by an attacker's fabricated transactions for as long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

Payment and changes

- 거스름돈은 어떻게 받나?

9. Combining and Splitting Value

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



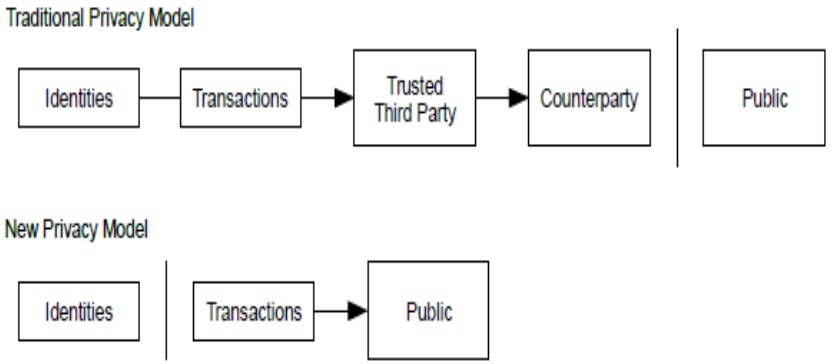
It should be noted that fan-out, where a transaction depends on several transactions, and those transactions depend on many more, is not a problem here. There is never the need to extract a complete standalone copy of a transaction's history.

Privacy, by Anonymous Pub Key

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

10. Privacy

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



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

How Difficulty to Attack?

- What happens when the attacker's chain dominates the honest chain?
- Prob(length of att. chain > length of h.chain)
- Invalid transactions are to be included in the attacker's chain.
- Invalid transactions are soon detected by the honest nodes.
- The honest nodes inform the network so that nodes are not accepting the chain with invalid transactions.
- The best attack that can be made is to alter its own transaction.
- Namely, reclaim what he has paid.

11. Calculations

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

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

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

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

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

Attacker is the payer, fooling the payee!

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

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

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

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

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

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

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

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

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

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

Converting to C code...

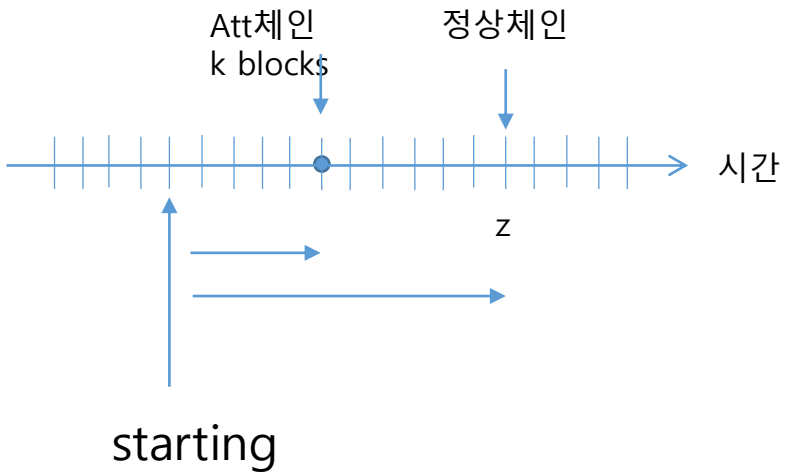
Z block 전에 들어갔던 내용을 변조해야 한다.
"A가 B에게 코인 1개준다" 를 "A가 C(A의 또다른 키)에게 코인 1개준다." 로 바꾸려 한다면

Z blocks of PoW done and published

After the new is published

There are two chains, the honest chain and the attacker's chain.

