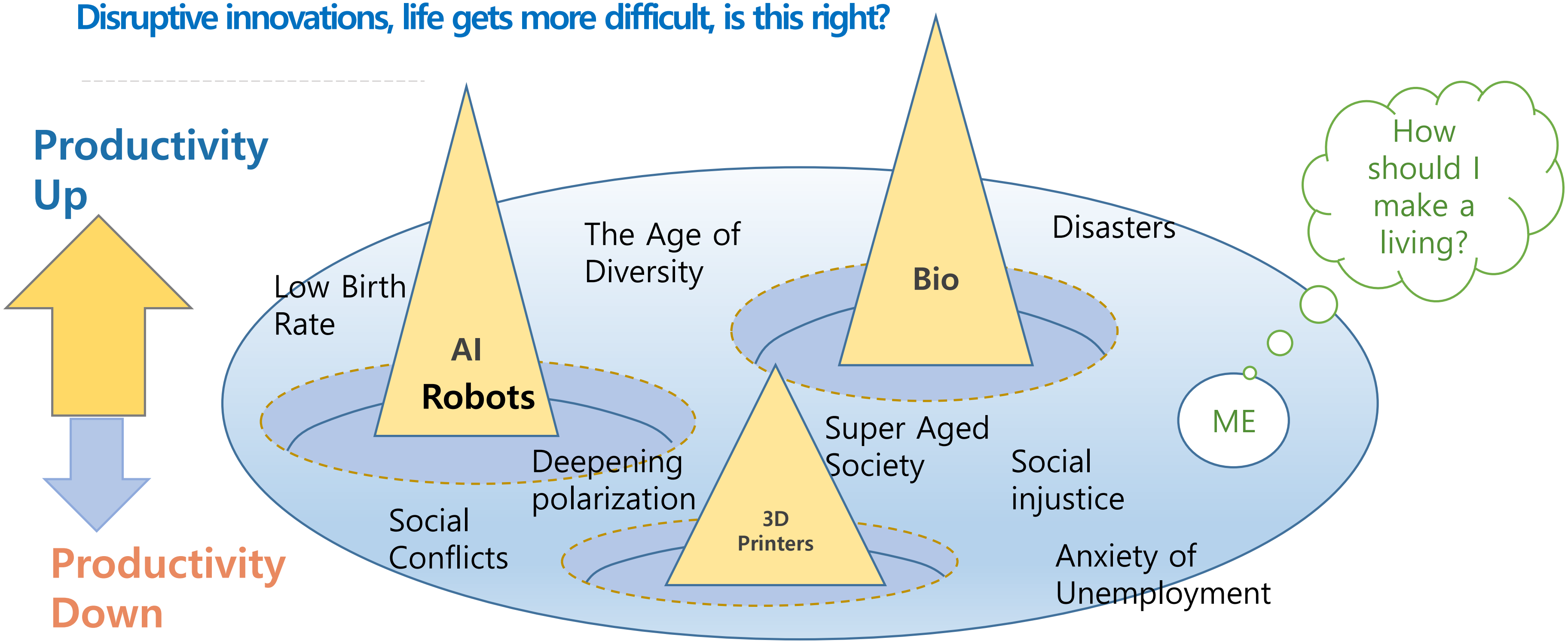
Blockchain and Its Applications

Heung-No Lee

March 5th 2018

Problem of disruptive tech~ W.T.A., inequality, no jobs

Disruptive innovations, life gets more difficult, is this right?



Major gain for a few innovators, gain for people at large, huge loss for people who lost the job!

Can we store the proofs of our usual work within blockchain such as programs, copyright, honest work in work places, and get compensated later on?
Can we make the society more responsive and cooperative using cryto trust?

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!

Lecture Materials

- Please use it unaltered.
  - Do not distribute widely without my consent.
  - Use it only for lecture notes in this course.
  - I wish to put them in the course web-site later on with some polishing done.

- When referencing a certain material in the lecture, please acknowledge it by giving the following citation note in your writing

Heung-No Lee, "Blockchain and its Applications,"

2018 Spring Semester Lecture Note.

Lecture Materials

- My lecture notes, distributed in e-mail in pdf files
- Lab homepage
  - Blockchain homepage https://infonet.gist.ac.kr/?page_id=6370
  - Class page in Facebook

- References
  - The bitcoin white paper by Satosh Nakamoto
  - The Ethereum white paper by Vitalik Buterin
  - Blockchain—a beginners guide, BlockchainHub, http://blockchainhub.net
  - The ever-growing list of published IEEE/ACM papers
  - Andreas M. Antonopoulos, "Mastering Bitcoin," O'Reilly, 2014. Note that the book is available at Github.
  - Melanie Swan, "Blockchain, blueprint for a new economy, 2015.
  - Github and other open sources https://github.com/.

Motivation

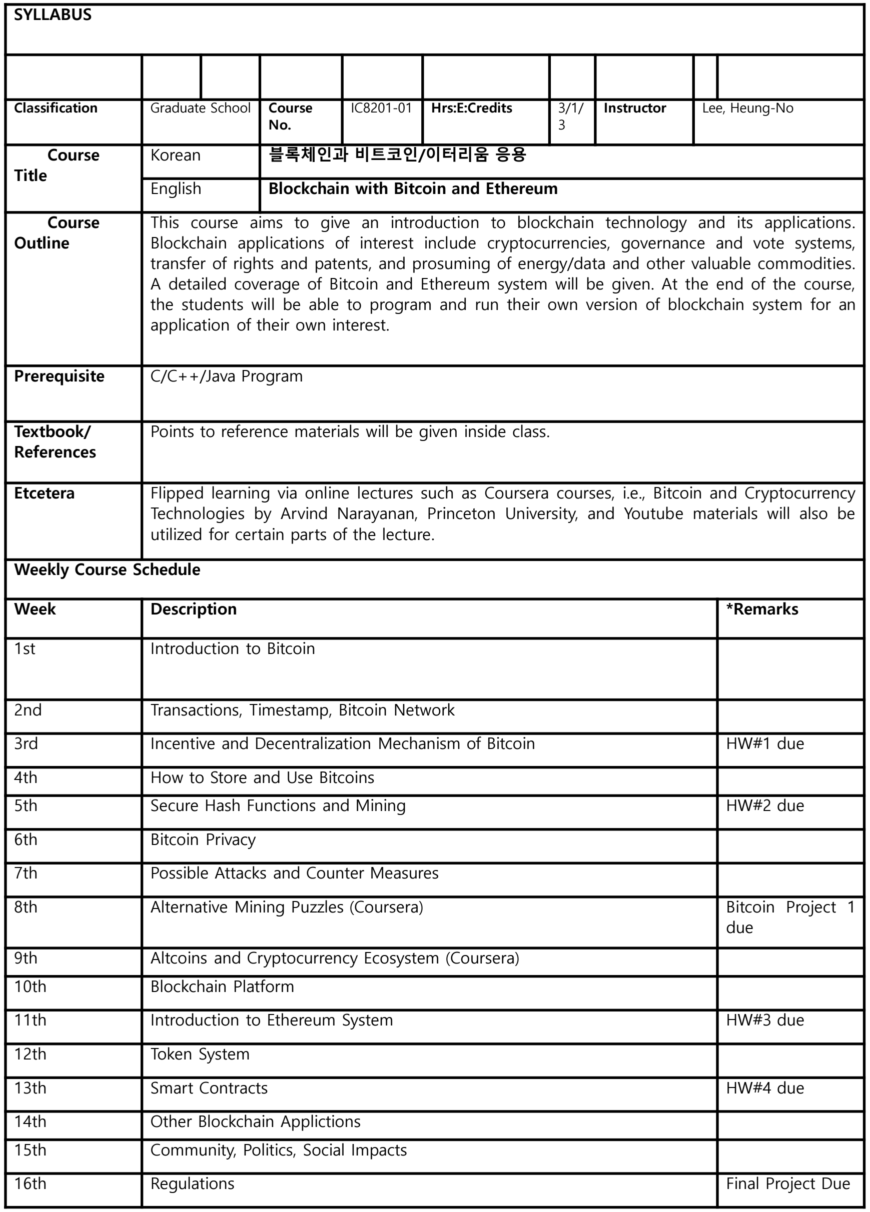
- Mega trends in the 4th industrial era?
  - Digital transformation, Internet of things, Big data,
  - Sharing economy, Unbundling of Centralized Authorities, Decentralized
  - Zero-marginal cost society, Small precision products, Prosumers

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

- Bitcoin and its blockchain
- Ethereum & smart contracts
- Other altcoins

Course Objectives

- Comprehension of cryptocurrency concepts
- Understand the importance of blockchain technology
- Understand the bitcoin network
- Bitcoin transactions validated by miners
- Create and use bitcoin account effectively
- Understand Ethereum blockchain
- Deploy your own blockchain and see operation of your chains
- Discuss the compelling use-cases



SYLLABUS

Classification	Graduate School	**Course No.**	IC8201-01	**Hrs:E:Credits**	3/1/3	**Instructor**	Lee, Heung-No
Course Title	Korean	**블록체인과 비트코인/이터리움 응용**					
	English	**Blockchain with Bitcoin and Ethereum**					
Course Outline	This course aims to give an introduction to blockchain technology and its applications. Blockchain applications of interest include cryptocurrencies, governance and vote systems, transfer of rights and patents, and prosuming of energy/data and other valuable commodities. A detailed coverage of Bitcoin and Ethereum system will be given. At the end of the course, the students will be able to program and run their own version of blockchain system for an application of their own interest.						
Prerequisite	C/C++/Java Program						
Textbook/ References	Points to reference materials will be given inside class.						
Etcetera	Flipped learning via online lectures such as Coursera courses, i.e., Bitcoin and Cryptocurrency Technologies by Arvind Narayanan, Princeton University, and Youtube materials will also be utilized for certain parts of the lecture.						

Weekly Course Schedule

Week	**Description**	***Remarks**
1st	Introduction to Bitcoin	
2nd	Transactions, Timestamp, Bitcoin Network	
3rd	Incentive and Decentralization Mechanism of Bitcoin	HW#1 due
4th	How to Store and Use Bitcoins	
5th	Secure Hash Functions and Mining	HW#2 due
6th	Bitcoin Privacy	
7th	Possible Attacks and Counter Measures	
8th	Alternative Mining Puzzles (Coursera)	Bitcoin Project 1 due
9th	Altcoins and Cryptocurrency Ecosystem (Coursera)	
10th	Blockchain Platform	
11th	Introduction to Ethereum System	HW#3 due
12th	Token System	
13th	Smart Contracts	HW#4 due
14th	Other Blockchain Applictions	
15th	Community, Politics, Social Impacts	
16th	Regulations	Final Project Due

Who should take this course?

- This course is designed to give students the insights and hands-on programming knowledge to see the opportunities and innovations the blockchain technology will bring in to the society. In the world today, we often feel that innovation is not enough. As innovation continues, the lives of ordinary people have worsened, while small group of technological elites absorbs the majority of the social wealth created by new technologies. Needed are the abled students who are responsive to these problems, such as underemployment problems, income inequality, social barriers to opportunities, and disappearance of blue collar jobs. Blockchain is envisioned to be a solution to these inequalities problems of the market driven society. More harmonious and inclusive society can be built with creative use of the blockchain technology.

GIST Students

- Grades

- Attendances
- 2 Quizzes (10 minutes)
- Four HWs
- 1 Midterm
- 1 course project and presentation by student group (up to 2 students)
- Plan to invite well known speakers and investors

4th Industrial Revolution

2017

The 4th Industrial Revolution and Our Strategy for a Better World

Director of GIST Institute Heung-No Lee

IEEE VTS APWCS 2017. 8. 24 Thursday Incheon National University
http://apwcs2017.incheon.ac.kr/

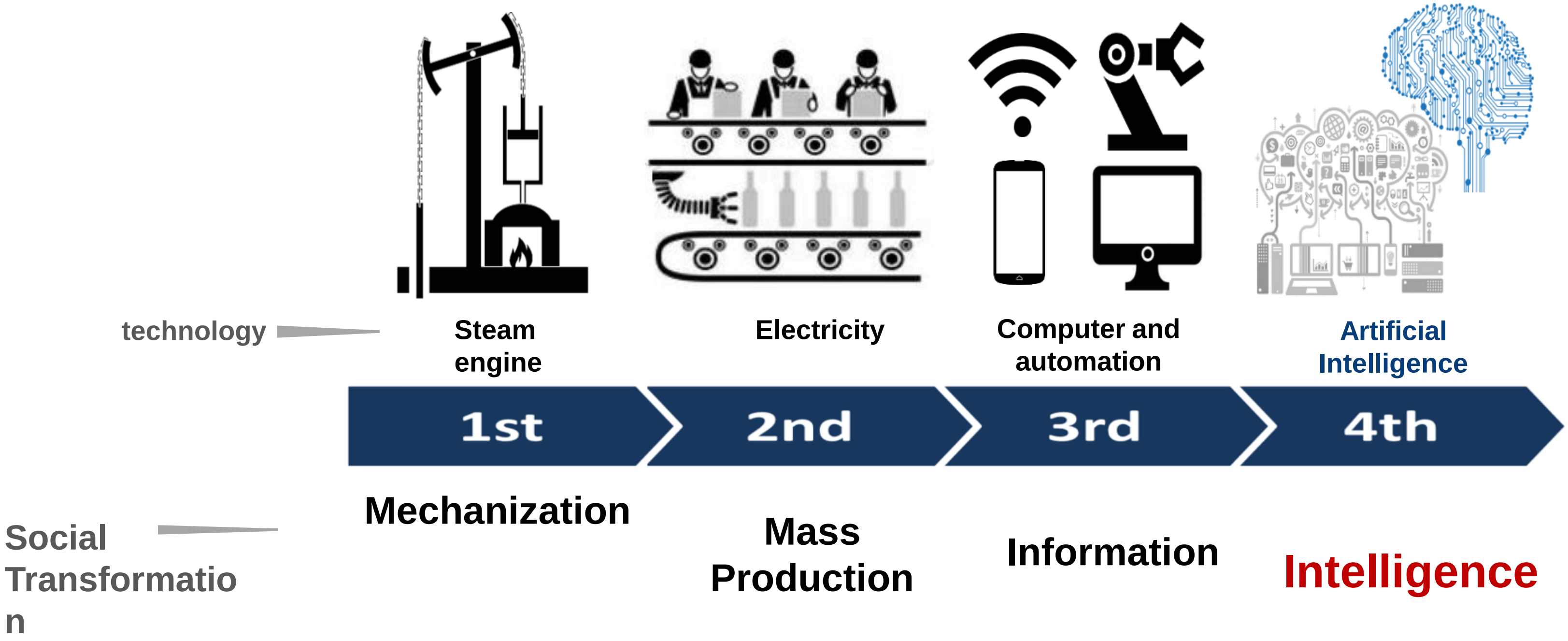
Abstract

The 4th Industrial Revolution was the main topic of discussion at the World Economic Forum (WEF) in 2016. Dr. **Klaus Schwab, the chairman of the WEF, has named it with an intention to describe how fast the world is changing driven by the so called disruptive technological advances and how deeply the lives of people are forced to alteration.** These waves of changes will hit every region around the globe and everyone will be forced to change. Words of warning go viral such that an entity leading such changes will thrive while the others who are not prepared for them will perish. This has created a Tsunami of discussions at least within Korea where the winning performance of AlphaGo Spring 2016 has proven how powerful today's breakthrough technology could be. The impact is indisputable. Almost everyone agrees immediately. Even an ordinary people can grab the importance of preparedness right away. While some are awed by them, others perceive opening of enormously many new opportunities that advances of new technologies will take the human to the next level. As we study more, visions with concrete action plans are being realized within leading nations such as Germany and U.S.A. with revolutionary outcomes being sprung up. For example, we see how Germans has renovated its old manufacturing industry under the theme of Smart Factory, a revolutionary idea incubated carefully, and executed for the last decade, by Dr. Zulke who coined the term **Industry 4.0**. The storm of discussions to date is to provide us with a chance to carefully thought out our future and prepare us to make the world a better place to live in. When we work together to shape out a desirable future, such a future will come true as reality someday. In this talk, **I aim to discuss** the narrative of 4th industrial revolution, showcase a selected set of fundamental technologies and thoughts deriving the effort, and discuss **how** they can be utilized **to make a better future for all.**

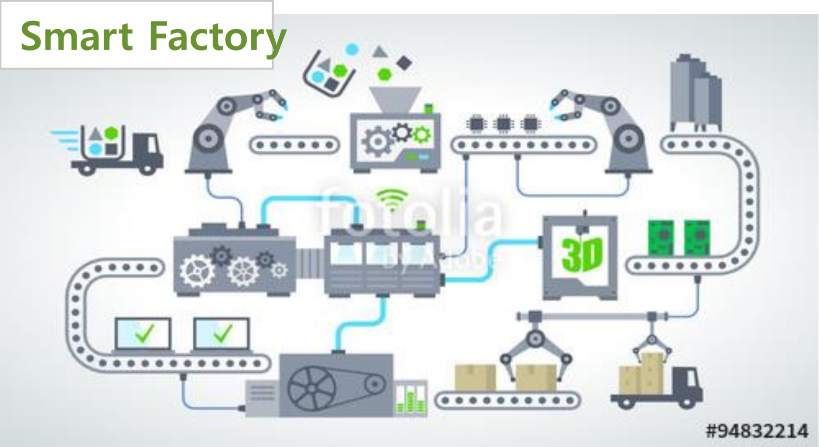
The 4th Industrial Revolution

The advent of intelligence society

Advances in technology lead the transformation of society to the next level!
Why has the 4th IR story made a big hit in Korea?
AlphaGo or a fear of losing jobs?

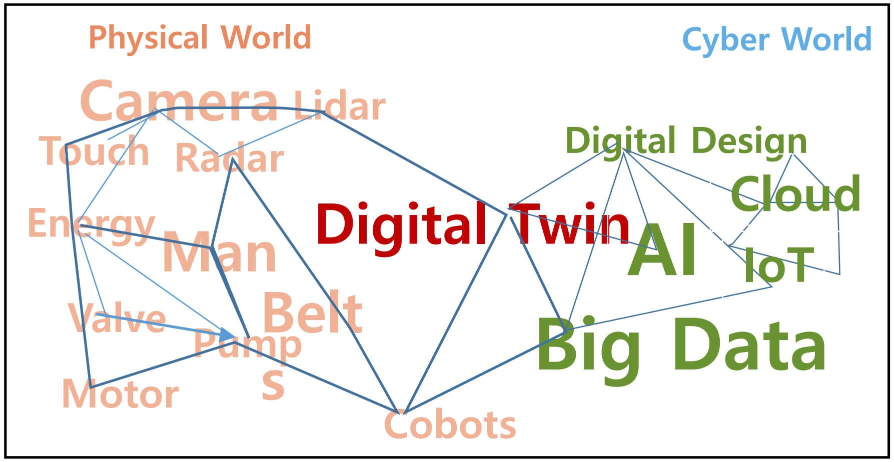


Hannover Messe 2017



Smart Factory

Production on Demand



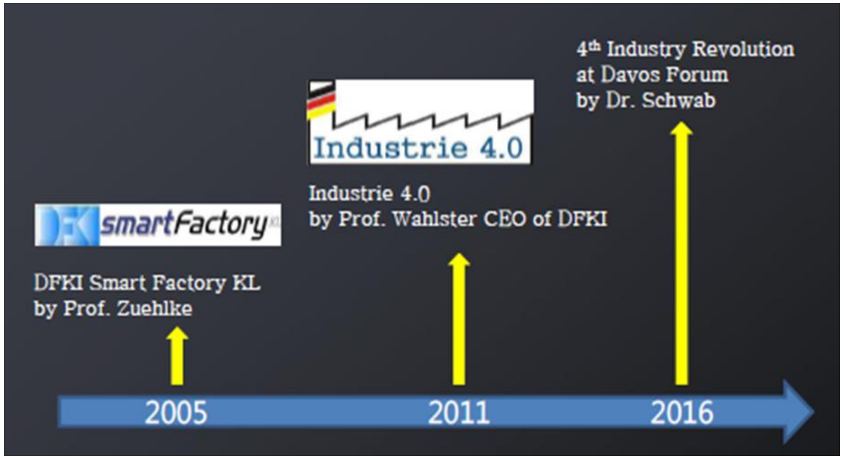
Physical World

Cyber World

Digital Factory
R.T. Surveillance
Prediction
Value creation
On demand
Precision
Productivity up

Industry 4.0 of Germany

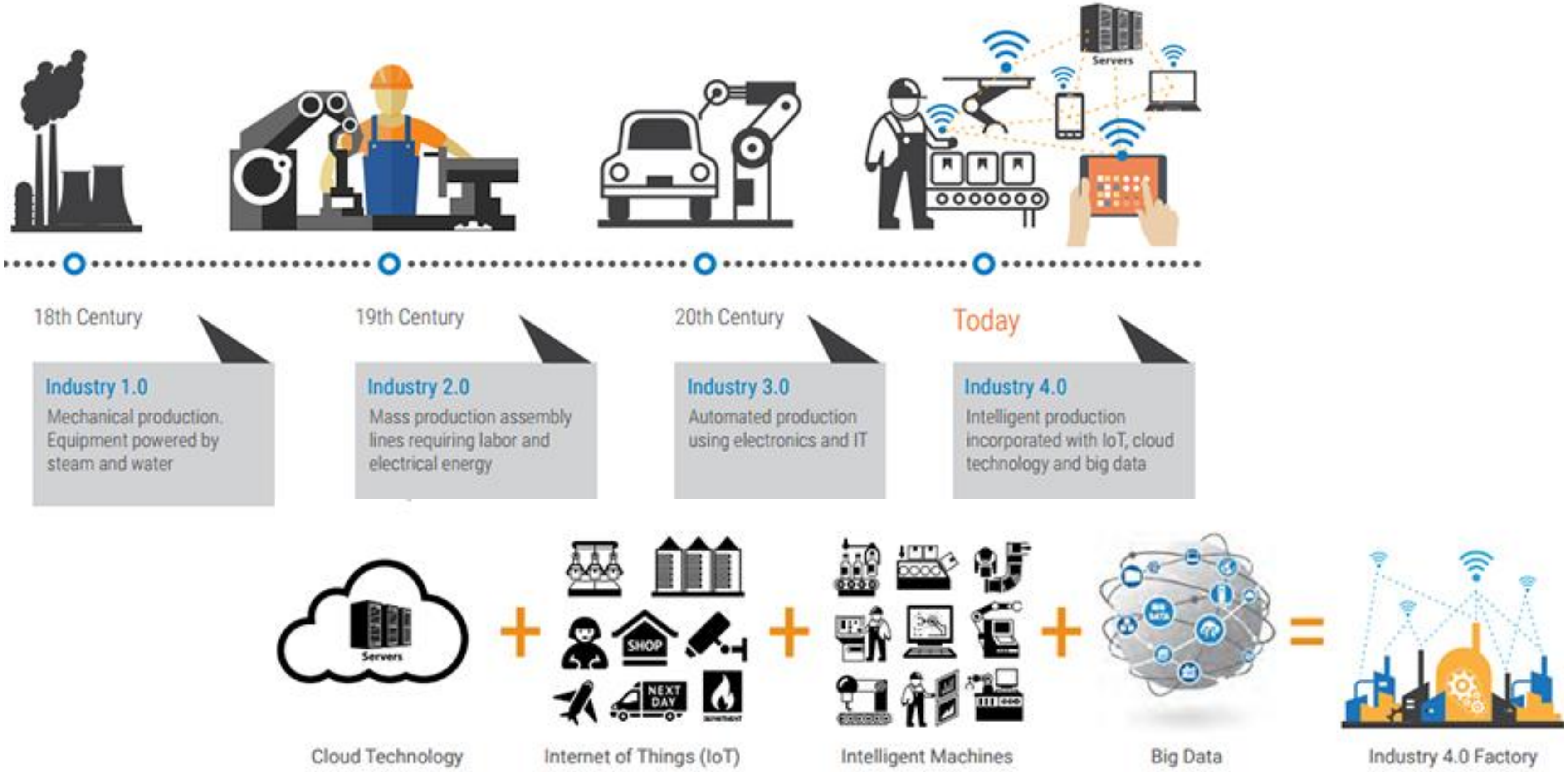
- 2005, DFKI Smart Factory” by Prof. Zuehlke
- 2011, Industry 4.0 termed at Hannover Fair
- 2012, in Gov. 10 Strategic High Techs
- 2013, 200M E Funding on CPS & IoT R&D
- 2015, Platform Industry 4.0



- Germany ~ the world leader in manufacturing industry
- GFG, aims to upgrade manuf. ind. with ICT, cloud computing, Robots & AI
- Able to keep manufacturing sites in Germany, revolutionizing the manufacturing ind.

DFKI: German Research Center for AI

Industry 4.0



18th Century

Industry 1.0
Mechanical production. Equipment powered by steam and water

19th Century

Industry 2.0
Mass production assembly lines requiring labor and electrical energy

20th Century

Industry 3.0
Automated production using electronics and IT

Today

Industry 4.0
Intelligent production incorporated with IoT, cloud technology and big data

Cloud Technology

Internet of Things (IoT)

Intelligent Machines

Big Data

Industry 4.0 Factory

Industry 4.0 and 4th Industrial Revolution

What's the difference?

4th IR was named by Klaus Schwab as the theme of WEF 2016.

Schwab aims to describe rapid techno-socio-economic changes erupting in the industrialized world.