The longer chain is to be accepted!



$$\sim\sum_{k=0}^{\infty}\begin{cases}(q/p)^{z-k} & k<z\\ 1 & k\geq z\end{cases}\ \text{Poisson}(\lambda = zq/p, \text{attack success rate in z unit time})$$

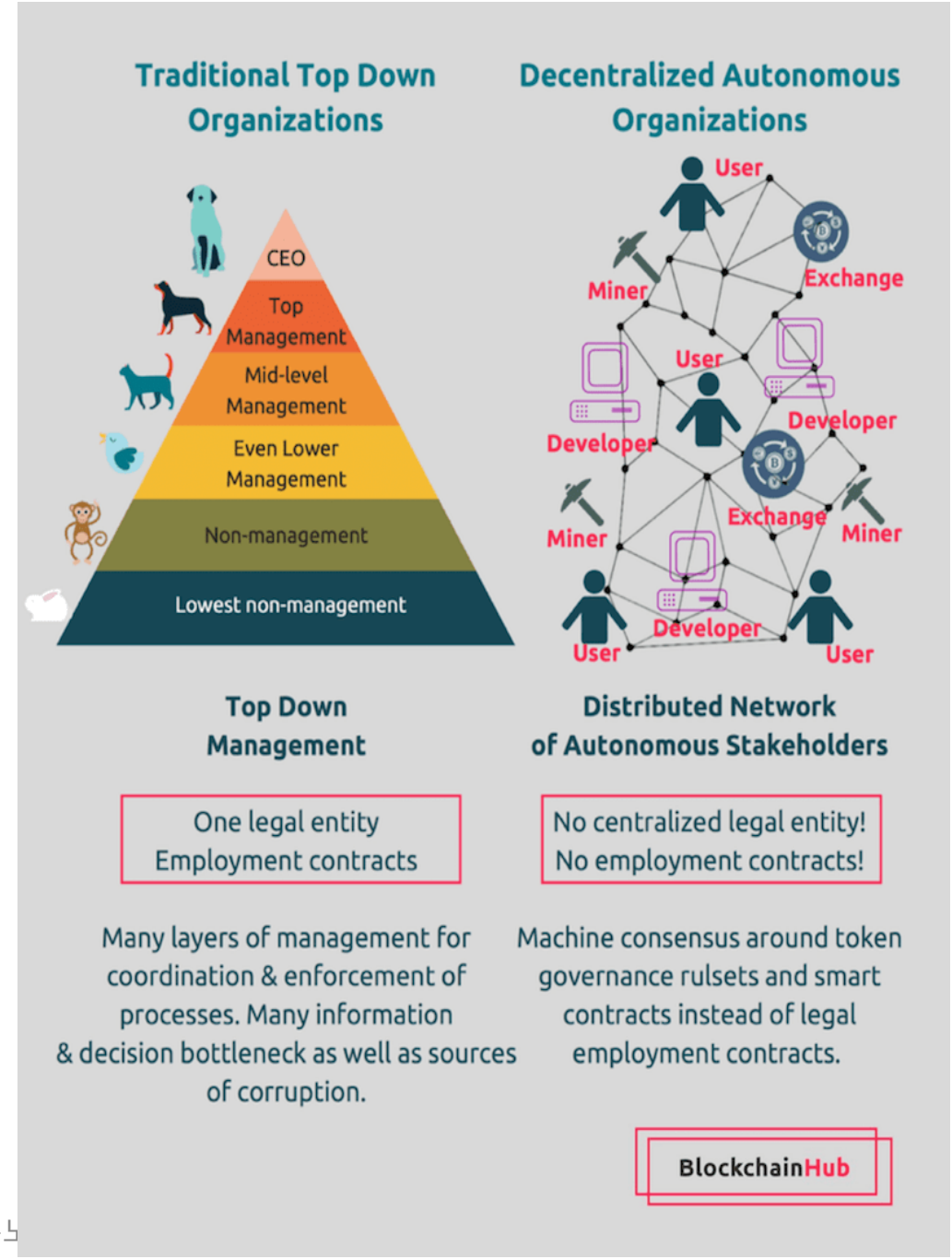
$$=\sum_{k=0}^{\infty}\begin{cases}(q/p)^{z-k} & k<z\\ 1 & k\geq z\end{cases}\frac{(zq/p)^{k}e^{-zq/p}}{k!}$$

Bitcoin Economy

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

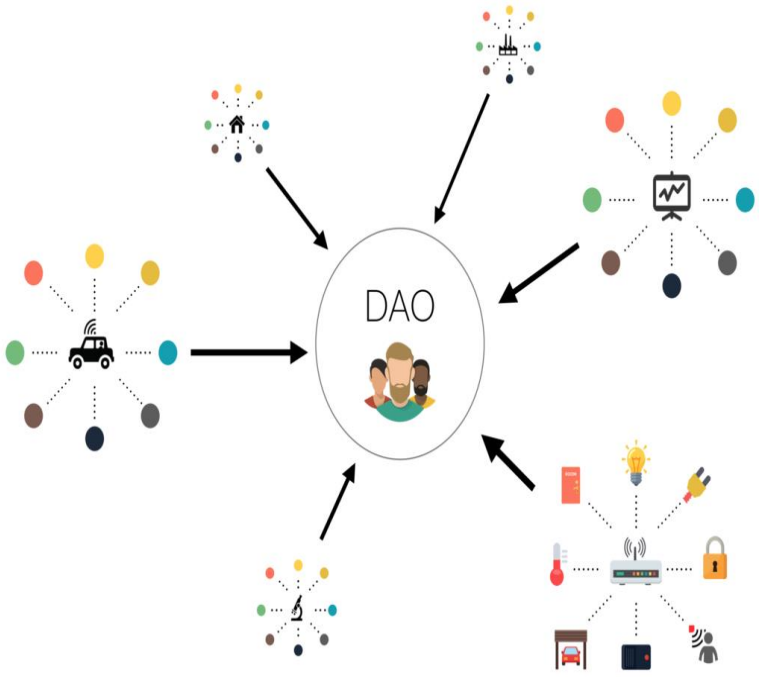
의도치 않았지만 생겨난

- Exchange
- 투자자
- Crowd funding
- DAOism의 탄생!