Definition: Making Modern System Intelligent. I will explain in the following several sentences:

- In a factory, motors, valves, belts, controllers, energy sources, mechanical robots, and etc.
- (*IoT*) These things can be digitalized by attaching a digital sensor to each of them.
- (*Digital twin*) A digital twin is created for each thing.
- (*Optimization*) A factory with digital twin can be optimized in a computer design.
- (*Big Data*) Digital data can be gathered, stored, and used to monitor the status of factory.
- (*Prediction*) Data stored up to present can be used to figure out a trend or predict the future.
- (*Value creation*) New value-chains, BMs, created by discovering new patterns cultivated from the stored data.
- (Extending "factory" to other items is 4th IR) The *smart factory* here can be extended to *smart home*, *smart school*, *smart city*, *smart energy*, *smart farm*, *smart hospital*, and etc.

Change or Disappear?

Silicon Valley

2017.01.30.
@Singularity Univ.

d.
Institute of Design at Stanford
With appreciation for their contributions to the d.school and the renovation of this building
Hasso Plattner Foundation
Brit and Alexander d'Arbeloff
Michael J. Levinthal
The Mericos Foundation
THE ONLY WAY TO DO IT IS TO DO IT.

2017.01.27.
@Institute of Design at Stanford

2017.01.31.
@Google Inc.

2017.01.27.
@K-12 Lab 세미나

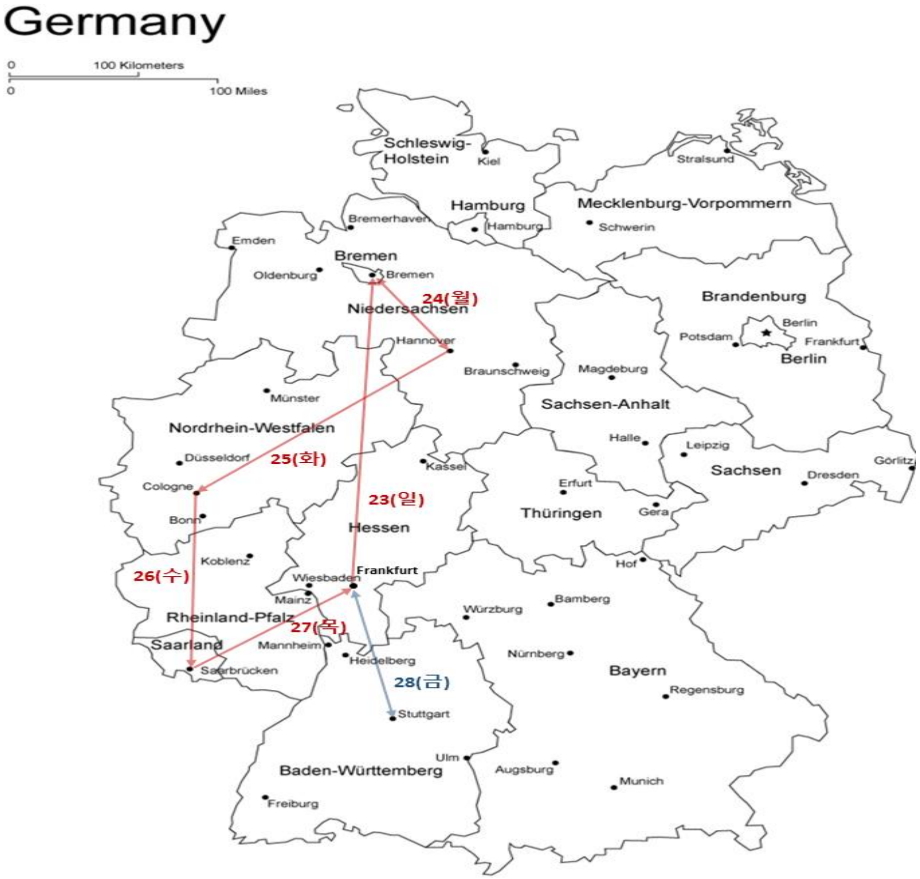
혁신의 상징

Silicon Valley

Stanford

Berkeley

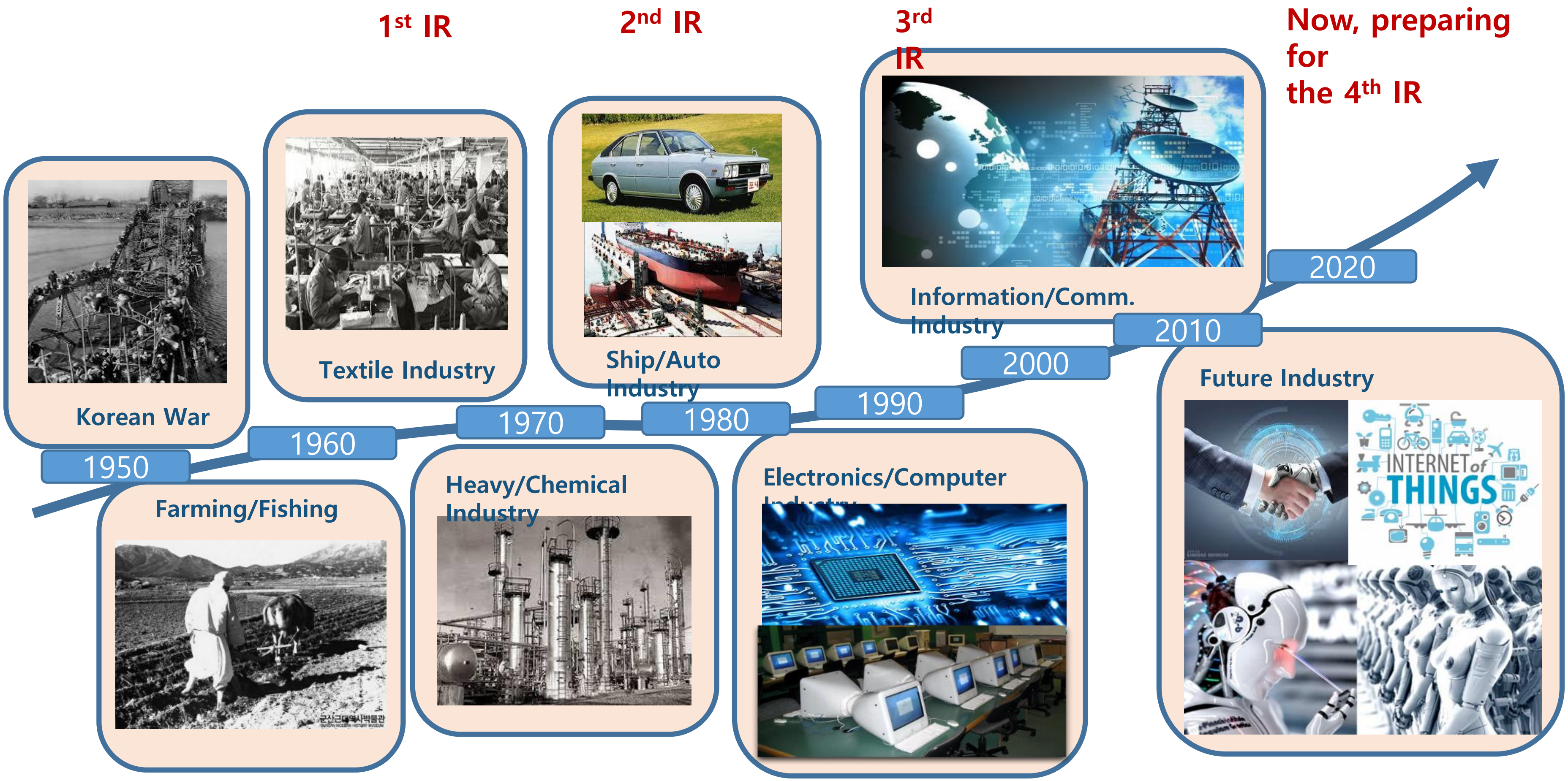
Visit to Hannover Messe 2017



Völklingen Ironworks
UNESCO World Cultural Heritage Site
Once largest steel prod. site, closed at 1986

"Change or Disappear"

Korea’s Impressive Growth!



1st IR

2nd IR

3rd IR

Now, preparing for the 4th IR

1950

Korean War

Farming/Fishing

1960

Textile Industry

1970

Heavy/Chemical Industry

Ship/Auto Industry

1980

Electronics/Computer Industry

1990

2000

Information/Comm. Industry

2010

Future Industry

2020

Again, it's not tech adv. that is bad.

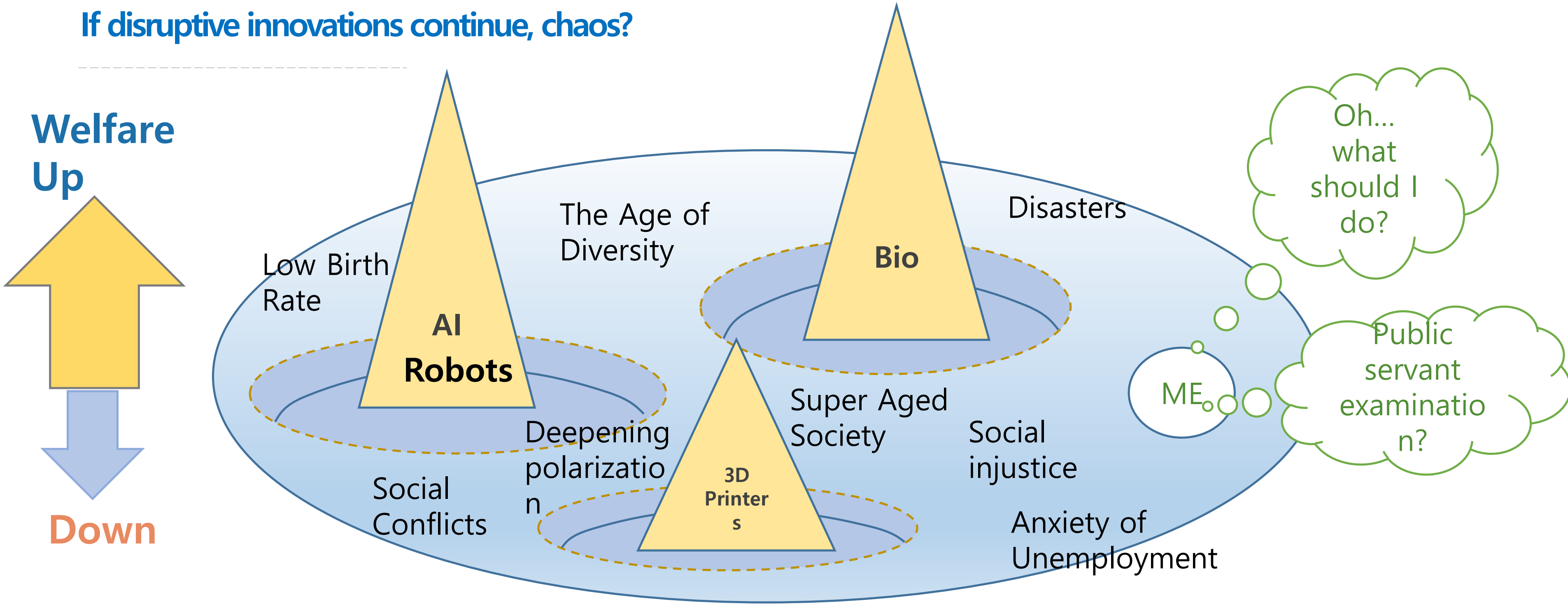
1950

2010

What is problem then?

Nature of Disruptive Innovations

If disruptive innovations continue, chaos?



Huge gain for few elite groups, gain for people at large, loss for displaced

What to do?

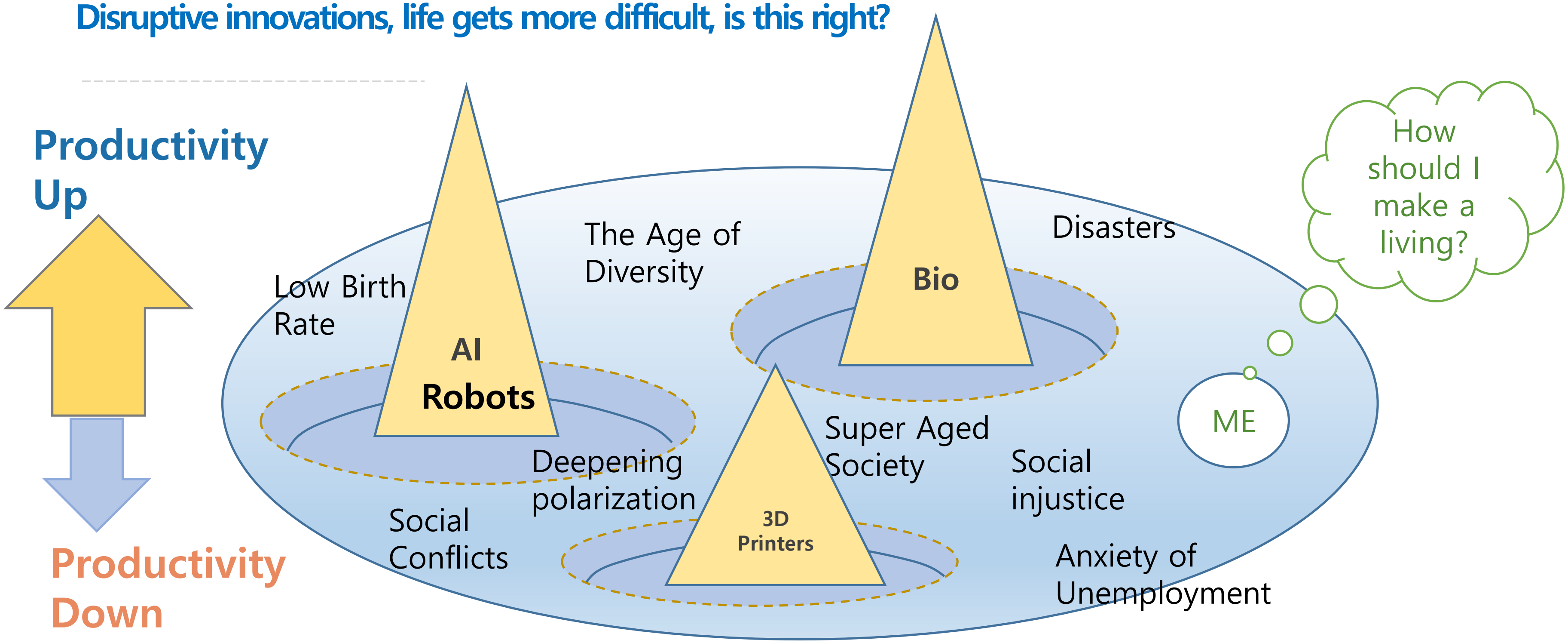
1. Sharing, Giving Society

2. Growth with continued Innovation

Why did I start to study blockchain?

Problem of disruptive tech~ W.T.A., inequality, no jobs

Disruptive innovations, life gets more difficult, is this right?



Major gain for a few innovators, gain for people at large, huge loss for people who lost the job!

Can we store the proofs of our usual work within blockchain such as programs, copyright, honest work in work places, and get compensated later on?
Can we make the society more responsive and cooperative using cryto trust?

Trust Enabled by Peers

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.

Using peer-to-peer energy-trading platforms to incentivize prosumers to form federated power plants

•Thomas Morstyn, Niall Farrell, Sarah J. Darby & Malcolm D. McCulloch

•*Nature Energy* **volume 3**, pages94–101 (2018)
•doi:10.1038/s41560-017-0075-y

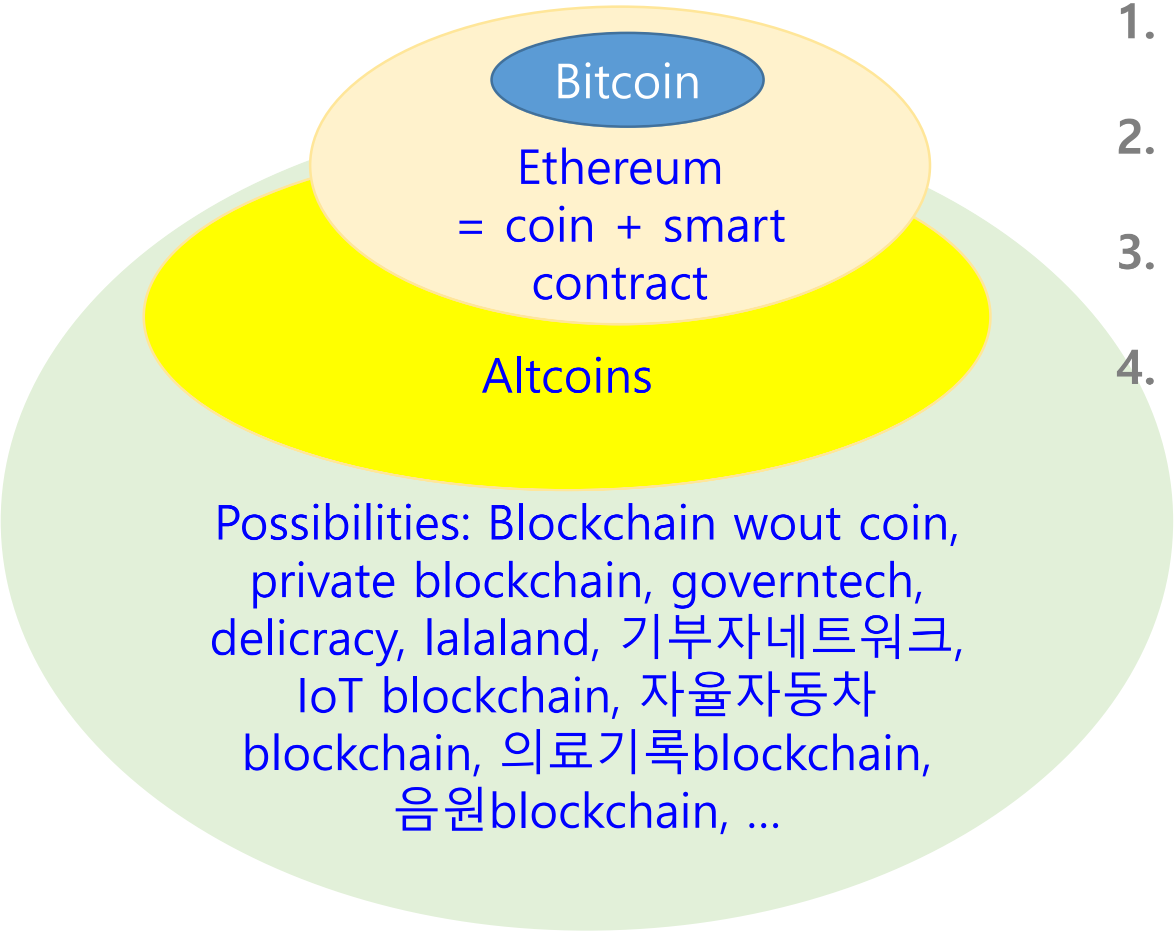
- **Abstract**
- Power networks are undergoing a fundamental transition, with traditionally passive consumers becoming ‘prosumers’ — proactive consumers with distributed energy resources, actively managing their consumption, production and storage of energy. A key question that remains unresolved is: how can we incentivize coordination between vast numbers of distributed energy resources, each with different owners and characteristics? Virtual power plants and peer-to-peer (P2P) energy trading offer different sources of value to prosumers and the power network, and have been proposed as different potential structures for future prosumer electricity markets. In this Perspective, we argue they can be combined to capture the benefits of both. We thus propose the concept of the federated power plant, a virtual power plant formed through P2P transactions between self-organizing prosumers. This addresses social, institutional and economic issues faced by top-down strategies for coordinating virtual power plants, while unlocking additional value for P2P energy trading.

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

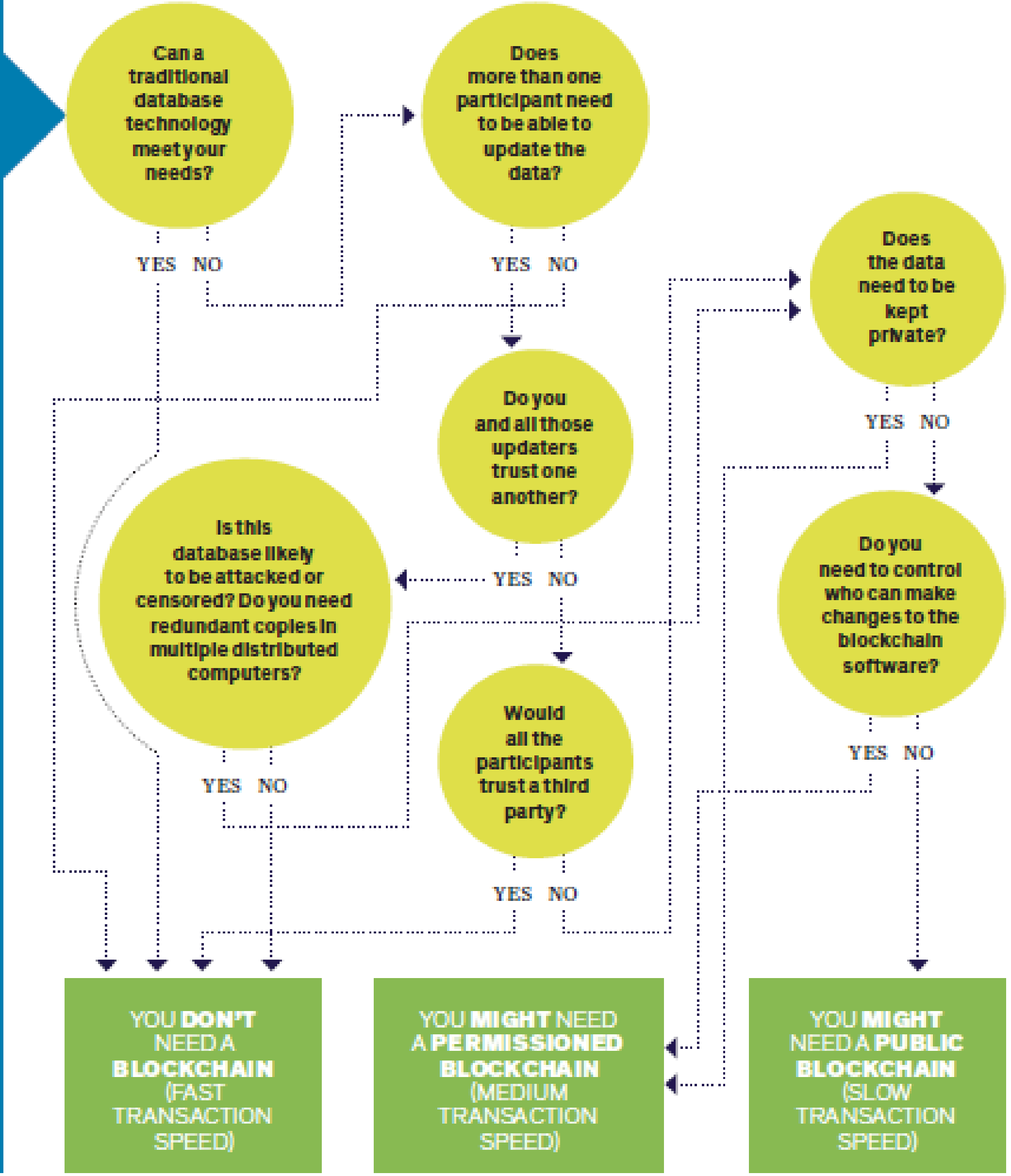

Bitcoin
Ethereum
= coin + smart
contract
Altcoins
Possibilities: Blockchain wout coin,
private blockchain, goverrntech,
delicracy, lalaland, 기부자네트워크,
IoT blockchain, 자율자동차
blockchain, 의료기록blockchain,
음원blockchain, ...

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 Blockchain!

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.



Can a traditional database technology meet your needs?

Does more than one participant need to be able to update the data?

Do you and all those updaters trust one another?

Is this database likely to be attacked or censored? Do you need redundant copies in multiple distributed computers?

Would all the participants trust a third party?

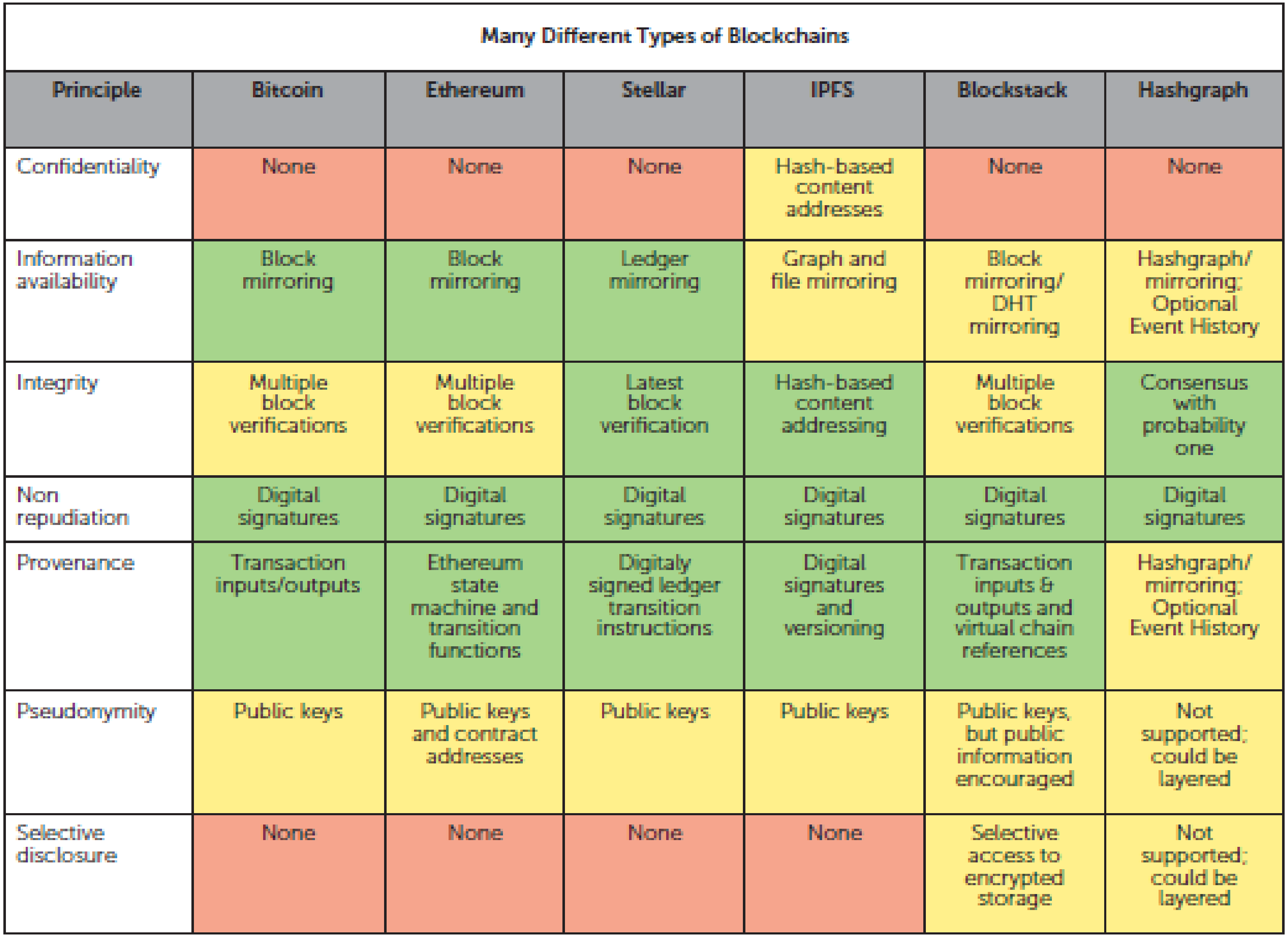
Does the data need to be kept private?