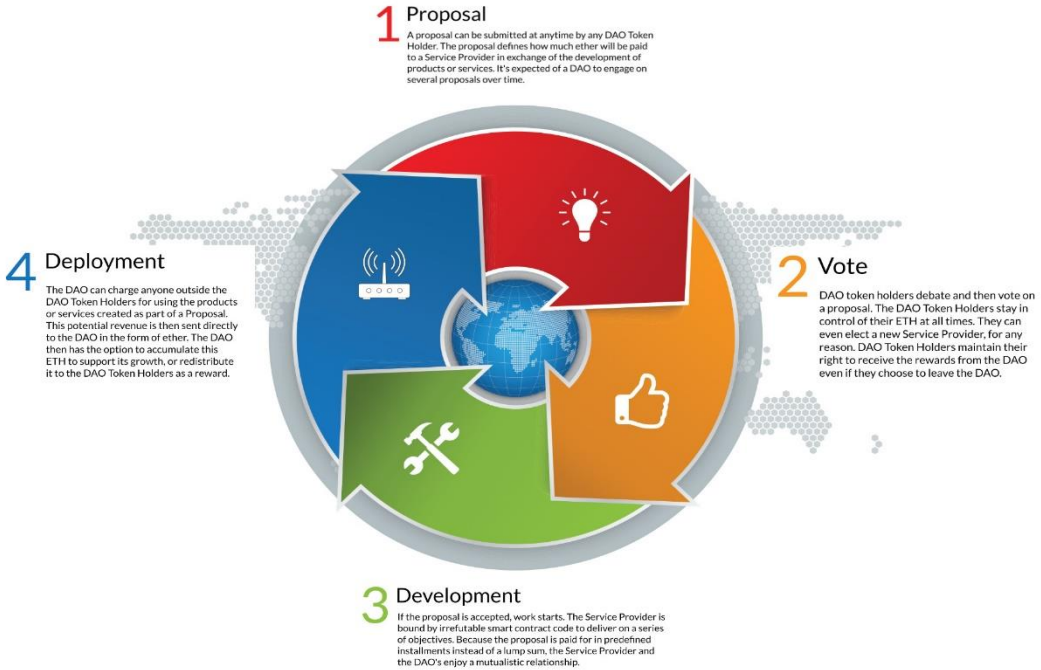
How DAOs work

- Decentralized Autonomous Organisations (DAOs) run through rules encoded as computer programs called smart contracts. It is an entity that lives on the internet and exists autonomously, but also heavily relies on hiring individuals to perform certain tasks that the automaton itself cannot do.
- **Tokens of Transaction:** In order to exist a DAO needs some kind of internal property that is valuable in some way, and it has the ability to use that property as a mechanism for rewarding certain activities.
- **Autonomous:** Once deployed the entity is independent of its creators and cannot be influenced by outside forces. DAOs are open source, thus transparent and incorruptible.
- **Consensus:** In order to withdraw or move funds from a DAO, a majority of its stakeholders (this percentage could be specified in the code of the DAO) must agree on the decision. Even if bugs are found in the code, they could not be corrected until a voting procedure has taken place and the majority of voters agreed on it, which could leave known security holes open to exploitation.
- **Proposals:** Proposals are the primary way for making decisions in a DAO.
- **Voting:** After submitting a proposal, voting takes place. DAOs allow people to exchange economic value with anyone in the world, like investing, money raising, lending, borrowing, without the need of an intermediary, just by trusting the code.



DAOs as Crowdfunding Vehicles

- A growing number of startups are beginning to raise risk capital to fund the development of individual products, services or protocols,
- in a way that shares the future success of the company with its users and investors.
- Instead of complex, uncertain and strictly-regulated legal contractual relationships between investors and founders, those startups rely fully on DAO-type smart contracts to manage those relationships.
- Circumventing legal systems and thereby legality itself, is, however, not the primary interest of most of those startups.
- Instead, it is the much lower barrier to entry as well as the new untapped market potential that motivates entrepreneurs to go down the route of token crowd sales.
- Ideals of a new kind of sharing economy, where the users of a service are at the same time its owners, give those startups moral grounds for venturing into legally gray areas.



DAO ~ our Brain

Melanie Swan

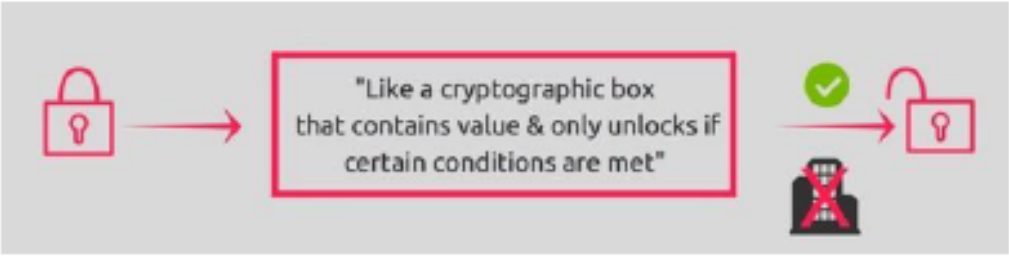
Blockchain Thinking

The Brain as a Decentralized Autonomous Corporation

Blockchains are a new form of information technology that could have several important future applications. One is blockchain thinking, formulating thinking as a blockchain process. This could have benefits for both artificial intelligence and human enhancement, and their potential integration. Blockchain thinking is outlined here as an *input-processing-output* computational system.

Smart Contracts

A smart contract is a computer code running on top of a blockchain containing a set of rules under which the parties to that smart contract agree to interact with each other. If and when the pre-defined rules are met, the agreement is automatically enforced. The smart contract code facilitates, verifies, and enforces the negotiation or performance of an agreement or transaction. It is the simplest form of decentralized automation. It is a mechanism involving digital assets and two or more parties, where some or all of the parties deposit assets into the smart contract and the assets automatically get redistributed among those parties according to a formula based on certain data, which is not known at the time of contract initiation.