Do you need to control who can make changes to the blockchain software?

YOU **DON'T** NEED A **BLOCKCHAIN** (FAST TRANSACTION SPEED)

YOU **MIGHT** NEED A **PERMISSIONED BLOCKCHAIN** (MEDIUM TRANSACTION SPEED)

YOU **MIGHT** NEED A **PUBLIC BLOCKCHAIN** (SLOW TRANSACTION SPEED)



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 & Blockchain

- What if we share things temporarily not in use?
- When goods and services such as cars, houses, parking lots, cpu time, not in use are opened up and shared, owners and users can create a situation that both parties can be benefited.
- To such an end, reservation and paying fees shall be very important.
- Blockchain and Smart Contract can be used for reservations, and payments can be executed automatically. Trust based sharing economy can be made.
  - In the concept of Smart City, there is blockchain!

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

- Fortune. “SNR, Big data, IoT, AI Ventures unbundling big companies, Unbundling, Decentralization”
- Unbundling Media, European Bank, Honeywell, FedEx …
- 1st IR Machine labor, 2nd IR Electricity/Mass Production, 3rd IR Automation/Computers/Internet
- 4th IR, Cyber-Physical System, IoT/BigData/AI/Mobile, Decentralized Autonomous Organization(DAO)
- Disruptive unbundling, Dis-intermediation, Decentralized Autonomous Networked Organization(DANO), DANSociety

Unbundling

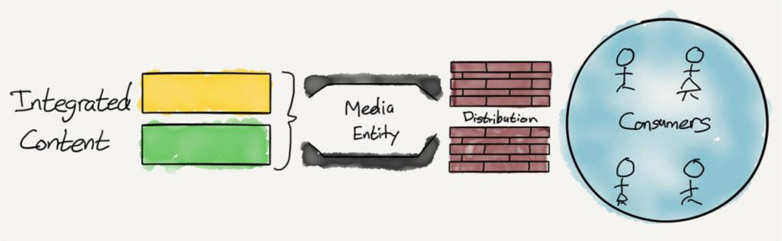
From Wikipedia, the free encyclopedia

- **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

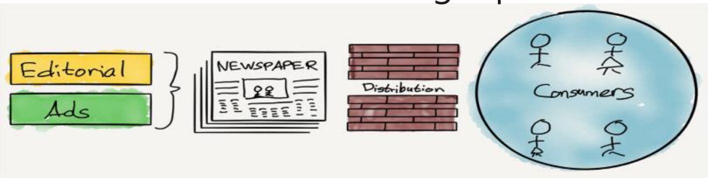
Ben Thompson

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

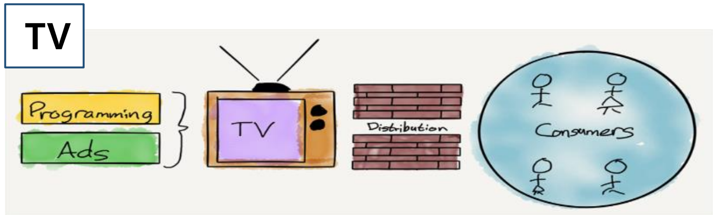


THE OLD MEDIA MODEL
Nearly all media in the pre-Internet era functioned under the same general model:
Note that there are two parts in this model when it comes to making money — distribution and then integration — and the order matters. Distribution required massive up-front investment, whether that 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:

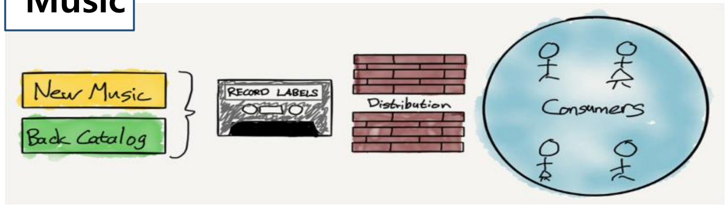
Print: Newspapers and magazines primarily made money by integrating editorial and advertisements into a single publication:



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

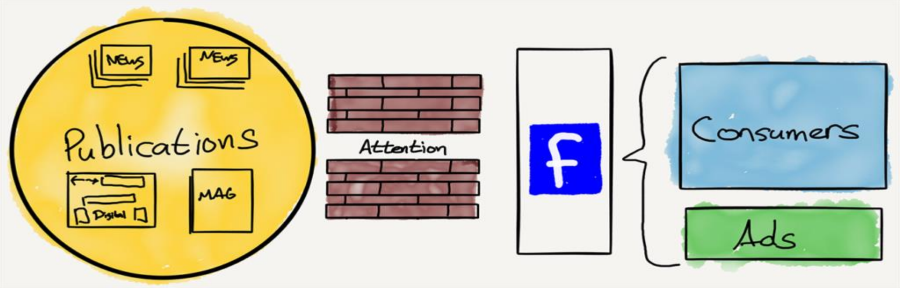
	ESPN	History channel
Sports lover	$10	$3
History lover	$3	$10

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

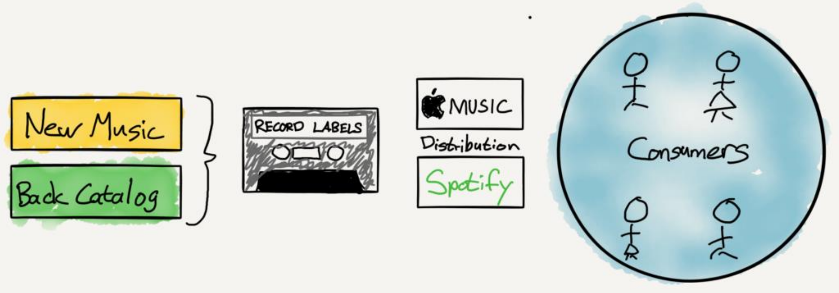
What happens, when distribution cost goes zero…

- 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 Cryptocurrency Forcast

- 1980 PC Windows
- 1995 Internet, Explorer
- 2005 Mobile, Android iOS
- 2015 WEF May Report Forcast, "27' 10% of World GDP in Cryptocurrency", "23' Nations taxing with cryptocurrency"
- 2016 Davos Forum, Big Data and Blockchain winners
- Korea GDP 1,400 BUSD 2015→ 1,800B 2027
  World GDP 80,000B 2015→ 100,000B 2027
- Cryptocurrency, 10B 2015, 10,000B 2027
  (0.01% → 10%, 1000x Growth)

Crypto currency market capitalization

March 2017

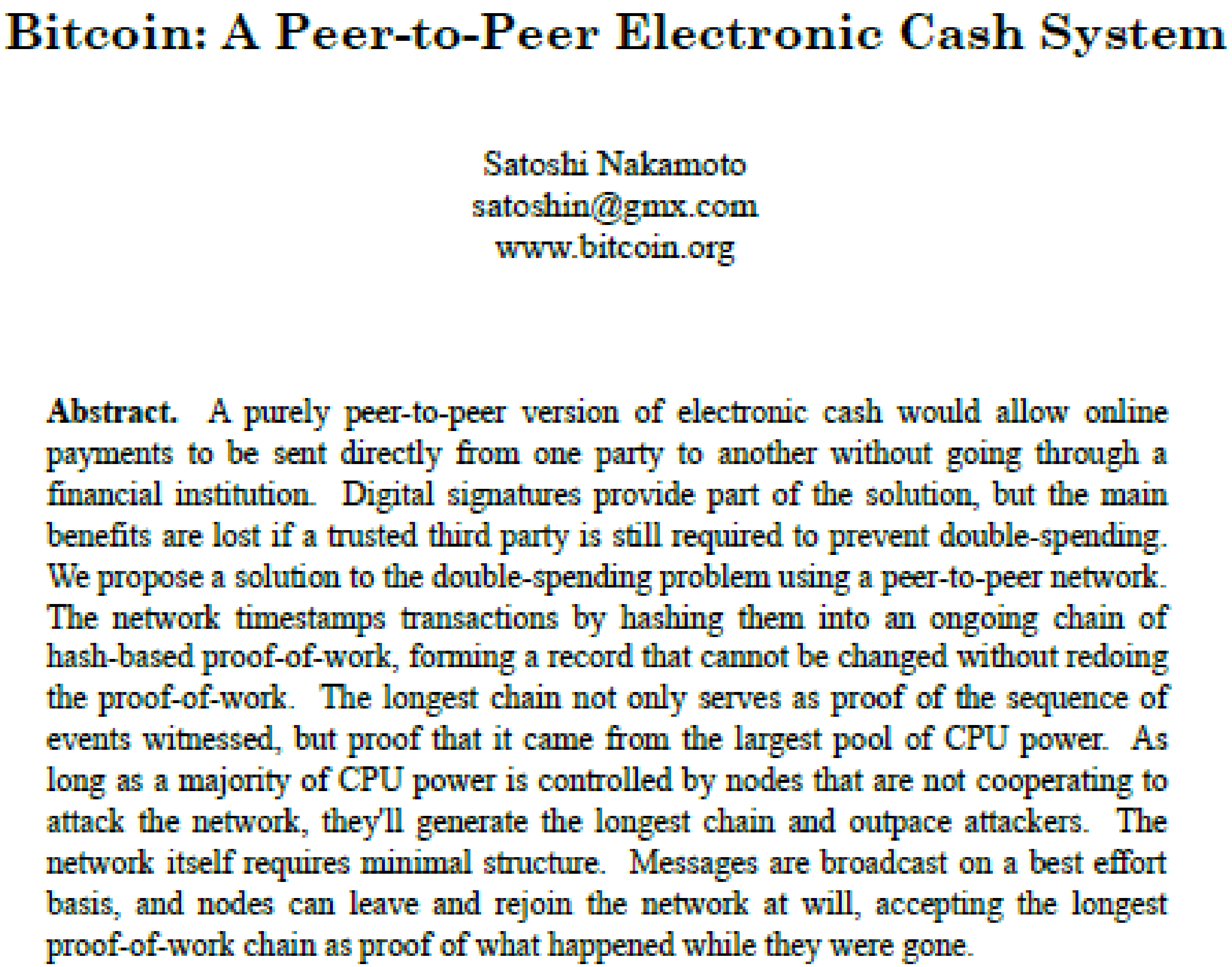
- Bitcoin 20B USD
- Ethereum 3B
- Dash 0.66B
- Monero 0.31B
- Ripple 0.24B
- Litecoin 0.21B
- Ethereum Classic 0.18B
- Augur 0.10B

Society with no fiat money and blockchain

- Sweden (Pub Transit, paying fees with money not accepted)
- Demark(enactment of a law in preparation not accepting money in retail stores—clothes/restaurants)
- Israel(Moneyless society promoted),
- China(Central bank, digital currency issuance planned)
- Korea(by 20' coinless society planned)
- Germany, England, Japan – Cryptocurrency is being accepted as money.

Bitcoin, what is it?

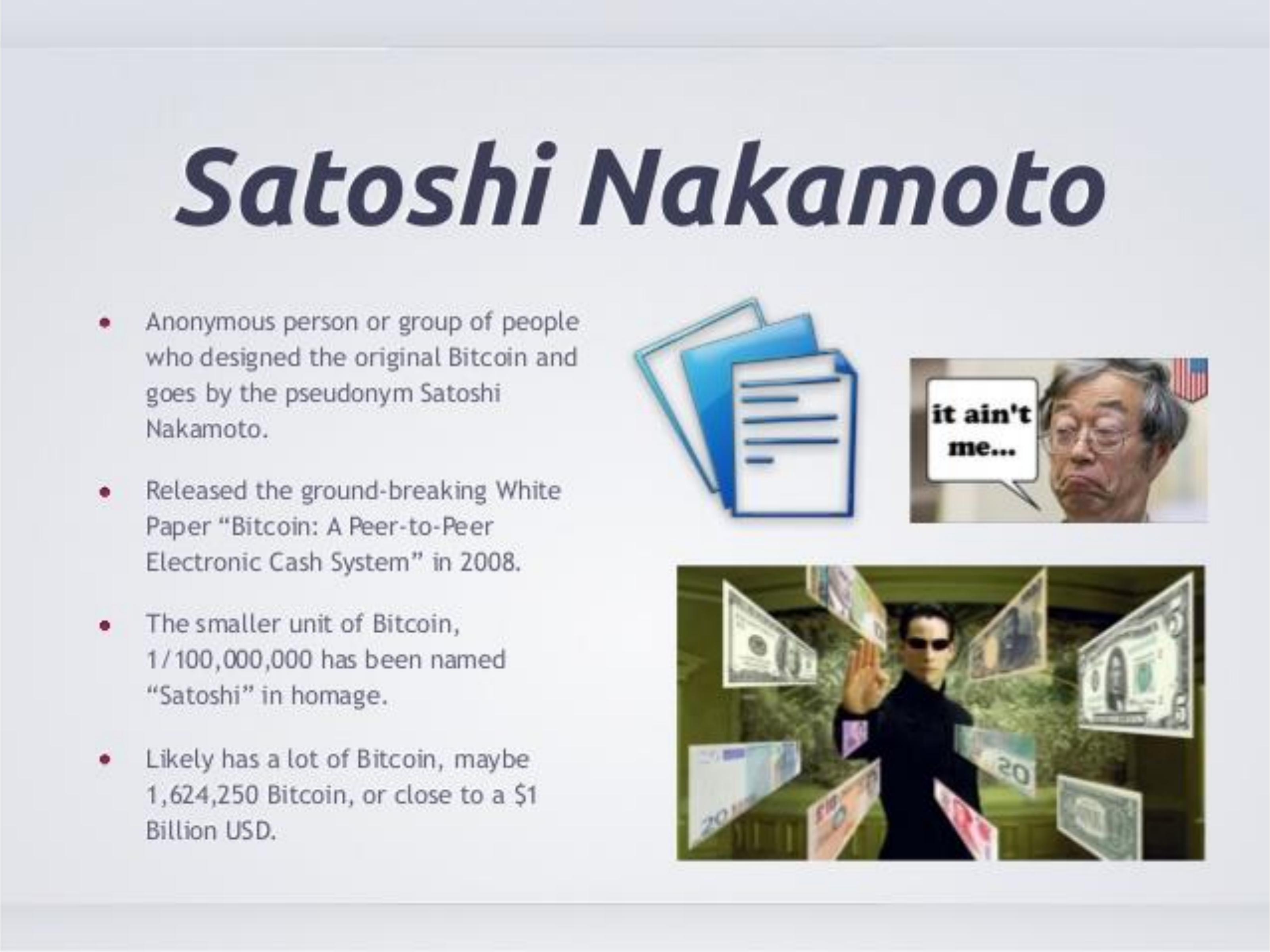
The first paper



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

Bitcoin is digital currency!

Currency works based on trust. You have the currency, then you can exchange it to get goods and services.

- **Today, money is simply numbers in our bank account. When these numbers is lowered in my account, the same amount of numbers appear in other account when I spend them.**

Value of a currency lies in a government who issues it and enforces any wrong uses.

- **Making Counterfeits are caught.**

Currency with high demands is valued high in the market.

Bitcoin has obtained the position of currency in the market without the involvement of a government.
Very high market value has been created for Bitcoin based on high demands.
This is a fact.
It is the reason why Bitcoin is important for us to study.
It is the first digital currency made it to such a level.
It is the invention of the humanity.

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.

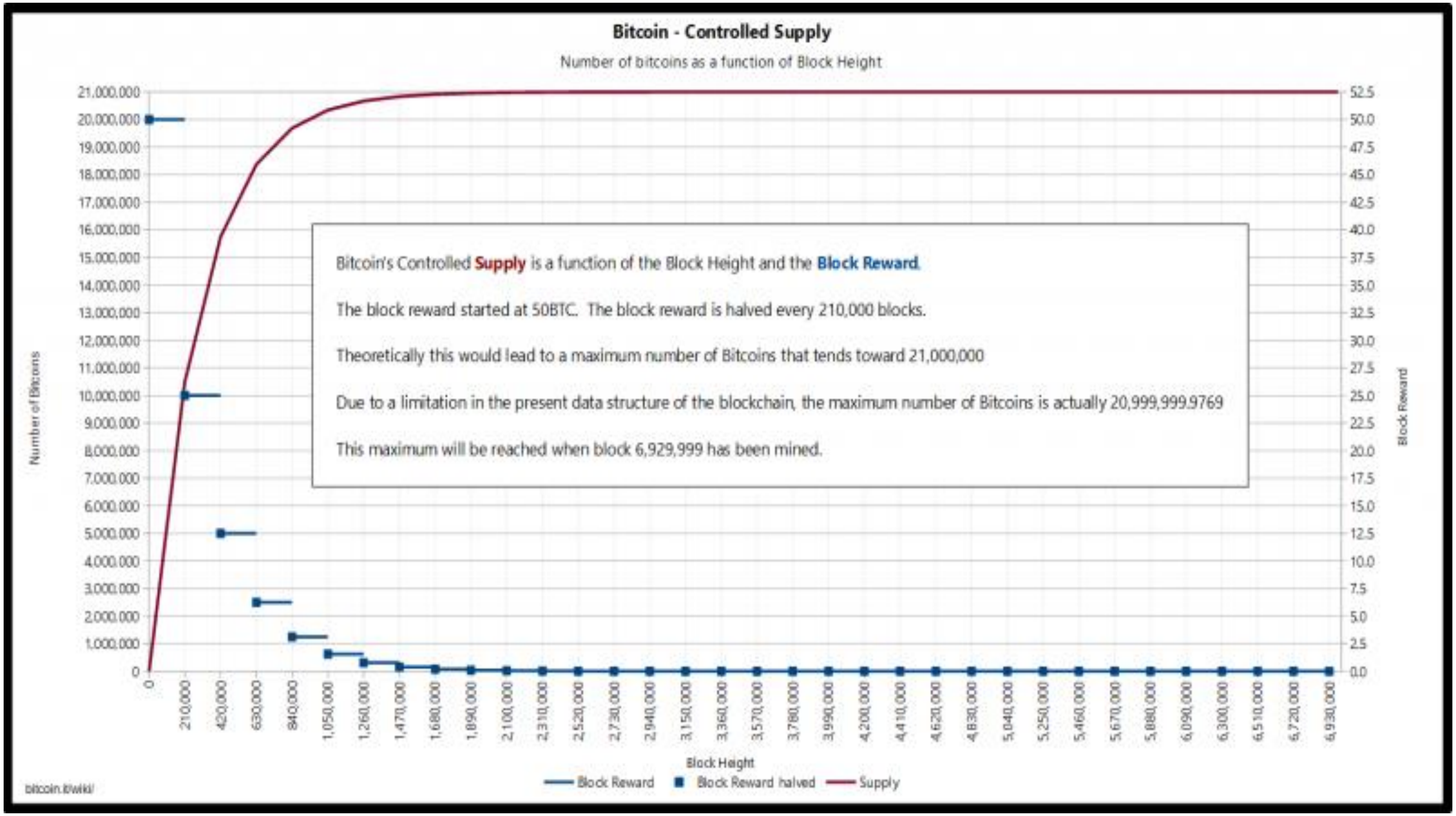
2015: Derivatives, Assets, Payments

- **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.

Bitcoin Issuance Schedule



Bitcoin - Controlled Supply

Number of bitcoins as a function of Block Height

Bitcoin's Controlled **Supply** is a function of the Block Height and the **Block Reward**.

The block reward started at 50BTC. The block reward is halved every 210,000 blocks.

Theoretically this would lead to a maximum number of Bitcoins that tends toward 21,000,000

Due to a limitation in the present data structure of the blockchain, the maximum number of Bitcoins is actually 20,999,999.9769

This maximum will be reached when block 6,929,999 has been mined.

bitcoin.it/wiki/

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%

Bitcoin

Bitcoin algorithm runs on a P2P network.
All computers in the network, cooperates and verifies the coin transaction.

It is designed to keep out faulty transactions such as unproven ownership and double spending.

This algorithm enables, a digital message such as “A gives B a single coin“ works as an in-person transfer of money if the message is verified, recorded and kept unaltered.

Without the involvement of a third party such as banks and middle man, anybody can open up a transaction with anyone in the internet.

How can such an invention be possible?

The answer was in fact very simple.

Namely, the content and time of a transaction are recorded, kept in a immutable way that can never be unaltered, and published in the internet so that anybody can open up and look.

Bitcoin

Each transaction is verified, verified transactions are recorded in the ledger, every record in the ledger are kept in an immutable way that the content can never be altered.

There are three parts to this:
1st Verification of ownership
2nd Double spending free
3rd Verified transactions are scribed into the blockchain (a digital file whose contents cannot be altered once recorded)

How?

- As the ledger is openly published and shared by the p2p computers in the internet, any transactions can be verified for valid ownership and free of double spending problem.
- Blockchain means also a new cryptographic technology which is to resolve the issue of how to keep the content of the digital file unaltered once recorded.

Blockchain is believed to have many usages beyond currency.

Blockchain 기술

A file of size 1Mbyte is called a block.
Written inside this file are the transactions content and time.
A series of such files connected in the order of time is called Blockchain.

Namely, blockchain is a digital ledger with many bound pages.

Time 1: A gives B two coins.
Time 2: B gives C one coin.
Time 3: C gives D 0.5 coin.

As given above, coin transactions are recorded with time.
Taking a look inside this ledger, one can always verify who owns how much coin, how much coin has been transferred from whom to whom.
This ledger is openly published in the internet and anybody can download it.
Opening up the ledger, anybody can see how much money is belong to a person.

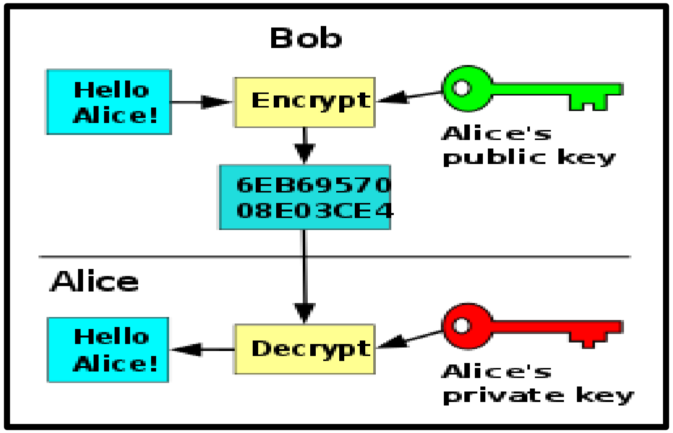
But please make no mistake.
This ledger however uses cryptographic hash values.
The coin ownerships are given to cryptographically made addresses.
Only the person who has the private key to the public address can claim the ownership of the coin.

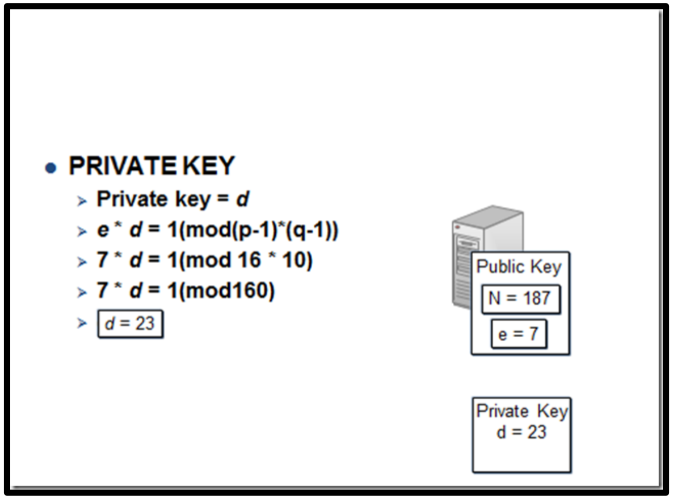
How to do Digital Signature (RSA example)

- 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.




- PRIVATE KEY
  - Private key = *d*
  - $e * d = 1(mod(p-1)*(q-1))$
  - $7 * d = 1(mod\ 16 * 10)$
  - $7 * d = 1(mod160)$
  - $\boxed{d = 23}$

Public Key
N = 187
e = 7
Private Key
d = 23

Google pictures

Digital Signing with RSA

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.

Private-key
Public-key

Note: bitcoin does not use RCA but Secure Hash Algorithms.

But for today, we use RSA because it is more familiar to us.

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).

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

An internet published and connected digital file.

A digital file?
Content can be forged or altered easily?

Novel way to resolve the problem of forgery and unwanted alterations.

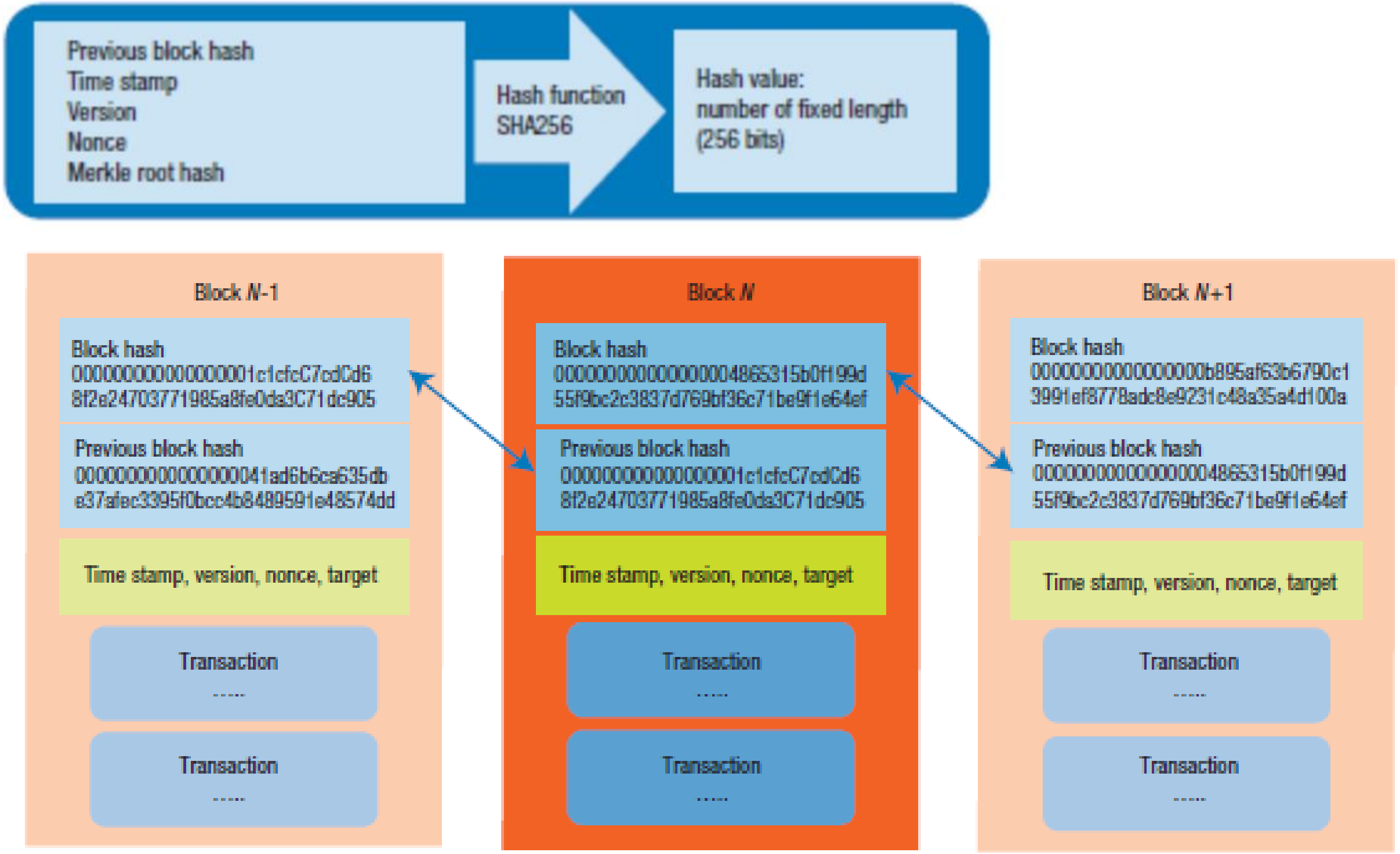
- Each block should include a block summary.

- Block summary should be good enough, the block with a good enough summary attated is connected to the existing chain of blocks.

Revolutionary new idea!

- Any single computer cannot find a good block summary within a given amount of computing time.
- If the number of computers is large enough and all are simultaneously working on finding a good summary for a block, a single computer among them can become successful in finding good summary.
- A reward is given to this computer which has found a good block summary.
- Once completed, a new race starts again for a new block.
- The more computers are gathered and the safer the system becomes.

Bitcoin Blockchain



Previous block hash
Time stamp
Version
Nonce
Merkle root hash

Hash function
SHA256

Hash value:
number of fixed length
(256 bits)

Block *N*-1

Block hash
0000000000000000001c1cfcC7cdCd6
8f2e24703771985a8fe0da3C71dc905

Previous block hash
00000000000000000041ad6b6ca635db
e37afec3395f0bcc4b8489591e48574dd

Time stamp, version, nonce, target

Transaction

Transaction

Block *N*

Block hash
0000000000000000004865315b0f199d
55f9bc2c3837d769bf36c71be9f1e64ef

Previous block hash
0000000000000000001c1cfcC7cdCd6
8f2e24703771985a8fe0da3C71dc905

Time stamp, version, nonce, target

Transaction

Transaction

Block *N*+1

Block hash
00000000000000000b895af63b6790c1
3991ef8778adc8e9231c48a35a4d100a

Previous block hash
0000000000000000004865315b0f199d
55f9bc2c3837d769bf36c71be9f1e64ef

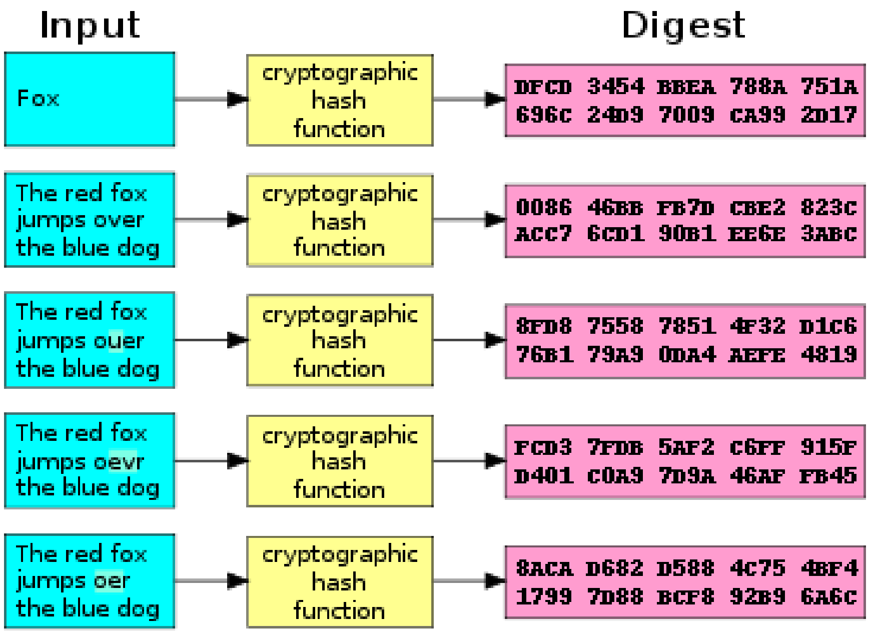
Time stamp, version, nonce, target

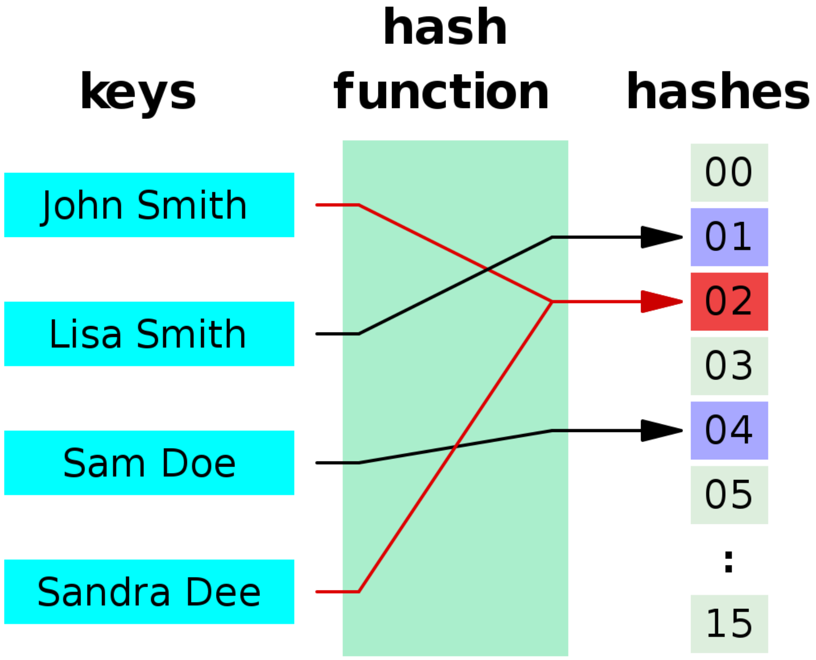
Transaction

Transaction

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.

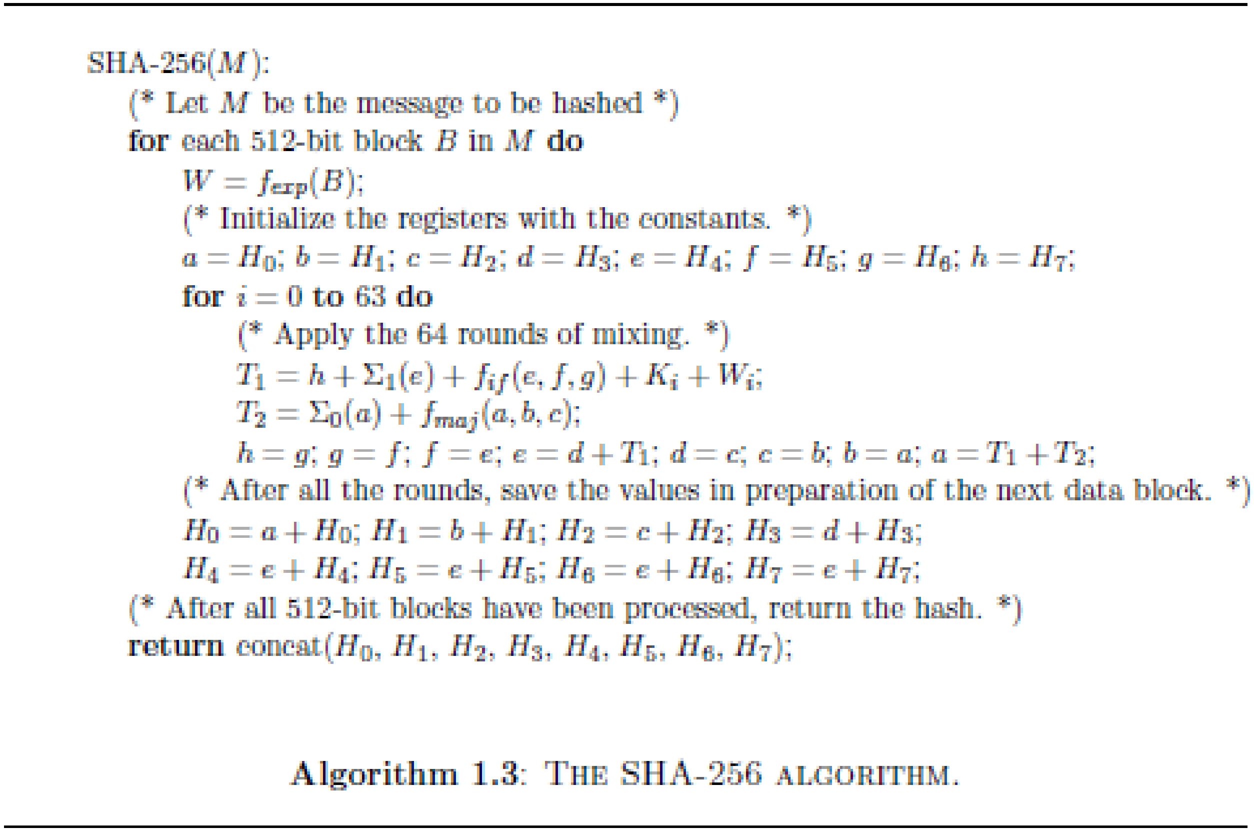
Secure Hash Function I/O


Input
Digest
Fox
cryptographic hash function
DFCD 3454 BBEA 788A 751A
696C 24D9 7009 CA99 2D17
The red fox jumps over the blue dog
cryptographic hash function
0086 46BB FB7D CBE2 823C
ACC7 6CD1 90B1 EE6E 3ABC
The red fox jumps ouer the blue dog
cryptographic hash function
8FD8 7558 7851 4F32 D1C6
76B1 79A9 0DA4 AEFE 4819
The red fox jumps oevr the blue dog
cryptographic hash function
FCD3 7FDB 5AF2 C6FF 915F
D401 C0A9 7D9A 46AF FB45
The red fox jumps oer the blue dog
cryptographic hash function
8ACA D682 D588 4C75 4BF4
1799 7D88 BCF8 92B9 6A6C



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

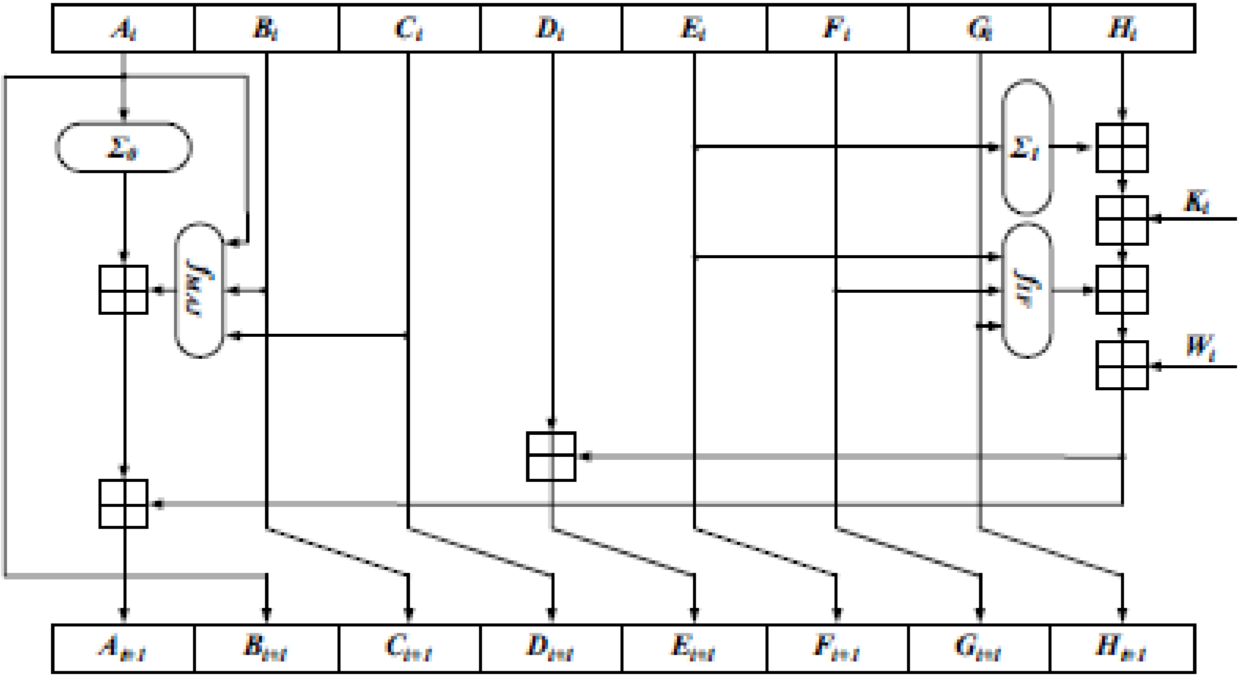


Figure 1.4: Schematic oveview of a 0 SHA-2 round. Note the added non-linear functions in comparison with SHA-1.

What is Hash Function?

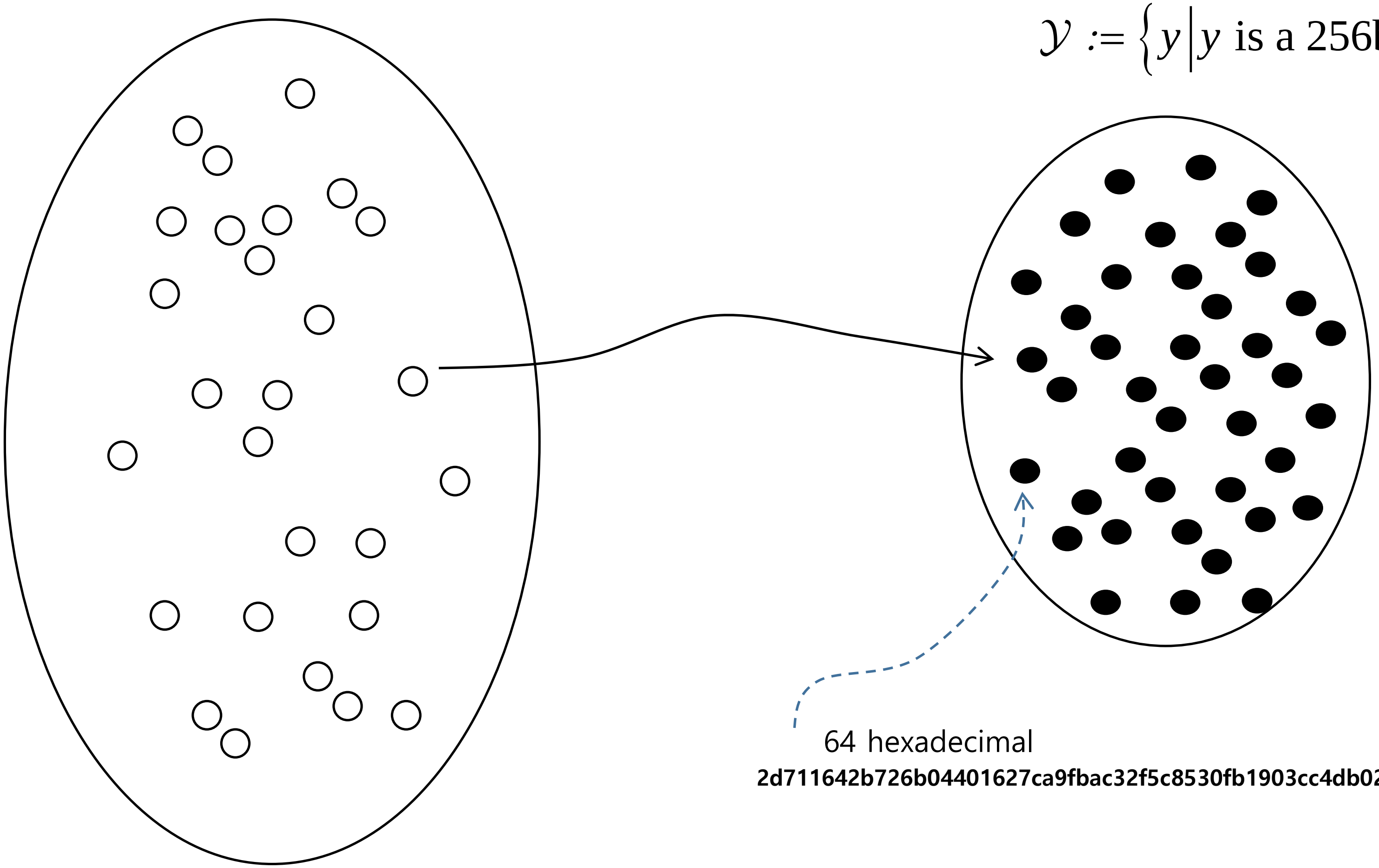
- Bitcoin uses SHA256.
- The input to the hash function is a text message or a file.
- The output of the hash function is 256 bit string.
- Conditions for Good Hash Function
    - (One way) With a little change in the input, the output is completely different.
        - Input distance has no relation 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!

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

SHA256, F(x) = y

$\mathcal{X} := \left\{ x \middle| x \text{ is a message up to 1 Mbyte in size} \right\}$

$\mathcal{Y} := \left\{ y \middle| y \text{ is a 256bit string} \right\}$



64 hexadecimal

2d711642b726b04401627ca9fbac32f5c8530fb1903cc4db02258717921a4881

Finding Good Block Summary

- Let H(*) be the Hash Function

- Function F takes an input x and gives output y

  y = F(x)

- F(block) = block summary (hash value)

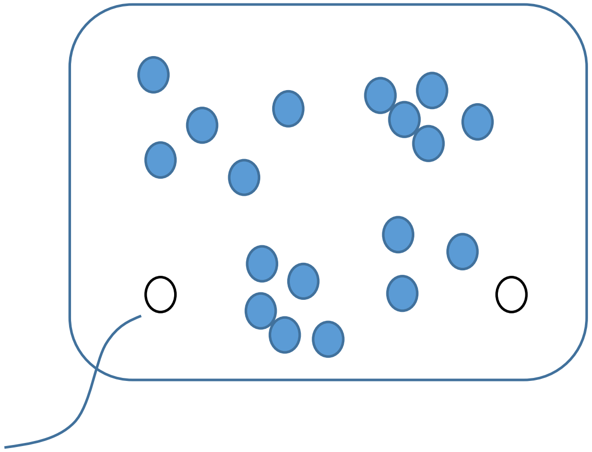
- Finding good block summary can be written as.

  F(block, *nonce*) < a certain value (PoW)

- Given a block, find nonce which satisfies the above inequality.

- Once *nonce* found, record it in the block header.

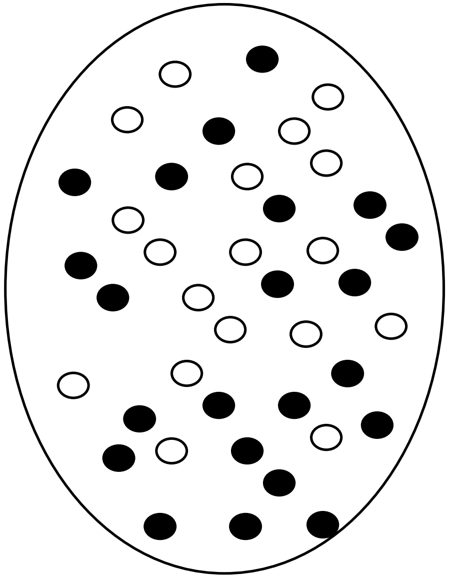
What is the probability to select a white ball?