Smart Contract
Source: Blockchainhub.net

The term smart contract is a bit unfortunate since a smart contract is neither smart nor are they to be confused with a legal contract:

- A smart contract can only be as smart as the people coding taking into account all available information at the time of coding.
- While smart contracts have the potential to become legal contracts if certain conditions are met, they should not be confused with legal contracts accepted by courts and or law enforcement. However, we will probably see a fusion of legal contracts and smart contracts emerge over the next few years as the technology becomes more mature and widespread and legal standards are adopted.

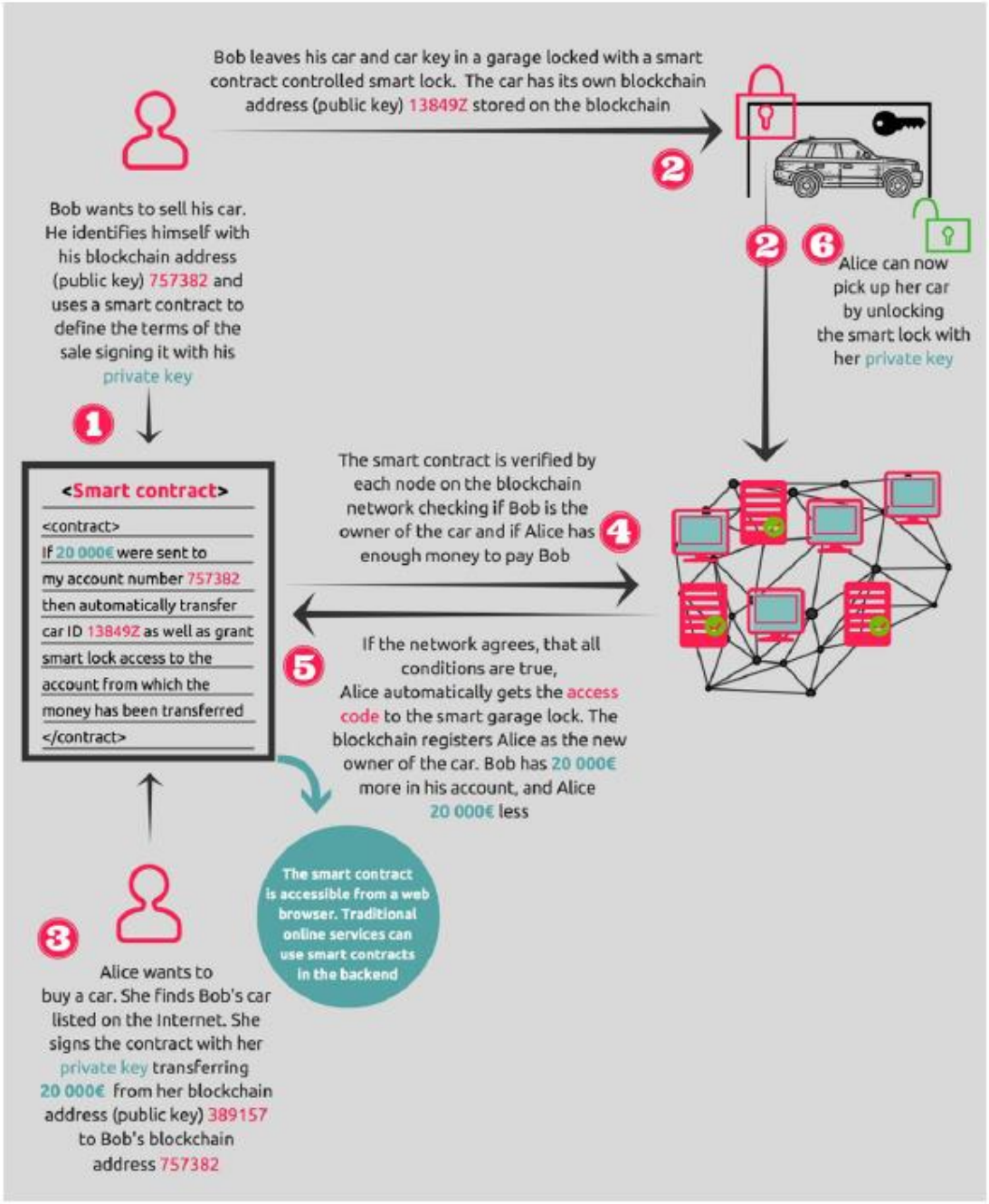
Buying a Car with Smart Contract

Smart contract

1. 파는 사람의 입장. If conditions are met, ownership is transferred.
2. 사는 사람의 입장. 돈을 내면, 곧바로 차를 인도 받고, 법적 owner로 등록이 되어야 한다.
3. …

이거면 될까? 과연?

1. 차의 상태에 대한 정보를 확인할 수 있게 할 수 없나?
2. Multisig 로 해결 가능?



Process of buying a car on the Blockchain