Function Output

The probability a cpu solves (PoW) in a single cycle, given the first four strings are zeros?

$$\mathcal{Y} := \left\{ y \middle| y \text{ is a 256bit string} \right\}$$



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

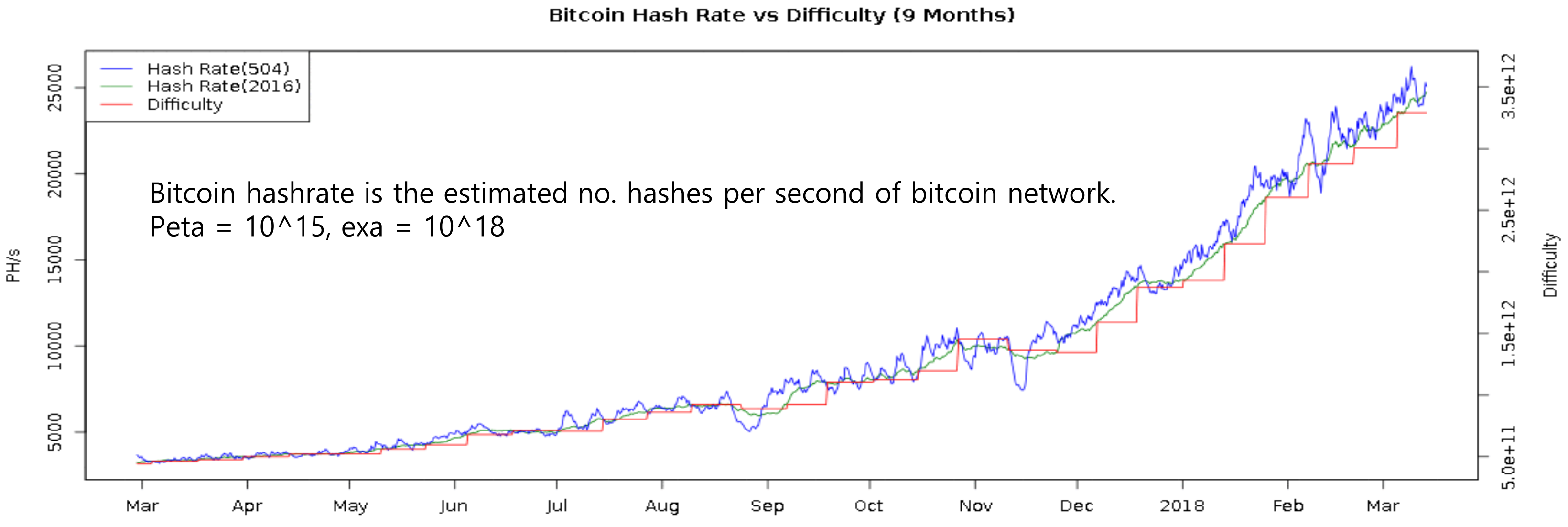
256 bit is 64 hexadecimal string

A hash value
2d711642b726b04401627ca9fbac32f5c8530fb1903cc4db02258717921a4881

A good hash value which passes the condition that the first four digits are 0s.
0000f727854b50bb95c054b39c1fe5c92e5ebcfa4bcb5dc279f56aa96a365e5a

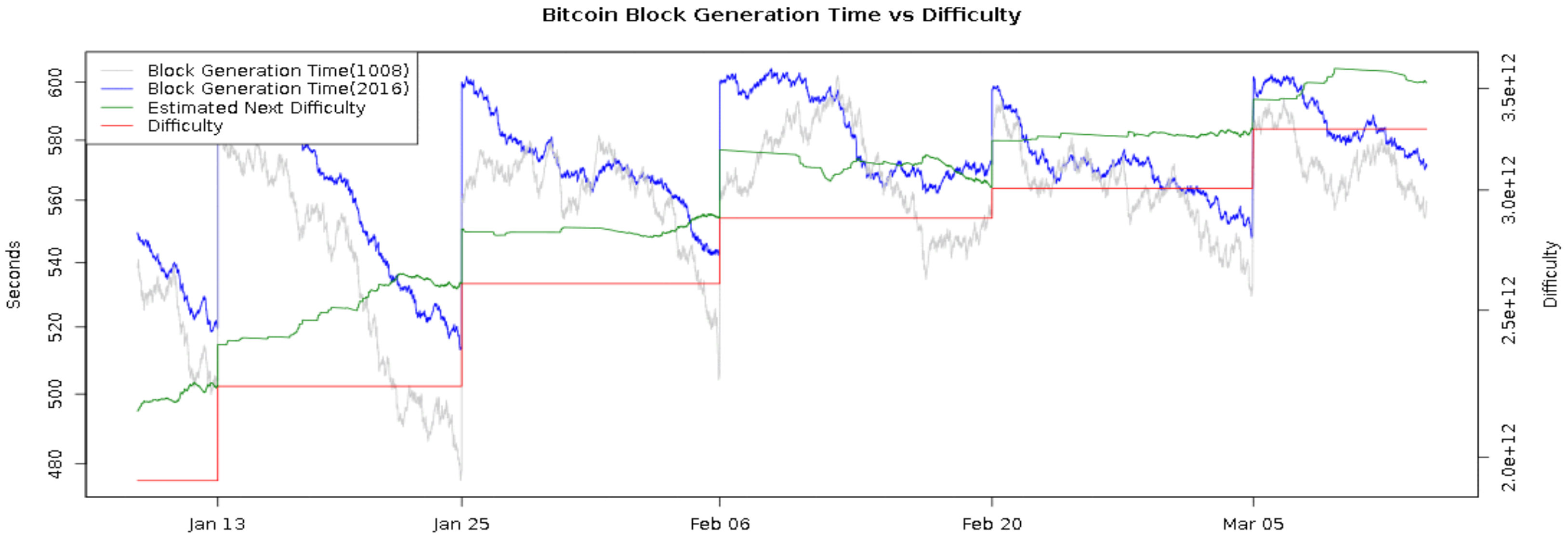
c = the set of any hash values = 2^256
a = the set of wanted hash values= 2^(256 – 16) = 2^240

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



Bitcoin Hash Rate vs Difficulty (9 Months)

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



Bitcoin Block Generation Time vs Difficulty

https://bitcoinwisdom.com/bitcoin/difficulty

ASIC Mining Hardware

Bitcoin double SHA256 ASIC mining hardware

Product	Advertised Mhash/s	Mhash/J	Mhash/s/$	Watts	Price (USD)	Currently shipping	Comm ports	Dev-friendly
AntMiner S1 [1]	180,000	500	800	360	299[2]	Discontinued	Ethernet	GPL infringement
AntMiner S2 [3]	1,000,000	900	442	1100	2259	Discontinued	Ethernet	GPL infringement
AntMiner S3 [4]	441,000	1300	1154	340	382[2]	Discontinued	Ethernet	GPL infringement
AntMiner S4 [5]	2,000,000	1429	1429	1400	1400	Discontinued	Ethernet	GPL infringement
AntMiner S5 [6]	1,155,000	1957	3121	590	370	Discontinued	Ethernet	GPL infringement
AntMiner S5+ [7]	7,722,000	2247	3347	3,436	2,307	No	Ethernet	GPL infringement
AntMiner S7 [8]	4,860,000	4000	2666	1,210	1,823	No	Ethernet	GPL infringement
AntMiner S9 [9]	14,000,000	10182	5833	1,375	2,400	Yes	Ethernet	GPL

Proof of Work is a ALone IMpossible Together Possible (Al-IM-To-Po) Problem!

The input set C can be divided into two sets.
Set A of elements each of which gives a wanted output.
Set B = Complement of A.
Let the size of each set be a, b, c.

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

Let there be a cpu which can take one input and gives one output.

What is the probability that this cpu gives a good summary?

P_1 = a/c
= 10^-6
= 0.000001

Suppose that this cpu can do 100 input/output cycles in 10 seconds.

What is the probability that this cpu can solve the PoW in 10 seconds?

P_2 = a/c + (b/c)*a/c + (b/c)^2*a/c + …
~ 100*a/c
= 10^-4 (2.384e-5 exact)

Suppose there are 10,000 such CPUs in the bitcoin p2p network which participate in PoW, what is the probability that at least one computer can find a good block summary?

Answer to Q

- **P_2 = 10^-4 is the probability that the cpu can solve the PoW in 10 seconds.**

- **What is the probability P_3 that at least one cpu finds a good block summary?**
- There are N =10^4 independently working cpu's.
- Let X1 = 1, cpu1 solves; X1 = 0, o.w.
- P3 = {at least one cpu success}

  = 1 – { no cpu success}

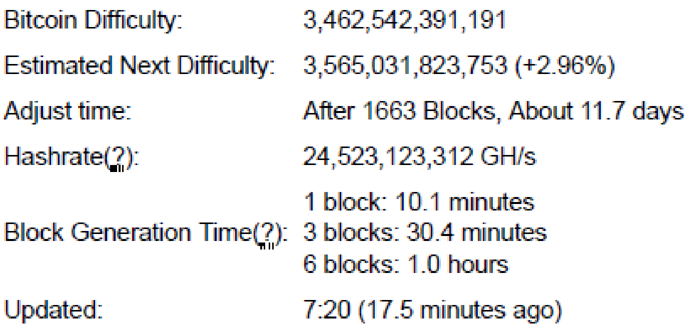
  = 1-(1 – P2)^10000

  = 0.3679 (0.2121)

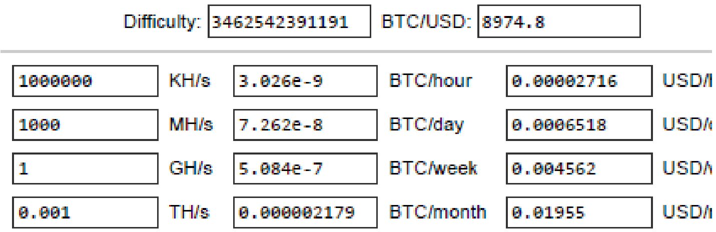
- When N = 1e5, P3 = 0.9078.

Bitcoin Difficulty

- The Bitcoin difficulty started at 1 (and can never go below that). Then for every 2016 blocks that are found, the timestamps of the blocks are compared to find out how much time it took to find 2016 blocks, call it T. We want 2016 blocks to take 2 weeks, so if T is different, we multiply the difficulty by (2 weeks / T) - this way, if the hashrate continues the way it was, it will now take 2 weeks to find 2016 blocks.

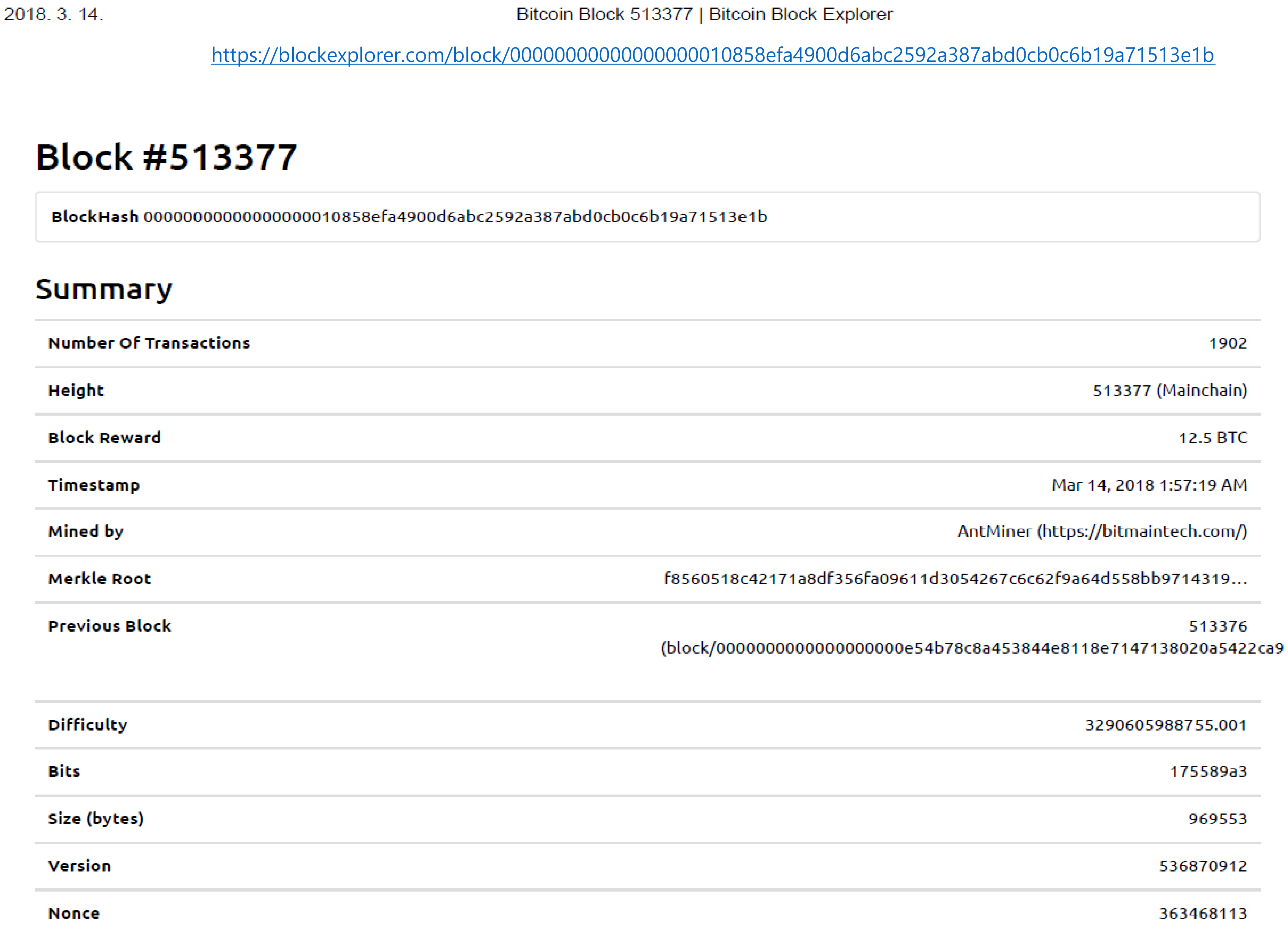


Bitcoin Difficulty:	3,462,542,391,191
Estimated Next Difficulty:	3,565,031,823,753 (+2.96%)
Adjust time:	After 1663 Blocks, About 11.7 days
Hashrate(?):	24,523,123,312 GH/s
Block Generation Time(?):	1 block: 10.1 minutes 3 blocks: 30.4 minutes 6 blocks: 1.0 hours
Updated:	7:20 (17.5 minutes ago)



Difficulty: 3462542391191 BTC/USD: 8974.8

1000000	KH/s	3.026e-9	BTC/hour	0.00002716	USD/
1000	MH/s	7.262e-8	BTC/day	0.0006518	USD/
1	GH/s	5.084e-7	BTC/week	0.004562	USD/
0.001	TH/s	0.000002179	BTC/month	0.01955	USD/



2018. 3. 14. Bitcoin Block 513377 | Bitcoin Block Explorer

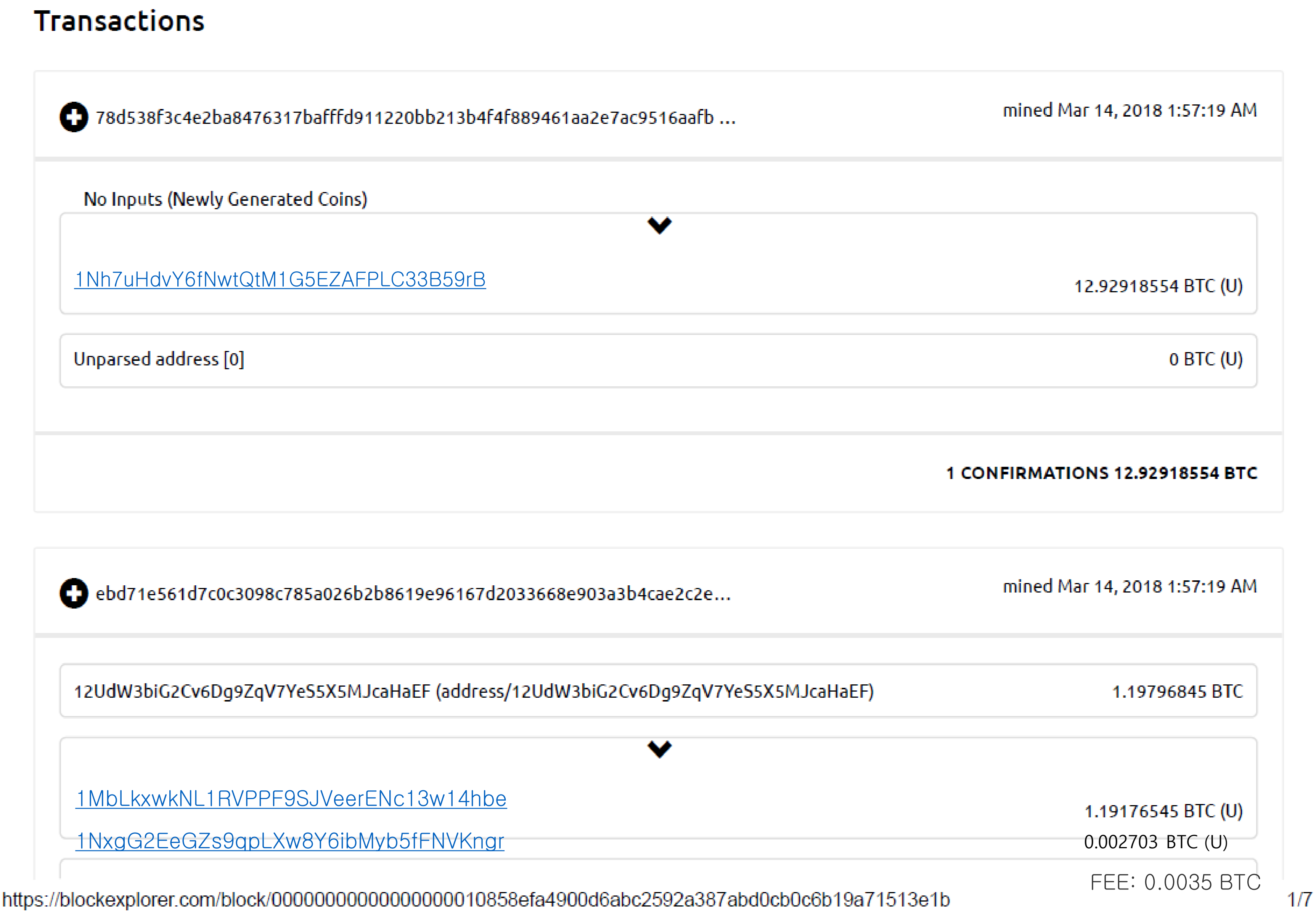
https://blockexplorer.com/block/00000000000000000010858efa4900d6abc2592a387abd0cb0c6b19a71513e1b

Block #513377

BlockHash 00000000000000000010858efa4900d6abc2592a387abd0cb0c6b19a71513e1b

Summary

Number Of Transactions	1902
Height	513377 (Mainchain)
Block Reward	12.5 BTC
Timestamp	Mar 14, 2018 1:57:19 AM
Mined by	AntMiner (https://bitmaintech.com/)
Merkle Root	f8560518c42171a8df356fa09611d3054267c6c62f9a64d558bb9714319...
Previous Block	513376 (block/0000000000000000000e54b78c8a453844e8118e7147138020a5422ca9
Difficulty	3290605988755.001
Bits	175589a3
Size (bytes)	969553
Version	536870912
Nonce	363468113



Transactions

78d538f3c4e2ba8476317bafffd911220bb213b4f4f889461aa2e7ac9516aafb ... mined Mar 14, 2018 1:57:19 AM

No Inputs (Newly Generated Coins)

1Nh7uHdvY6fNwtQtM1G5EZAFPLC33B59rB 12.92918554 BTC (U)

Unparsed address [0] 0 BTC (U)

1 CONFIRMATIONS 12.92918554 BTC

ebd71e561d7c0c3098c785a026b2b8619e96167d2033668e903a3b4cae2c2e... mined Mar 14, 2018 1:57:19 AM

12UdW3biG2Cv6Dg9ZqV7YeS5X5MJcaHaEF (address/12UdW3biG2Cv6Dg9ZqV7YeS5X5MJcaHaEF) 1.19796845 BTC

1MbLkxwkNL1RVPPF9SJVeerENc13w14hbe 1.19176545 BTC (U)

1NxgG2EeGZs9qpLXw8Y6ibMyb5fFNVKngr 0.002703 BTC (U)

FEE: 0.0035 BTC

https://blockexplorer.com/block/0000000000000000010858efa4900d6abc2592a387abd0cb0c6b19a71513e1b 1/7

Proof of Work and Data Immutability

- Proof of work(작업증명 in Korean) is to have a large set of miners find a solution satisfying (PoW).
  The first miner which succeed in solving it obtains the right to produce a certain amount of new coins to himself.
- It is the key mechanism for enforcing data integrity stored inside the blockchain.
- Blockchain is a very large stone!
- Each and every transaction is checked for validity and scribed into the stone.
- How can it be done with digital file?
- Answer is simple!
- Let a large number of computers work together simultaneously. Let the first computer which is successful at finding a good answer get rewarded. Have a new race begin by having the computers work on a new problem (new block) and reward another winner. The proof of work that a large number of computers have worked together is written into the block. If any computer, or a group of computers, aims to change the block content, then the same amount of work needs to be redone.
- How is the proof of work done?
  Use a Secure Hash Function(SHA).
  Characteristics of this function is that it is a forward-only function. That is, given the output value of this function, one cannot make any good guess about what the input value was. Thus, the only way to find a good answer to (PoW) problem is to try repeatedly with different input values as fast as possible until run across a satisfying one.
- Once a good answer is found, the input value which produces this good output value is scribed into the block (more specifically, into the blockheader).
- Anybody can figure out if it is a good answer or not. How?

Immutable File Keeping Technology

- The problem can almost never be solved alone, but it is designed in such a way that it can be solved within a desired time span when many computers come and compete to find a solution.
- It also has a means to measure the total amount of work done in probabilistic sense. If the difficulty level of the problem is increased, the number of computers in competition has to increase as well.
- This is used to protect the integrity of the data stored in the blockchain. Because it is a Al-Im-To-Po, a small group cannot fool the majority.
- PoW is to find the nonce which matches with the block content and put this nonce into the blockheader.
- What is the reason that those transactions once scribed inside the blockchain are not alterable?
- The block content are locked with the nonce.
- When the block content is changed somehow, the content no longer matches with the nonce found.
- Such blocks are easily detectable and thus a chain containing such block are also easily detectable and thrown away.
- Thus, anybody who aims to launch an attack of changing the content, the person needs to redo the PoW again to find a new nonce reflecting the changed block content.

But it is not the end.
The hash value of the previous block, F(block, nonce) in (PoW), is written inside the header of the next block.
Blocks are connected in a serial way by these hash values.

Thus, it is more difficult to change the content of a block which is buried deep inside the chain, since if it happens, then all the block headers subsequent to the altered one are changed as well.
This requires the attacker to redo all the PoWs for the subsequent blocks.

Recalling that it is very difficult to find the nonce for a single block, it becomes almost impossible for a single computer to find the nonces for a series of blocks.

It may become possible if there are a pool of miners that the attacker can control, and this pool is large enough compared to the pool of honest miners.

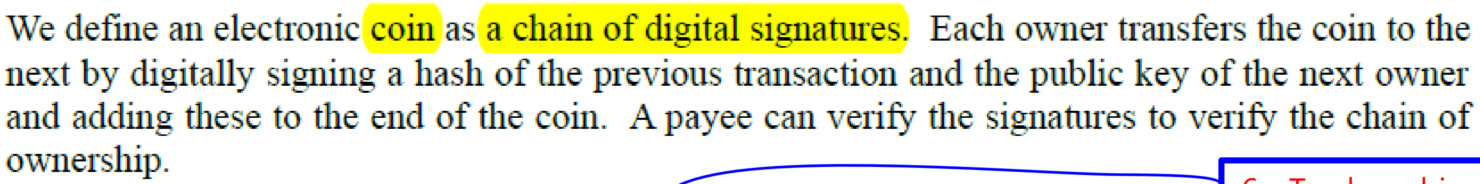
In the Bitcoin white paper, it is supposed to be an unlikely event to have such an attacker with a sizeable pool of computers works working for him in the network of decentralized and independent participants.

The problem though is that there are too many computers working as miners today and their power consumption is enormous. To resolve this issue, other mining methods have been proposed. One of the more prominent on is the use of Proof of Stake!

Bitcoin

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

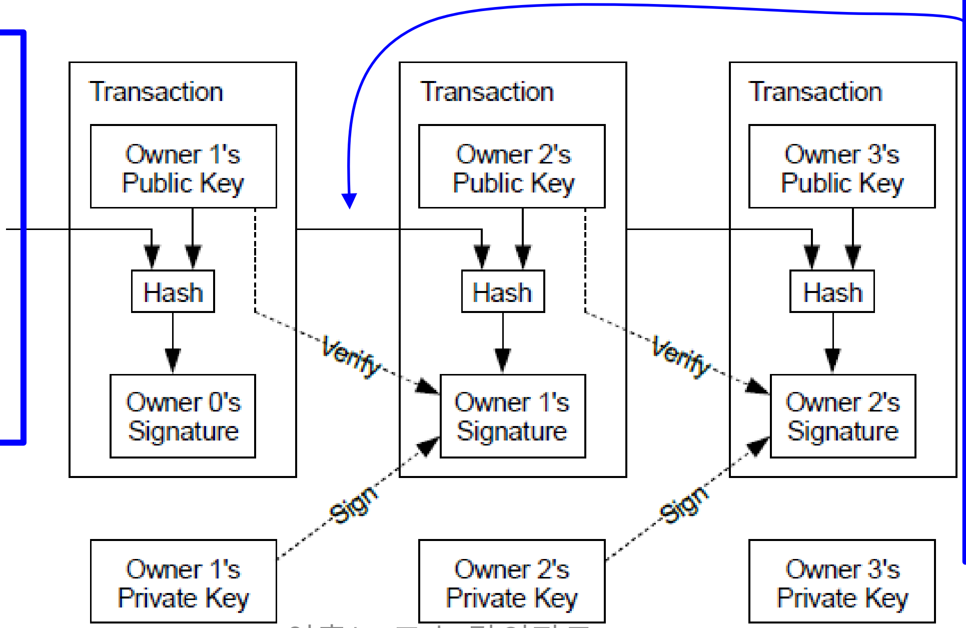
An e-coin is a chain of signatures.



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.

2nd Tx scene

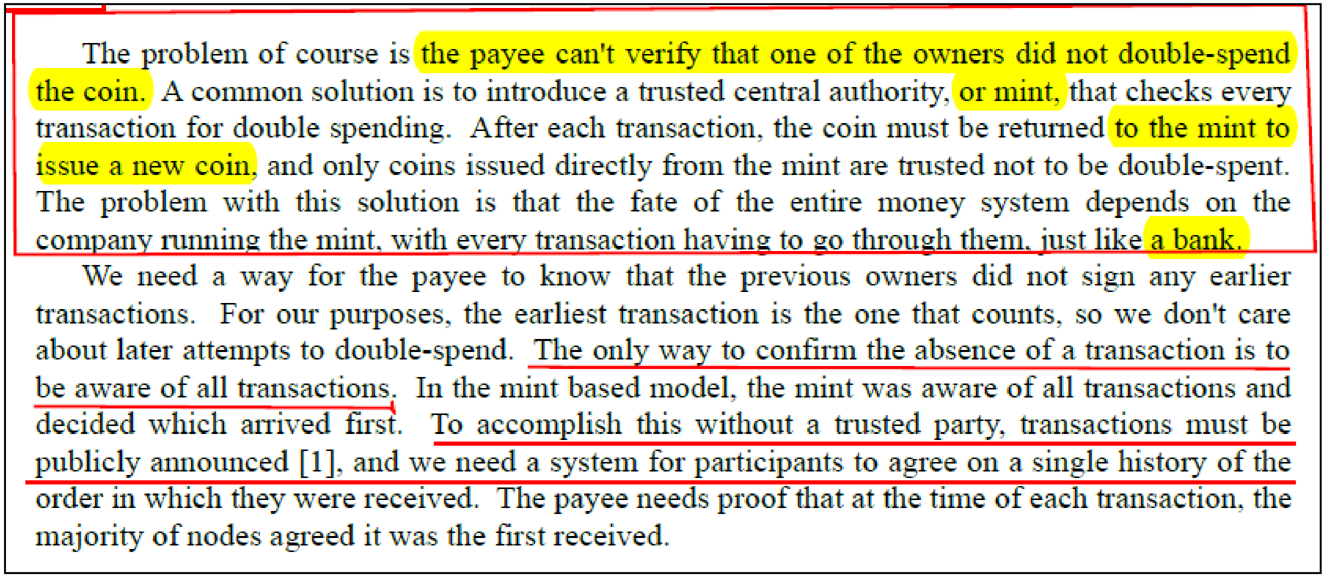
1. The first TX shows that O1 owns the coin.
2. O1 can transfer it to anybody, say O2.
3. O1 writes TX 2.
4. O1 asks Owner2, the new owner, for his public key.
5. O1 hashes the received public key and TX1, and writes down the hash value in TX2.



6. To show his ownership status, O1 signs the hash value and leaves the signature in TX2.
7. Now, anybody can verify O1's signature with O1's pubic key written in Tx1.

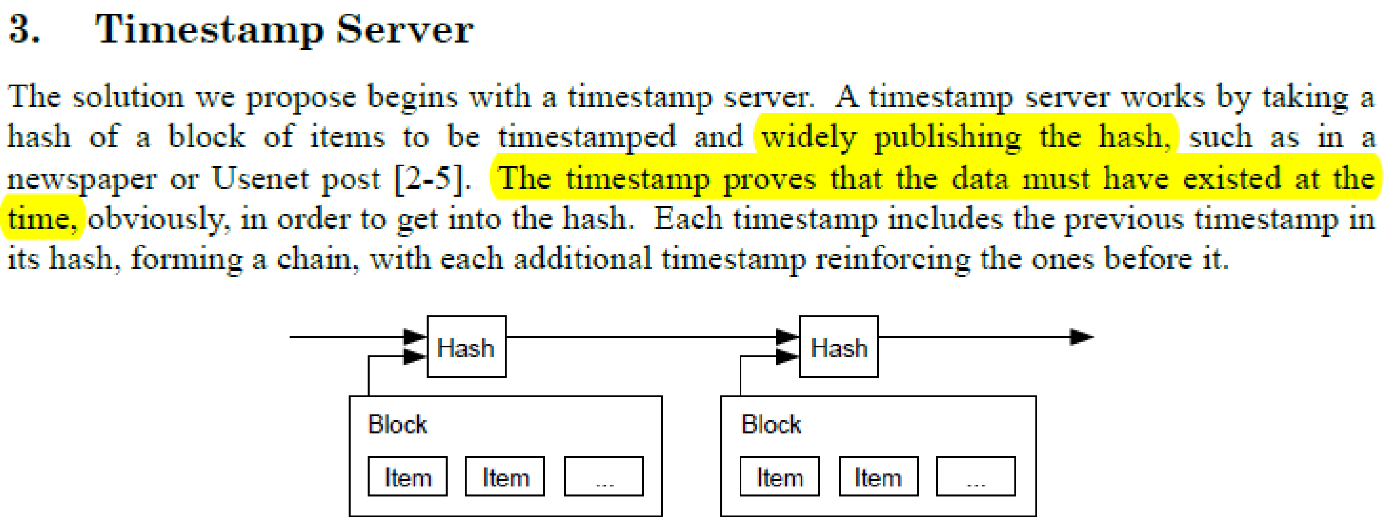
Once TX 2 recorded and published, anybody can easily see TX2 and knows that O1 has transferred his coin ownership to O2.

Double Spending Problem



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.



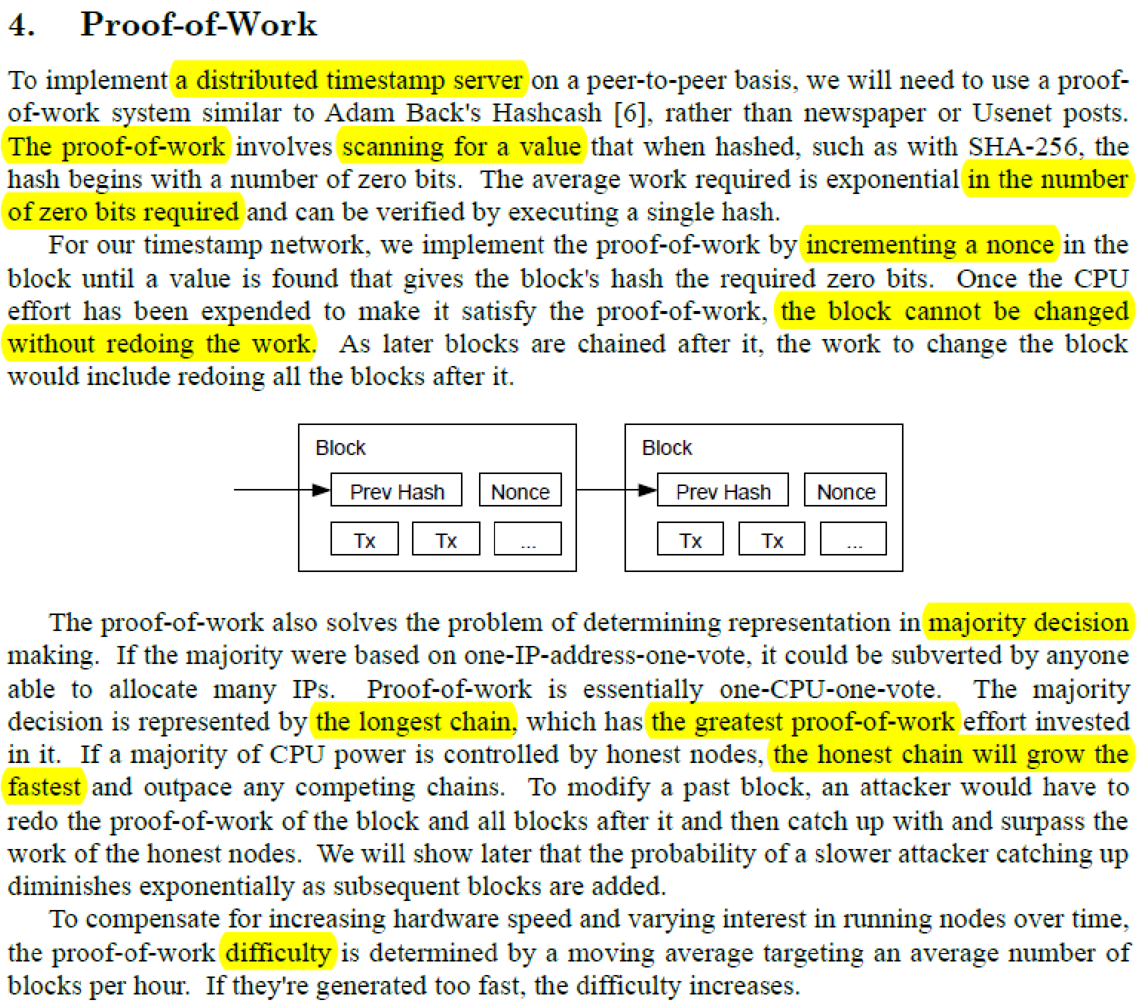
3. Timestamp Server

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.

- If a timestamp server indicates the existence of hash value at a certain time point, then a legitimate ledger can indeed be made?
  - If hash values only are published while no block contents are published, there will be no issue of scalability, and privacy can be kept since no one other than the parties involved in the transactions can see the content of transactions!
  - But how can one verify for coin ownership and double spending transactions.
- The problem is to decide who should run the timestamp server?
- If a government runs it, it becomes a private blockchain (social terms it is a public chain)!
- What possible problems are there if run by government?

Blockchain & Proof-of-Work

- Aim to make a timestamp Server in a P2P network.
  - Why?
  - Not to rely on the central authority.
  - Central authority such as banks and states
  - Within a nation, the state government can run the timestamp server
  - But for trades overseas, P2P across different nations is needed.
- Solution?
  - Distributed timestamp P2P network
  - Distributed, thus, it is difficult to maintain the integrity of data.
  - To keep the integrity of data, PoW system is proposed!



4. Proof-of-Work

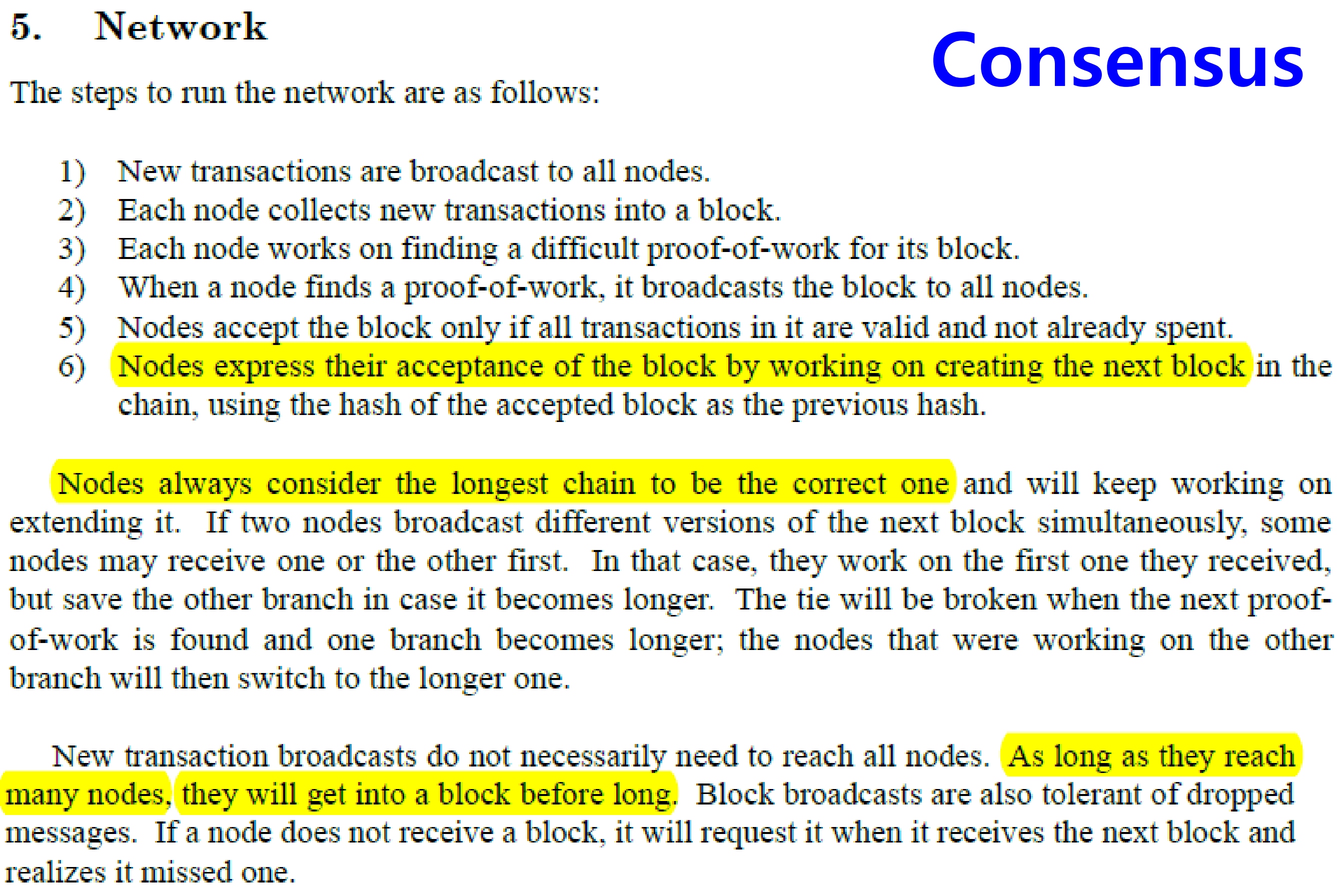
To implement a distributed timestamp server on a peer-to-peer basis, we will need to use a proof-of-work system similar to Adam Back's Hashcash [6], rather than newspaper or Usenet posts. The proof-of-work involves scanning for a value that when hashed, such as with SHA-256, the hash begins with a number 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.

Consensus Rule



5. Network

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.

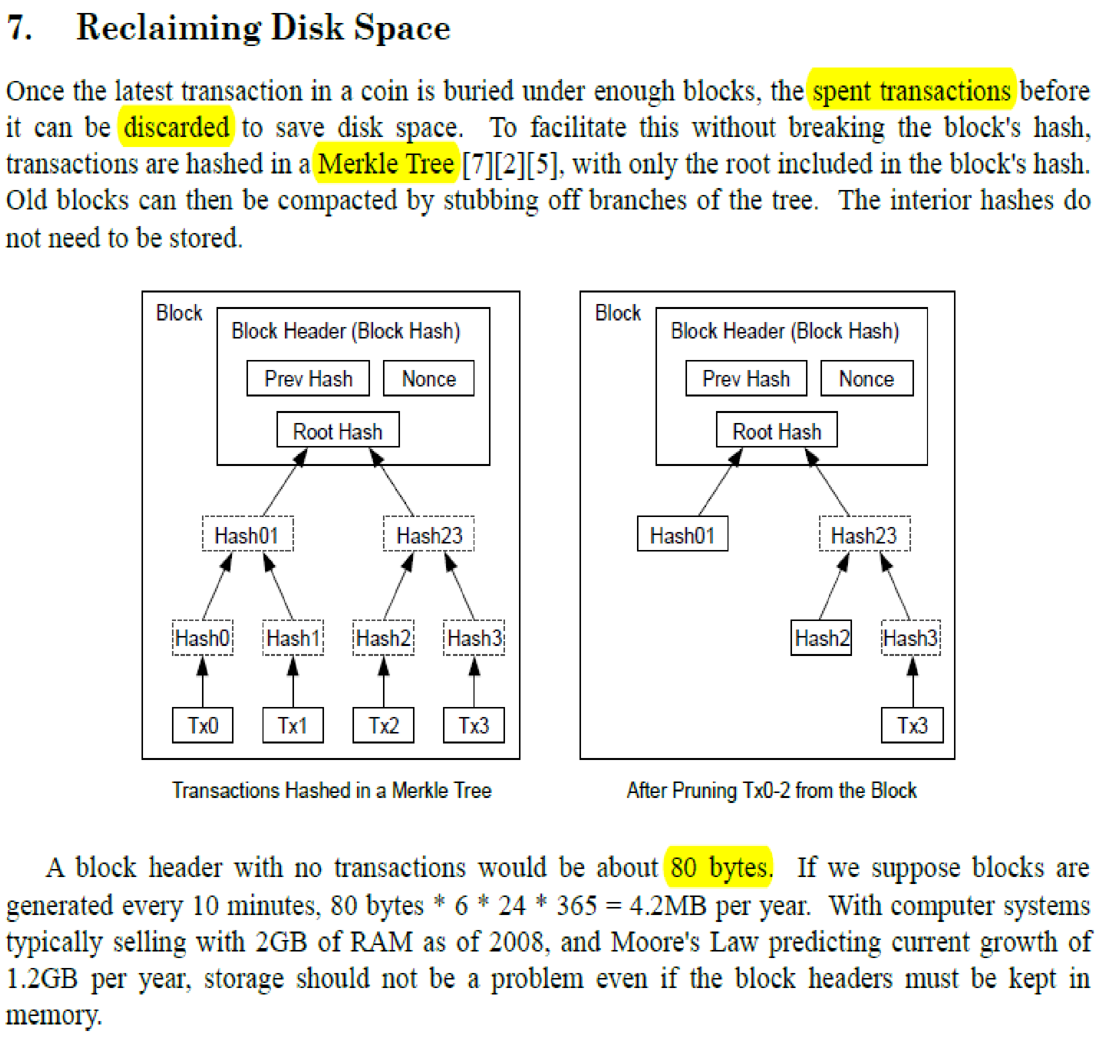
- Are there any guarantee for transactions to be included into blocks?
- With a large incentive(tx fee), a tx can be put on high priority, but if the production rate of txs is higher than the service rate, then there must be some transactions not to be end up in the blockchain.

Blockchain Scalability

- Use Merkle tree and save disk space
- Save the blockhash in the header.
- Those tree branches recording past transactions are erased but the hash values.
- 80 byte Blockheader

.

1. Prev hash: 256 bit = 2^8 = 2^5*(2^3) = 2^5 Bytes = 32 Bytes
2. Roothash = 32 Bytes
3. Nonce = 4 Bytes = 32 bit
4. Time
5. Difficulty
6. version



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.

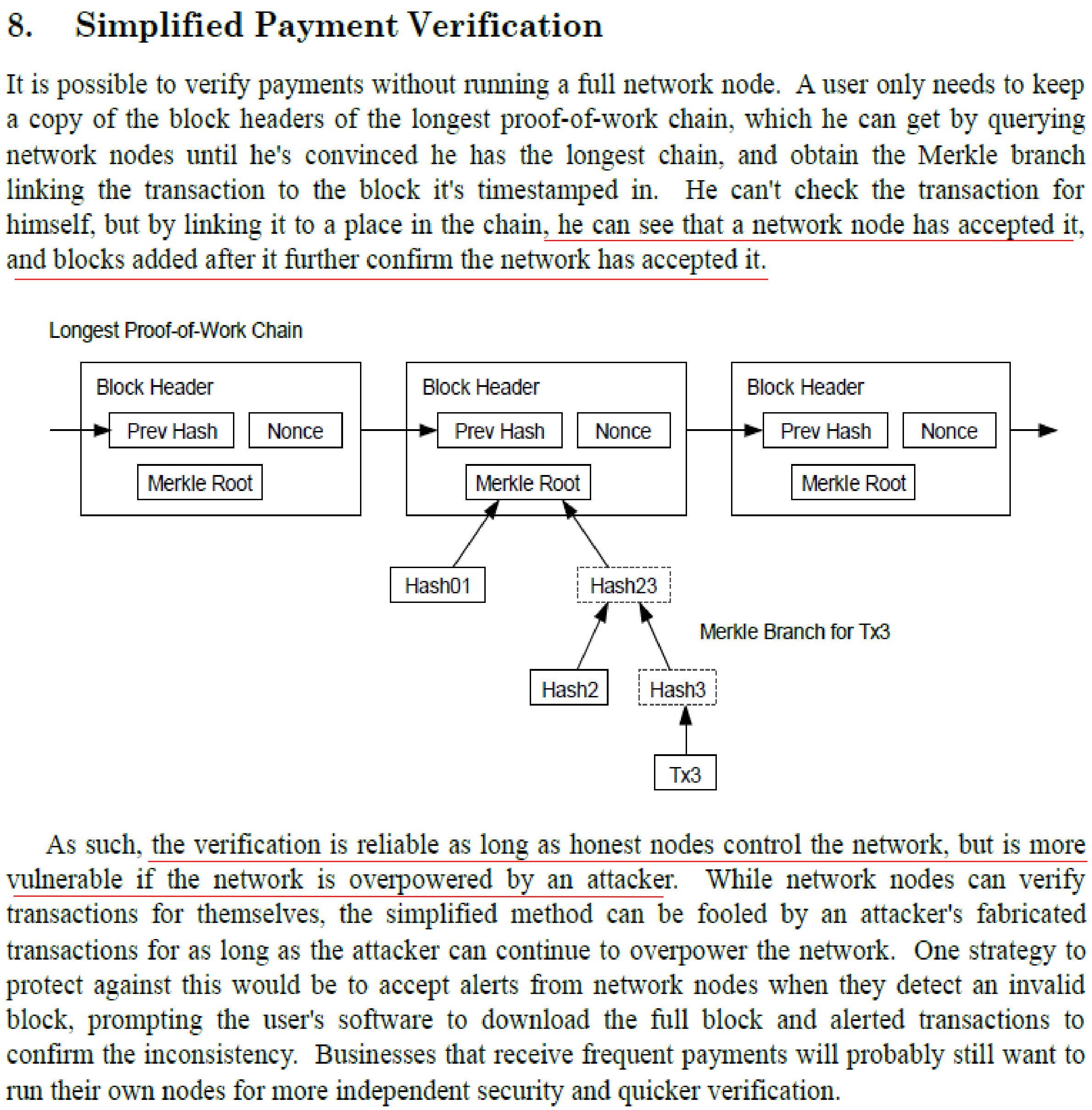
80 Byte Block Header

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 order of 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?

- A 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.



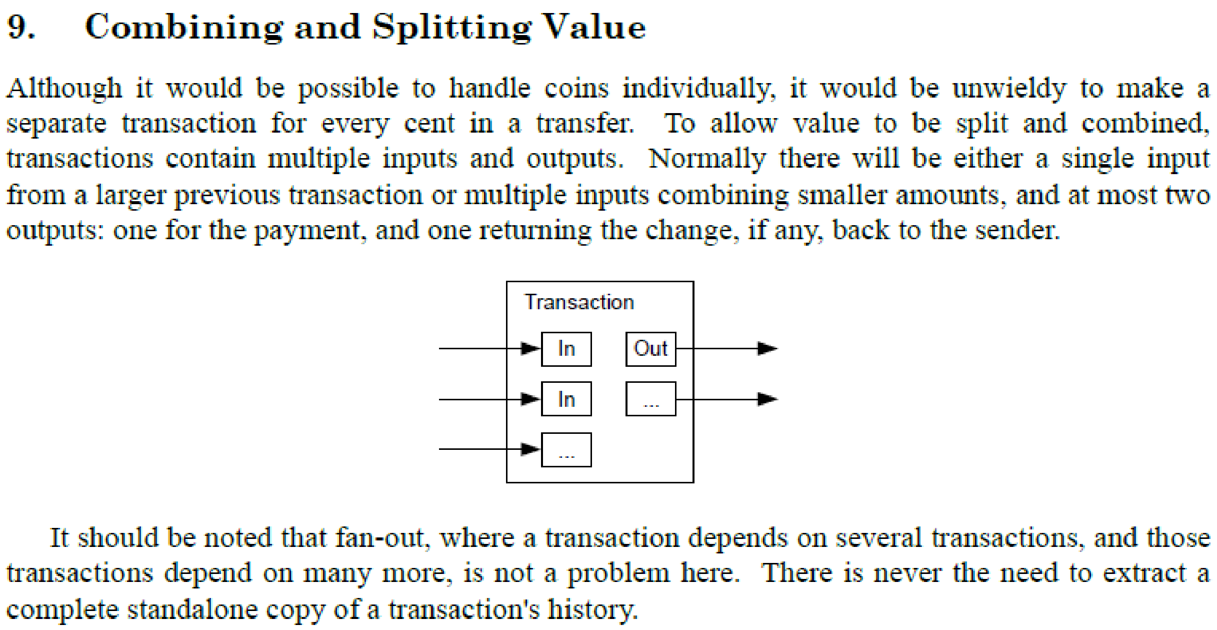
8. Simplified Payment Verification

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

- How to get the change?



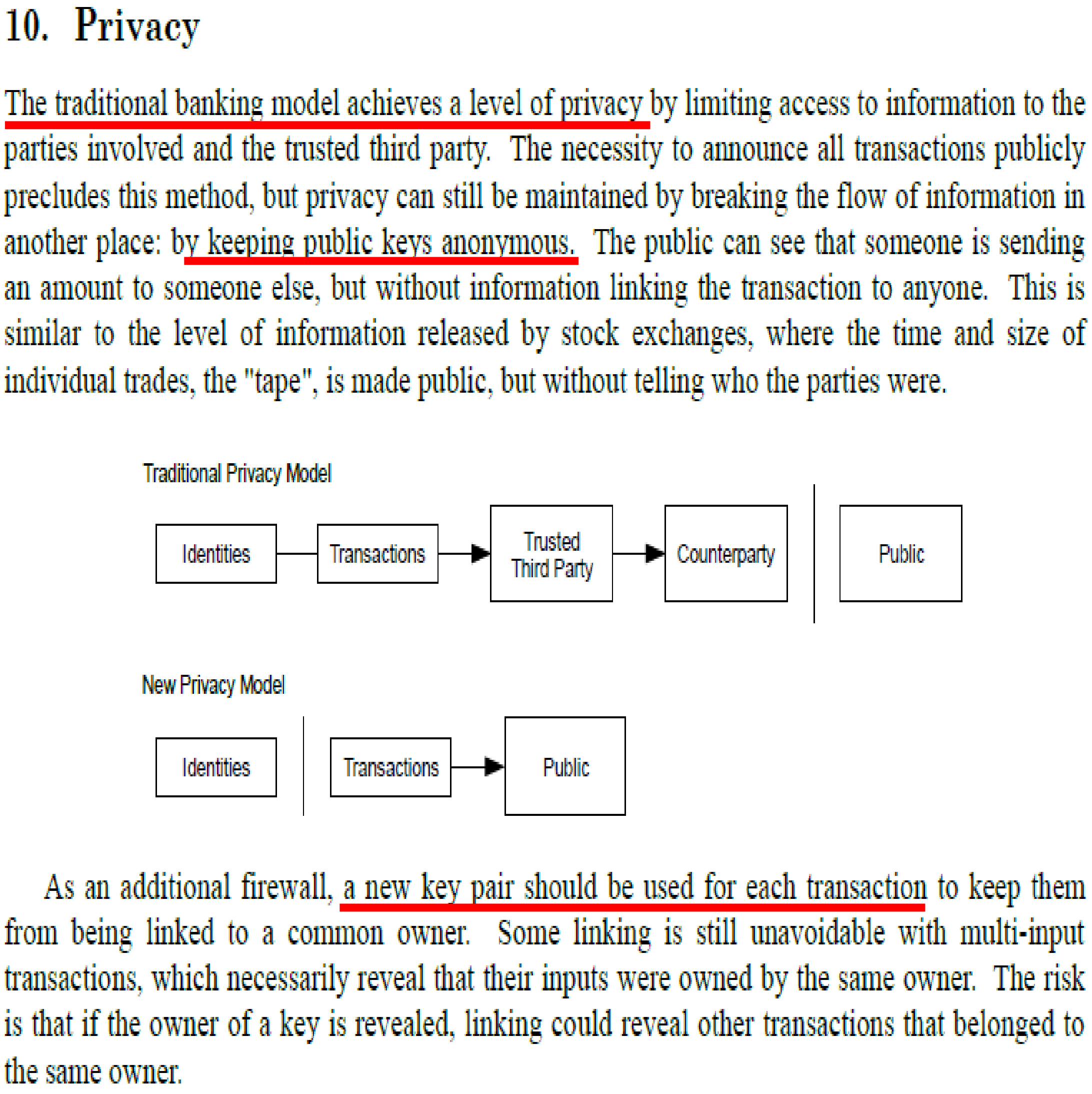
9. Combining and Splitting Value

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!