Source: Blockchainhub.net

유시민과 블록체인

유시민 작가는 역시 대단 했습니다.
비트코인 기술을 너무 잘 이해하고 있었고,
알기 쉽게 설명해 주었습니다.
블록체인은 공개된 장부인데, 위변조를 못 하게 하기 위해서,
채굴이라는 것을 해야 한다.
채굴해 주는 사람들을 끌어 모으기 위해
코인을 발행하고 채굴자에게 나눠준다.

여기까지는 좋았는데, 꼬이기 시작했습니다.
내재적 가치는 없는데,
사람들을 끌어 모아 가치를 높이는 이런 게 바로 폰지 사기다.
"비트코인 기술은 공학자들의 장난감에 불과하며,
거래소와 투기꾼들이 이 장난감을 이용해 만들어낸
인류역사 상 최대 사기극"이라고 결론짓고 말았습니다.

영향력이 매우 큰 분이, 용감하게, 또 매우 설득력 있게
잘 못된 결론을 내리는 상황이 안타까웠습니다.

그러나, 사실 유시민 작가 뿐 만이 아닙니다.
워런버핏은 "비트코인은 버블이다." 라고 하였고,
JP모건의 CEO 제이미 다이먼은 "비트코인은 사기다."
라고 선언하였지요.

공학자의 장난감 비트코인

정재승 교수처럼 정 반대 입장에 서서
완전히 다른 결론을 내리는 사람들도 많습니다.
애플공동창업자 스티브 워즈니악은
"비트코인은 금이나 달러보다도 낫다고 생각한다." 라고 했습니다.
라가르드 IMF총재는
"암호화폐가 기존 통화를 대체할 가능성이 매우 크다."라고 말했지요.

뭐가 맞는 것인지, 누가 옳은 것인지 헷갈립니다.
왜 그럴까요?
둘 다 맞기 때문입니다.

한 쪽은 새로운 기술이, 실익은 없고, 사용하기는 어색하고,
불편하기만 한, 구체적 현실을 이야기 합니다.
다른 한 편은 그 새로운 것이 앞으로 어떻게 세상을 이롭게 할 것인가, 가능성, 즉 추상적인 부분을 이야기 하지요.

현실에 발을 딛고 보는 입장에서는,
처음 보는 것이 신기하기는 하지만,
쓰기에 편리하지도 않고, 부작용만 보이기 때문에,
"쓸모없다." 라고 말 하는 것입니다.
가령, 너무 느리다. 1초당 거래 7개 밖에 못 한다.
또, 가치가 너무 빨리 변해서 가치의 척도를 제공하지 못 한다
등 등
그래서 통화는커녕, 화폐 역할도 못 한다는 것입니다.