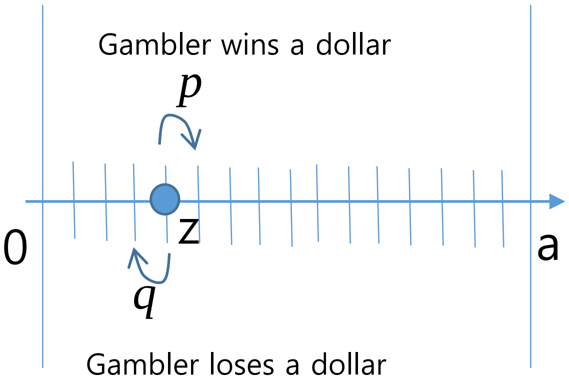
10. Privacy

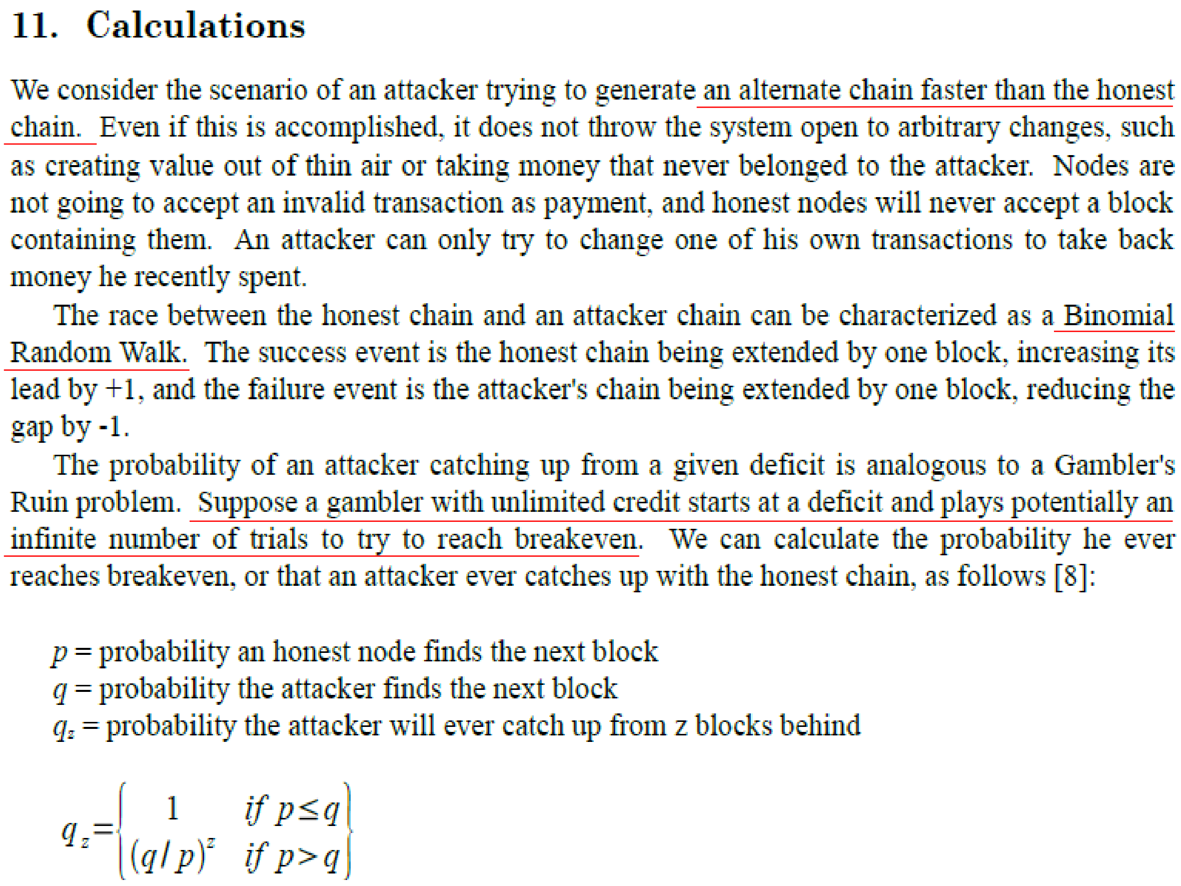
The traditional banking model achieves a level of privacy by limiting access to information to the parties involved and the trusted third party. The necessity to announce all transactions publicly precludes this method, but privacy can still be maintained by breaking the flow of information in another 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?
- 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]:

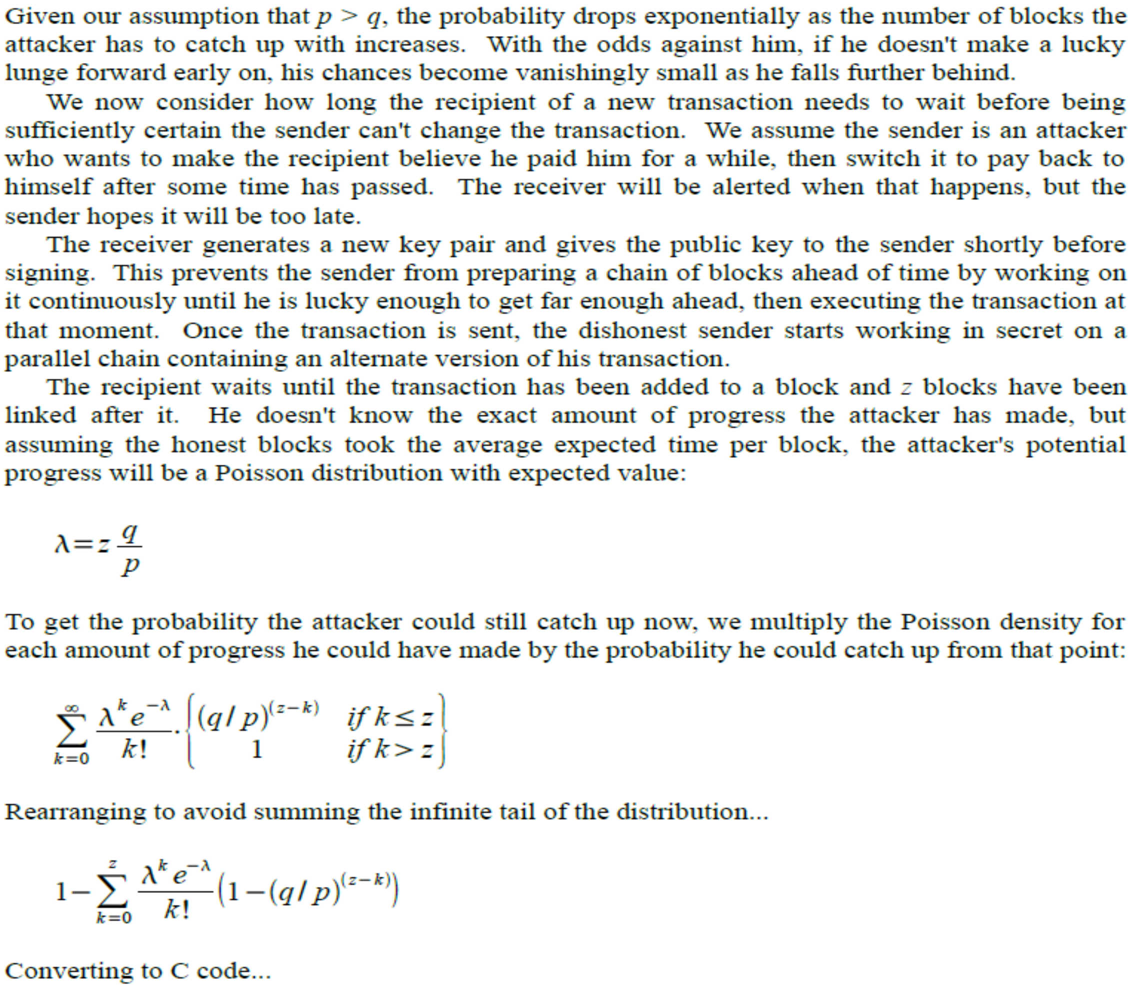
p = probability an honest node finds the next block
q = probability the attacker finds the next block
q_z = probability the attacker will ever catch up from z blocks behind

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

Attacker is the payer, fooling the payee!

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

What is the probability that the attack is successful?



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:

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

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...

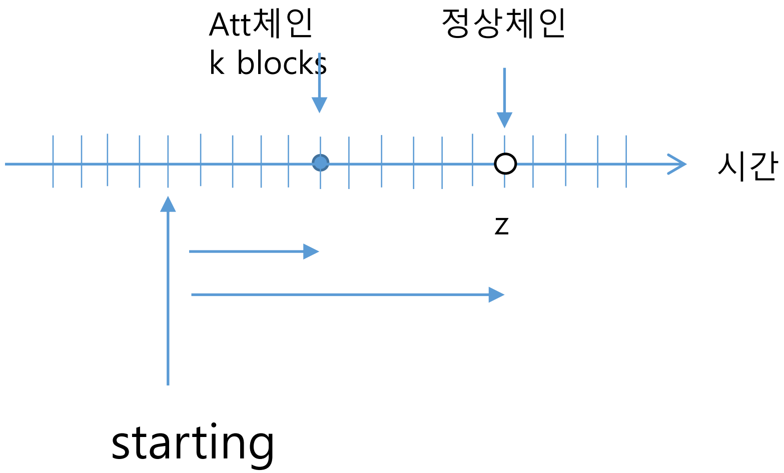
z blocks has passed. The recipient has waited until then. Now, the attacker likes to launch an attack by changing the transaction stored the z blocks past in the chain from
“A pays B 1 BTC” to “A pays C(A’s other public key)1BTC.”

Z blocks of PoW done and published

After the new chain is published,

there are two chains, the honest chain and the attacker’s chain.

The longer chain is to be accepted!



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

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

금융공학과 블록체인

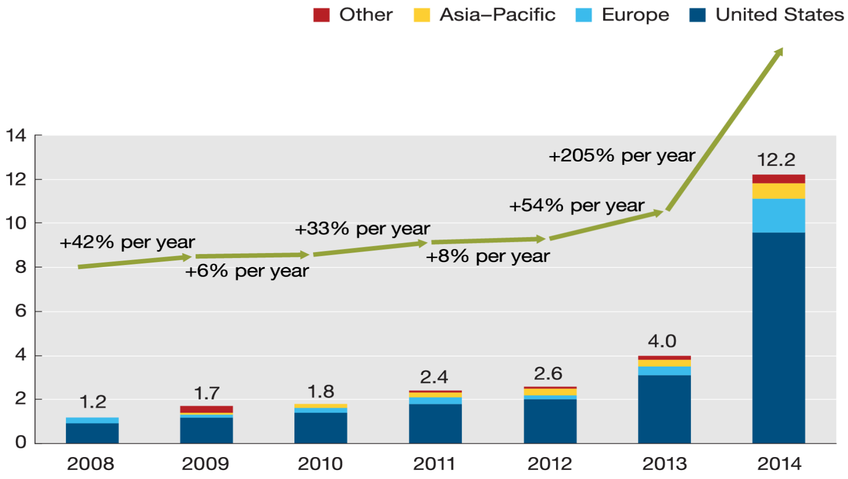
왜 금융공학인가?

어디로 투자가 되고 있는지 봐라!

광주가 할 수 있나?

The level of venture-capital investment in financial technology has recently accelerated.

Global investment in financial technology,
$ billion

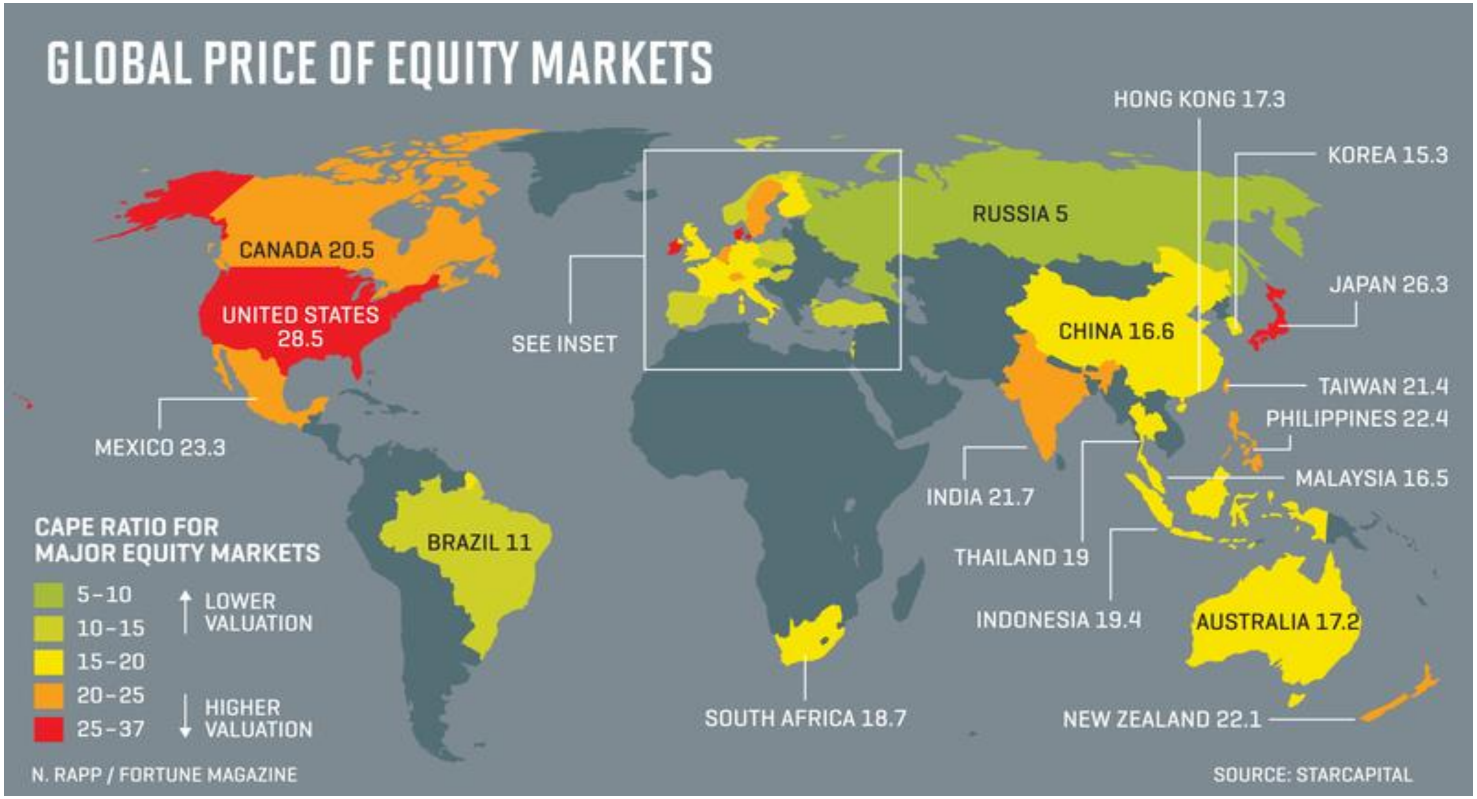


Source: CB Insights; analysis of data provided by McKinsey Panorama (a McKinsey Solution)

McKinsey&Company

This Map Will Show You the World's Most Expensive Stock Markets
FORTUNE, 2017/08/18

Cyclically Adjusted Price/Earnings ratio



A Brief History of Money

Or, how we learned to stop worrying and embrace the abstraction

By **James Surowiecki**

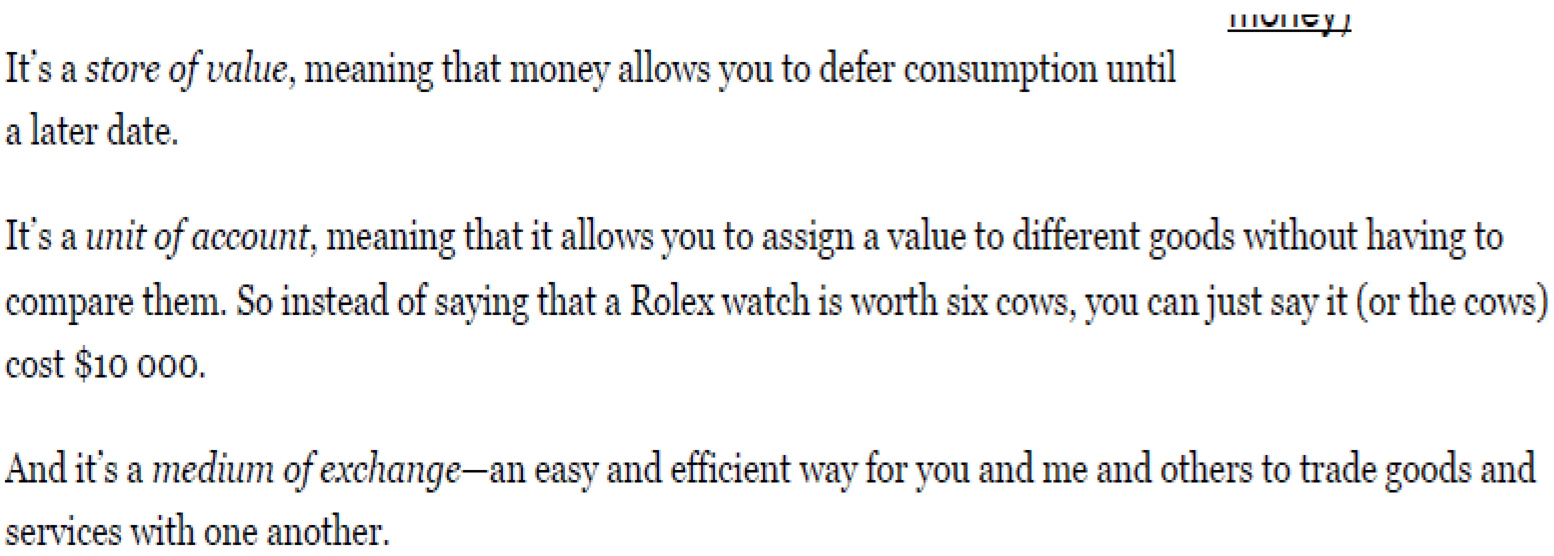
Photo: Levi Brown; Prop Stylist: Ariana Salvato

In the 13th century, the Chinese emperor Kublai Khan embarked on a bold experiment. China at the time was divided into different regions, many of which issued their own coins, discouraging trade within the empire. So Kublai Khan decreed that henceforth money would take the form of paper (http://www.britannica.com/EBchecked/topic/324254/Kublai-Khan/3994/Social-and-administrative-policy).

It was not an entirely original idea. Earlier rulers had sanctioned paper money, but always alongside coins, which had been around for centuries. Kublai's daring notion was to make paper money (the *chao*) the dominant form of currency. And when the Italian merchant Marco Polo visited China not long after, he marveled at the spectacle of people exchanging their labor and goods for mere pieces of paper. It was as if value were being created out of thin air.

Kublai Khan was ahead of his time: He recognized that what matters about money is not what it looks like, or

What Money is used for



money)

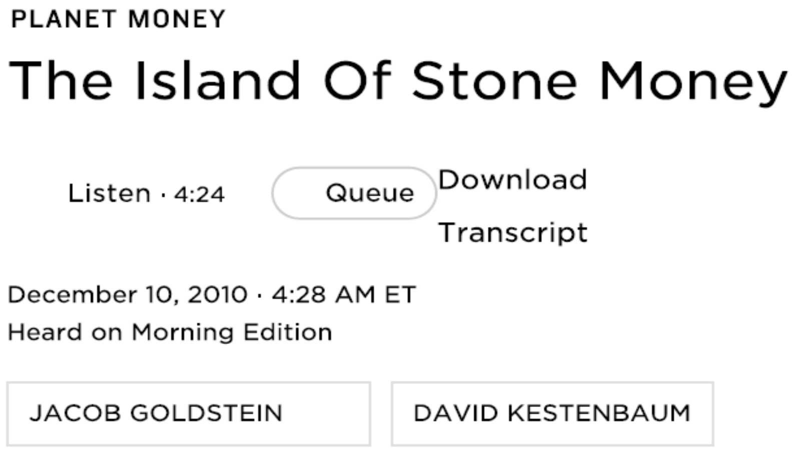
It's a *store of value*, meaning that money allows you to defer consumption until a later date.

It's a *unit of account*, meaning that it allows you to assign a value to different goods without having to compare them. So instead of saying that a Rolex watch is worth six cows, you can just say it (or the cows) cost $10 000.

And it's a *medium of exchange*—an easy and efficient way for you and me and others to trade goods and services with one another.

Barter → Coin → Paper money by decree → Fiat money → USD, KRW, EURO → Credit Cards → Internet money?

1000BC 600BC 13th Century 1661AD 19th Century 20th Century



PLANET MONEY

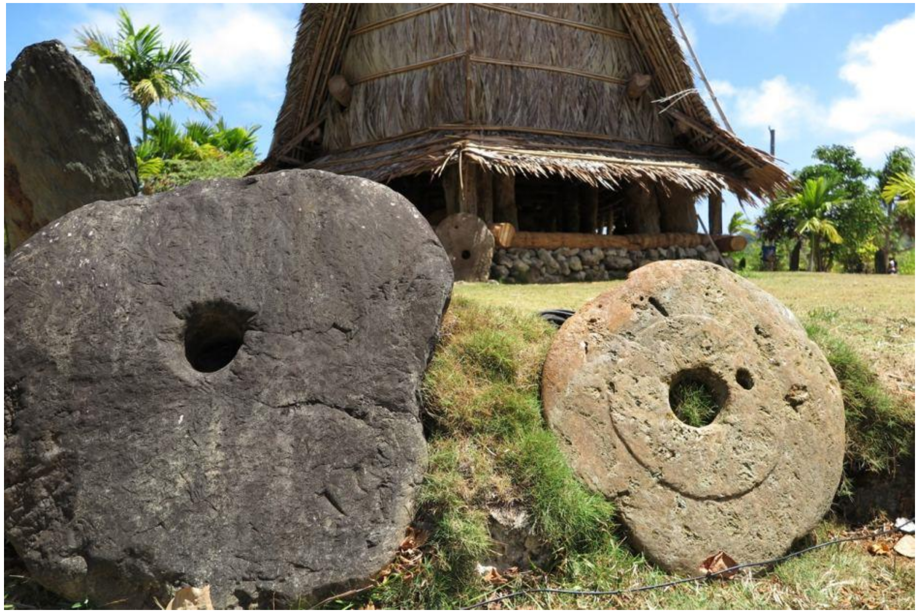
The Island Of Stone Money

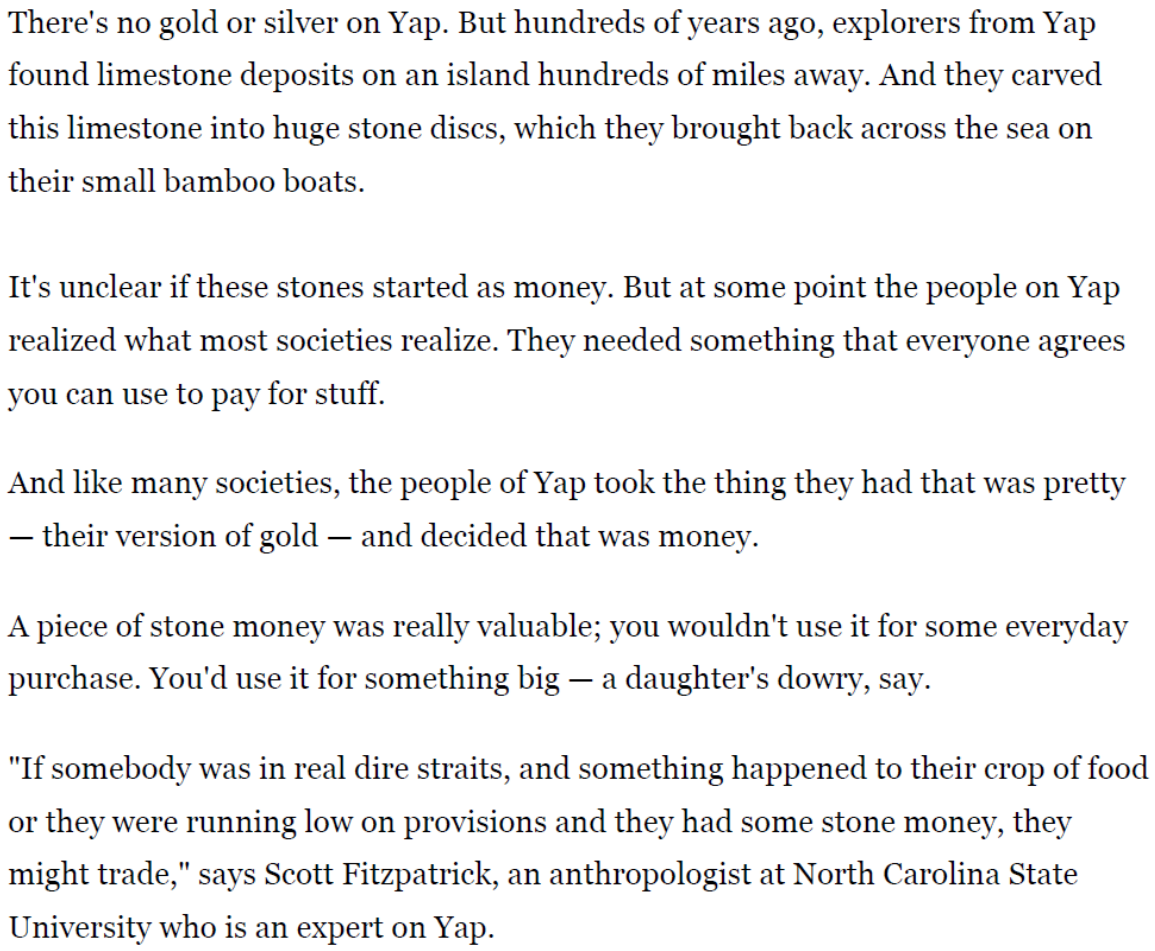
December 10, 2010 · 4:28 AM ET
Heard on Morning Edition

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?