혁신을 지속해온 EECS공학

미래응용을 보는 입장에서는,
현재는 제약이 많지만,
어디에 그 기술이 쓰일 수 있는 지 생각해보고,
미래를 앞당겨 현실로 만들려고 노력합니다.
전 세계의 과학기술자들과 경쟁을 하며 기술을 개발해온 공학자 입장에서는
위와 같이 “느리다,” “빨리 변한다” 와 같은 불평은
시간이 너무 쉽게 해결할 수 있는 단순한 문제입니다.

저는 90년대에 박사학위를 했습니다.
무선이동통신이 미래기술로 주목 받을 때 였습니다.
제가 97년에 논문을 발표하러 학회에 갔습니다.
미래연구 방향을 제시하는 패널토론에서,
학계의 원로가 실시간 비데오 이동통신 연구의 필요성을 역설하였습니다.
그 때 저의 머릿속에 든 생각입니다.

야. 무슨, 음성통화도 어려운 판에 실시간 화상 통화냐.
연구비 따 낼려고, 논문 게제 하려고 비약이 너무 심하다.
그런 게 개발 되었다 쳐도, 얼마나 비쌀 것이며,
필요한 사람이 몇 이나 되겠냐,
경제성 제로다, 등등을 생각 했습니다.
오늘날 인터넷, 핸드폰 시스템을 보십시오.
예전에는 전부 말도 안 되고, 상상도 못 했던 것들 입니다.

Bitcoin 혁신!

암호화폐인 비트코인은 현재로서는,
국경을 초월한 송금수단 정도로만 쓰이고 있는 게 사실입니다.
불법증여, 세금탈루, 마약거래 등 음성적 사용 위험성도 큽니다.

그러나 기술의 부작용은 추적기술 개발로 막을 수 있습니다.
기술의 오남용은 법과 제도의 운용으로 퇴치할 수 있습니다.
또한 잘못된 투자행위와 시장과열은, 투자 위험성을 알리고
교육하는 것을 통해 가라앉혀야 할 부분입니다.
제 2세대, 제 3세대 코인시스템 개발이 빠릅니다.
처리속도와 불법거래 추적기술이 개발되고 있으며,
비트코인의 문제점이 개선되고 있습니다.

암호화폐 기술은
누가 돈 들여 키우지 않았는데도, 생겨 난지 10년도 안 돼서,
지갑을 사용하는 사람의 숫자가 전 세계에서 2천5백만명에 육박하였고,
시장가치를 인정받아 높은 값에 거래되는 혁신입니다.

인간 상호 작용과 교류범위 확대

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.

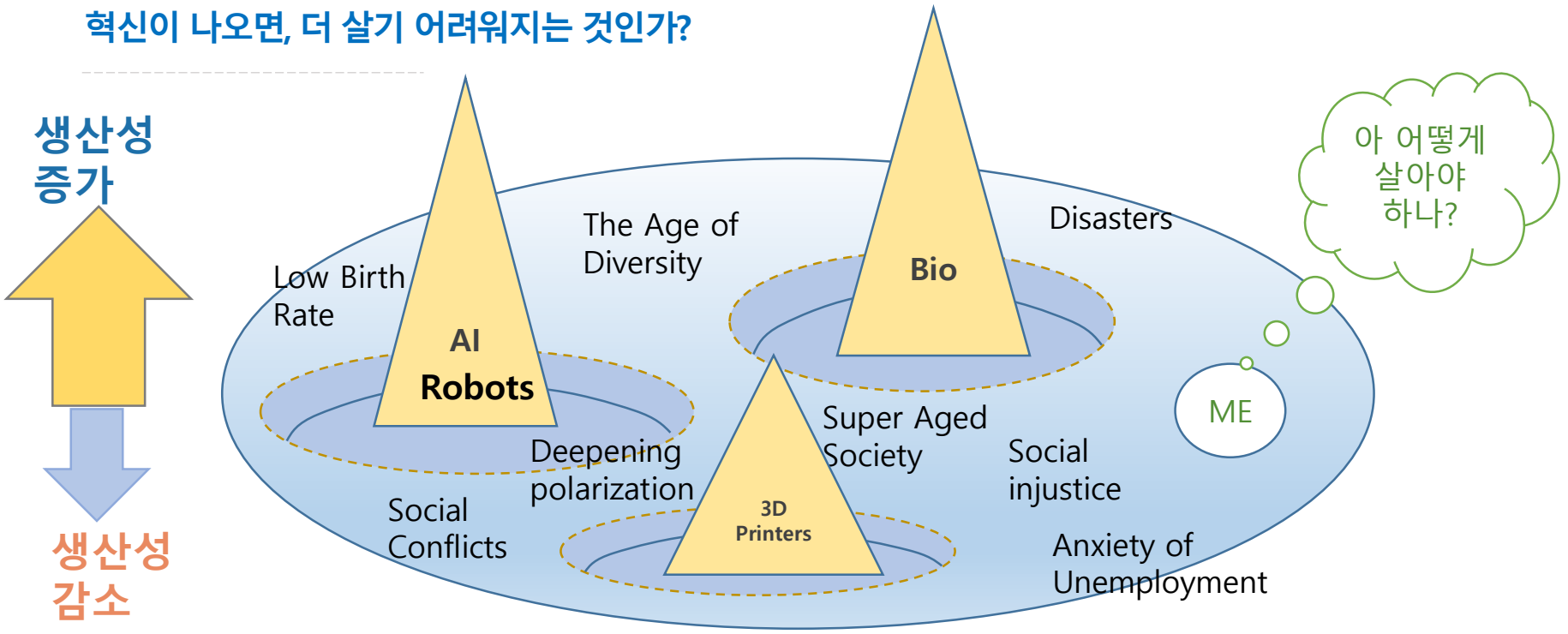
연결하는 것이 창의성입니다.

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

Why did I start to study blockchain?

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!**

4차 산업혁명은 정신 개혁운동이다!

기술혁신은 좋은 것이다. 혁신기술은 생산성은 높이고 비용은 낮춘다.

그러나 혁신은 쉽지 않다. 실패의 반복이다.

혁신이 지속되는 사회를 건설하려면, 각자의 경험을 공유하고 개방해야 한다.

실패해도 다시 도전할 수 있도록 기회를 제공해야 한다.

개개인의 노력을 인정해주고 더불어 잘사는 **포용적 사회**를 만드는 것 이다.

대한민국의 과거 모습

소수엘리트
Closed
양극화
분절
불통
악순환
소유
불신
Pyramid

건강한 미래 사회 – 상호 보완적 협력

대한민국의 미래 모습

다수엘리트
Open
나눔
융합
소통
선순환
공유
협력
신뢰
분권
Decentralized

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.

Conclusion

블록체인의 가능성은 무궁무진

마켓에서 확인된 것은 bitcoin이나 Ethereum

새로운 영역 개척을 위해서는 여러 가지 실험을 해 봐야

여러 실험에는 막대한 예산과 인력 투입 필요

규제 연구 필요, 규제가 필요하나, 최소한에 그쳐야 산업 촉진

- 책임 형 투자 촉진
- 거래소 운영 및 ICO의 투명성 제고
- 치고 빠지고 가격 올리기 배제
- 수익에 대한 과세
- 과세 위한 실명제? 가 미치는 영향력 고려, 차선책 연구 필요

References

- 이흥노 교수 랩 블록체인페이지 https://infonet.gist.ac.kr/?page_id=6370
- 박창기, “블록체인과 4차 산업혁명,” e-biz forum @Samsung Economy Research Institute, March 16, 2017.
- Blockchain.net
- Bitcoin.org
- Coursera course on Crytocurrencies
- MIT Blockchain center
- Blockchain A beginner’s guide, Blockchain Hub
- Satosh Nakamoto’s Bitcoin white paper.
- 그 외