There's no gold or silver on Yap. But hundreds of years ago, explorers from Yap found limestone deposits on an island hundreds of miles away. And they carved this limestone into huge stone discs, which they brought back across the sea on their small bamboo boats.

It's unclear if these stones started as money. But at some point the people on Yap realized what most societies realize. They needed something that everyone agrees you can use to pay for stuff.

And like many societies, the people of Yap took the thing they had that was pretty — their version of gold — and decided that was money.

A piece of stone money was really valuable; you wouldn't use it for some everyday purchase. You'd use it for something big — a daughter's dowry, say.

"If somebody was in real dire straits, and something happened to their crop of food or they were running low on provisions and they had some stone money, they might trade," says Scott Fitzpatrick, an anthropologist at North Carolina State University who is an expert on Yap.

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

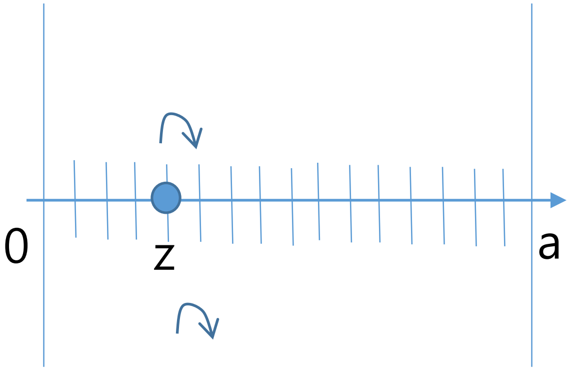
Seigniorage and the Federal Reserve

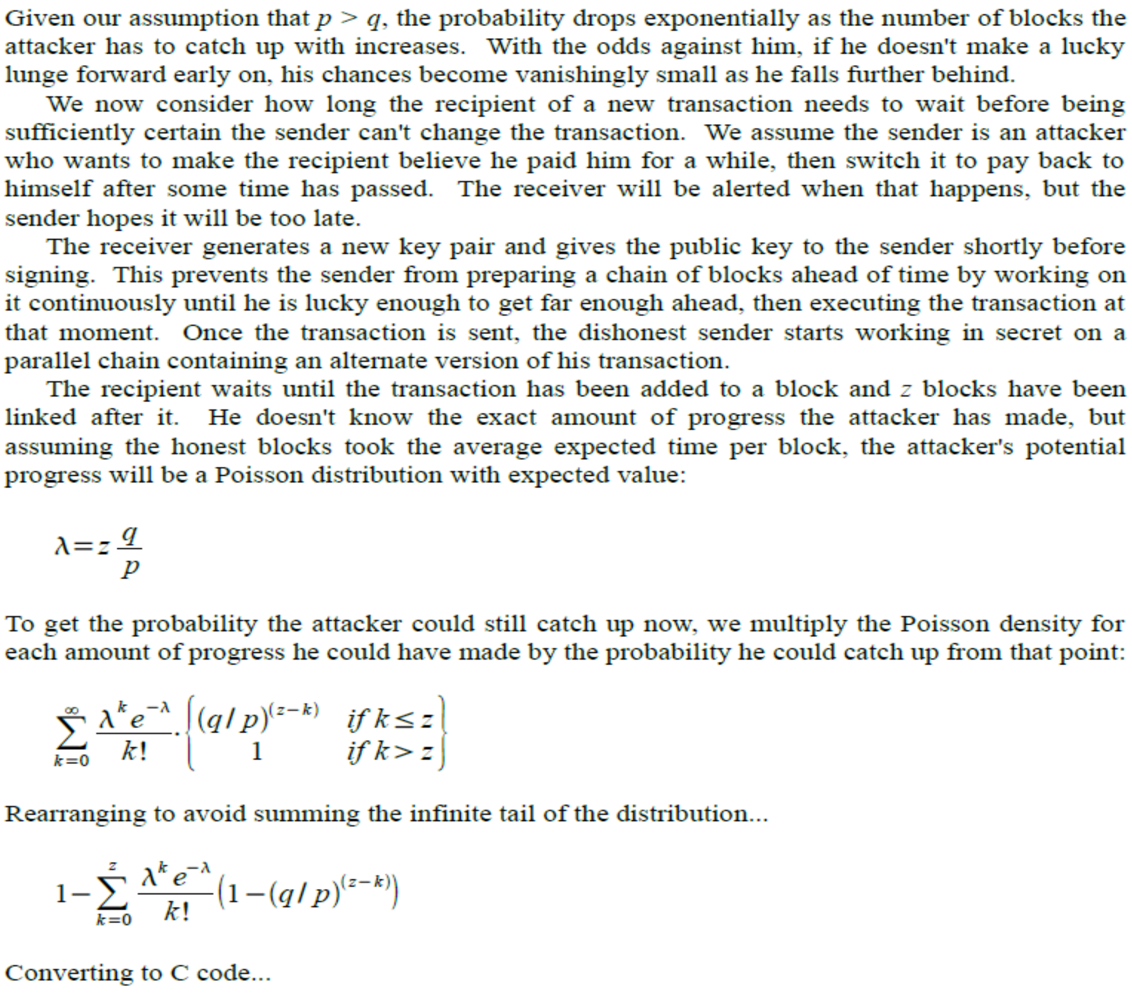
- While the basic principle behind seigniorage suggests that a country can profit from the production of new bills, there can be other factors affecting the entire transaction. Within the United States, if the Federal Reserve agrees to increase the number of dollars available within the U.S. economy, 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

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:

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

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

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

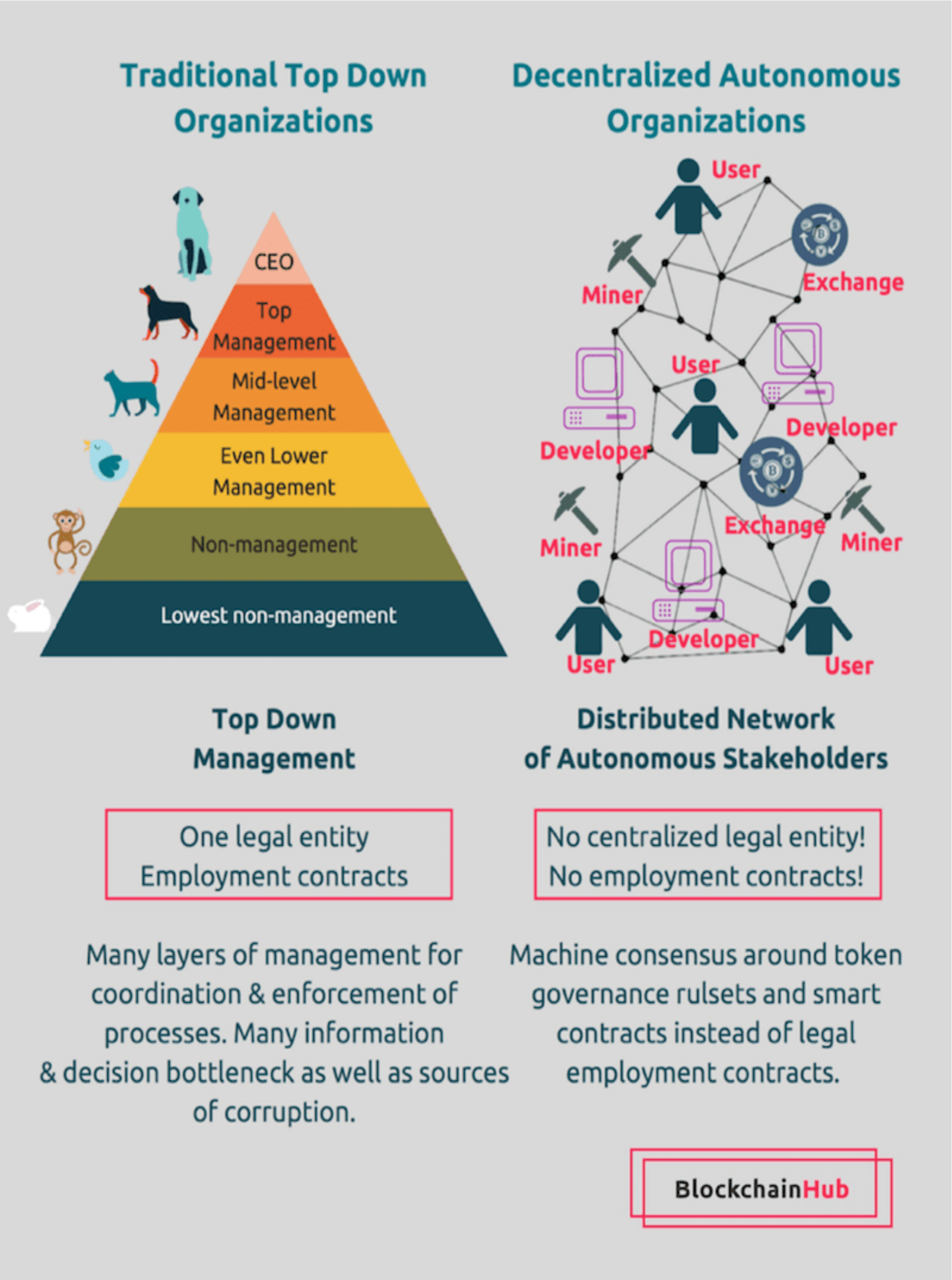
Converting to C code...

Bitcoin Economy

- Designer
  - Yearly planning of coin issuance, determination of system parameters such as block size, speed of services, incentive, contents to be included in the blockchain
- Developers pool
  - Bugs and other problems
  - System maintenance
- Users pool
  - Money transfers, retails, saving
- Miners pool

Not intended but

- Exchanges
- Investors
- Crowd funding
- Born of DAOism!



Traditional Top Down Organizations

Decentralized Autonomous Organizations

Top Down Management

Distributed Network of Autonomous Stakeholders

One legal entity
Employment contracts

No centralized legal entity!
No employment contracts!

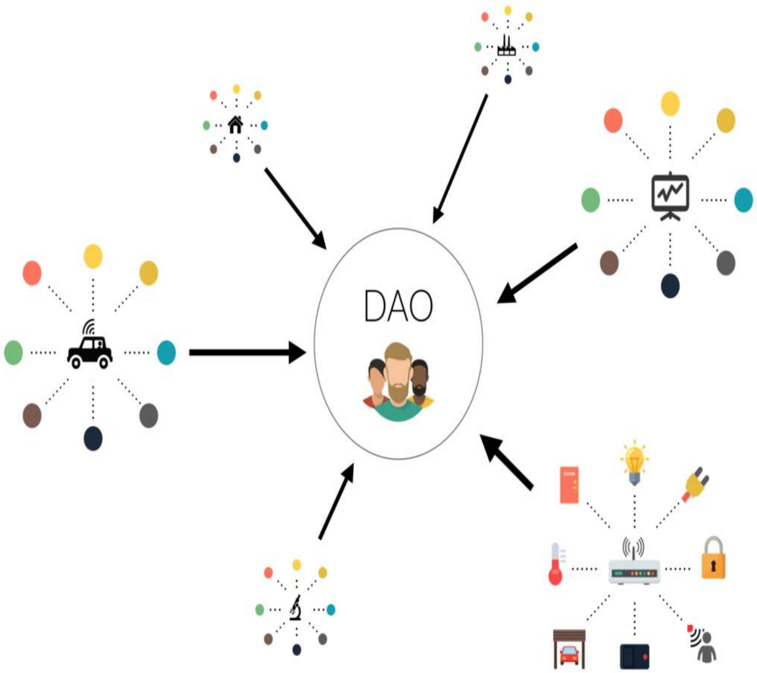
Many layers of management for coordination & enforcement of processes. Many information & decision bottleneck as well as sources of corruption.

Machine consensus around token governance rulsets and smart contracts instead of legal employment contracts.

BlockchainHub

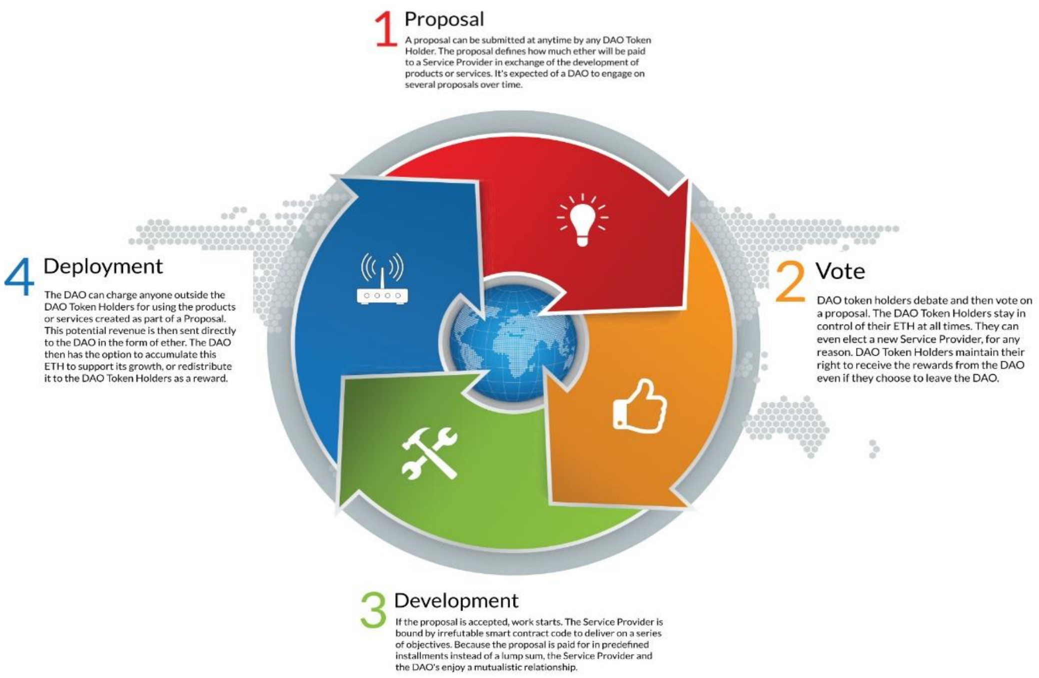
How DAOs work

- 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.



1 Proposal

A proposal can be submitted at anytime by any DAO Token Holder. The proposal defines how much ether will be paid to a Service Provider in exchange of the development of products or services. It's expected of a DAO to engage on several proposals over time.

2 Vote

DAO token holders debate and then vote on a proposal. The DAO Token Holders stay in control of their ETH at all times. They can even elect a new Service Provider, for any reason. DAO Token Holders maintain their right to receive the rewards from the DAO even if they choose to leave the DAO.

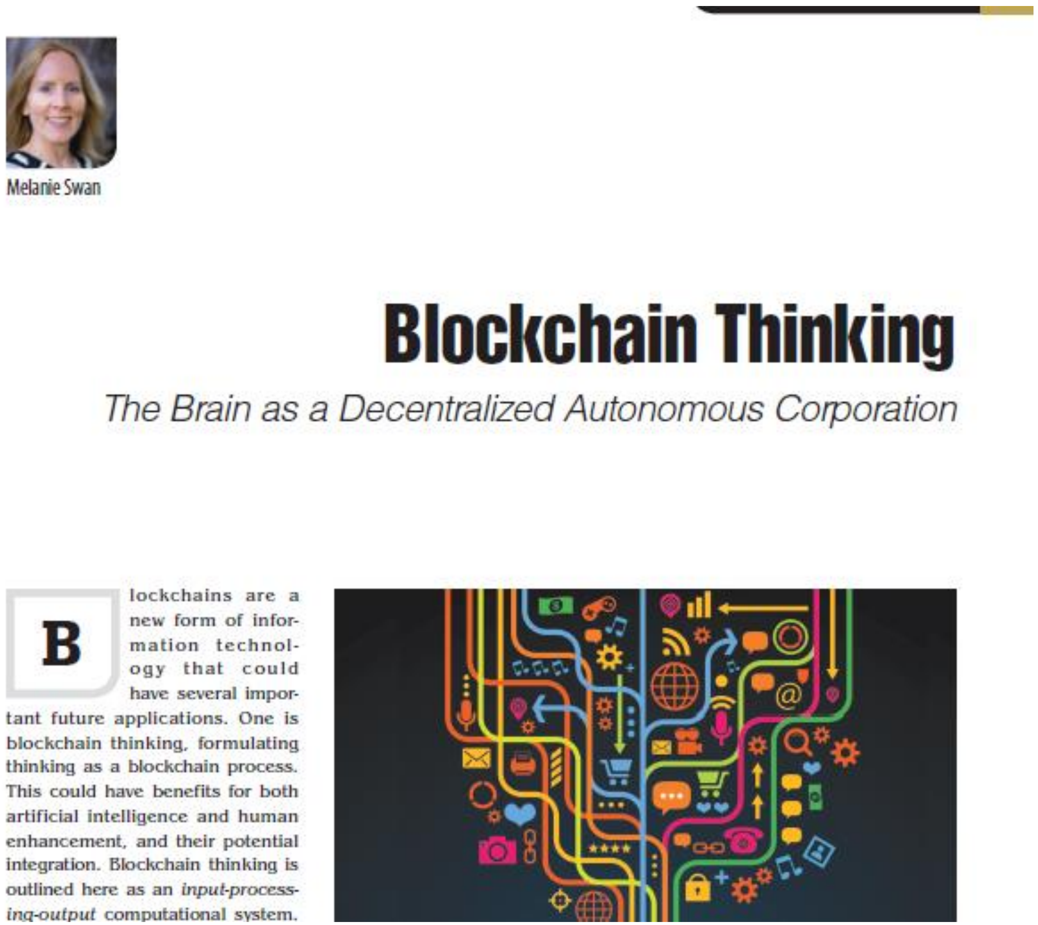
3 Development

If the proposal is accepted, work starts. The Service Provider is bound by irrefutable smart contract code to deliver on a series of objectives. Because the proposal is paid for in predefined installments instead of a lump sum, the Service Provider and the DAO's enjoy a mutualistic relationship.

4 Deployment

The DAO can charge anyone outside the DAO Token Holders for using the products or services created as part of a Proposal. This potential revenue is then sent directly to the DAO in the form of ether. The DAO then has the option to accumulate this ETH to support its growth, or redistribute it to the DAO Token Holders as a reward.

DAO ~ our Brain



Melanie Swan

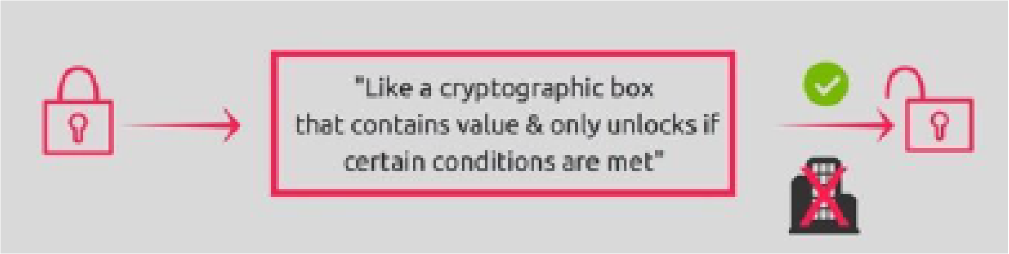
Blockchain Thinking

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.


"Like a cryptographic box
that contains value & only unlocks if
certain conditions are met"

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.

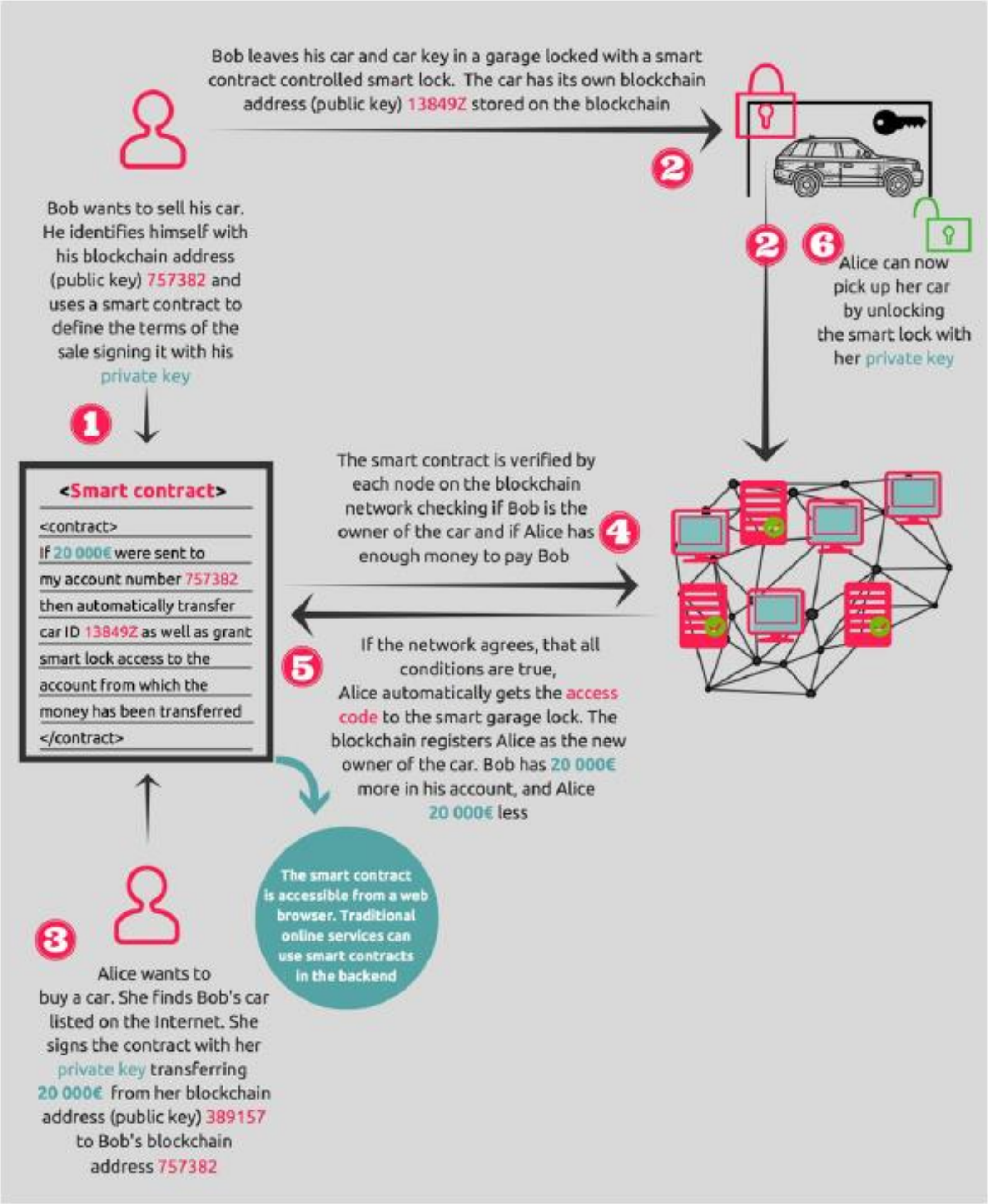
Buying a Car with Smart Contract

Smart contract

1. Seller's position. If conditions are met, ownership is transferred.
2. Buyer's position. Give money, get the car right away, get registered as the owner of the car.
3. …

Well, is this enough?

1. What about the car conditions?
2. Use of multisignature solves all problems?



1 Bob wants to sell his car. He identifies himself with his blockchain address (public key) 757382 and uses a smart contract to define the terms of the sale signing it with his private key

2 Bob leaves his car and car key in a garage locked with a smart contract controlled smart lock. The car has its own blockchain address (public key) 13849Z stored on the blockchain

<Smart contract>
<contract>
If 20 000€ were sent to
my account number 757382
then automatically transfer
car ID 13849Z as well as grant
smart lock access to the
account from which the
money has been transferred
</contract>

3 Alice wants to buy a car. She finds Bob's car listed on the Internet. She signs the contract with her private key transferring 20 000€ from her blockchain address (public key) 389157 to Bob's blockchain address 757382

The smart contract is accessible from a web browser. Traditional online services can use smart contracts in the backend

4 The smart contract is verified by each node on the blockchain network checking if Bob is the owner of the car and if Alice has enough money to pay Bob

5 If the network agrees, that all conditions are true, Alice automatically gets the access code to the smart garage lock. The blockchain registers Alice as the new owner of the car. Bob has 20 000€ more in his account, and Alice 20 000€ less

6 Alice can now pick up her car by unlocking the smart lock with her private key

Process of buying a car on the Blockchain

Source: Blockchainhub.net

유시민과 블록체인

유시민 작가는 역시 대단했습니다.
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 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 것 이지요. 왕성하게 활동한 회원들은 금전적인 가치도 보상으로 받게 되는 것 입니다.

Conclusion

- Many Possibilities of Blockchain
- Verified by the market are Bitcoin and Ethereum
- To explore new territory, experiments are needed

  with budgets and man power invested.
- Needed are the research on regulation as regulations should be kept at the minimal level and more emphasis shall be on cultivation of new ideas.
- Obvious regulations should be in place right away
  - Responsible investment culture
  - Improved clarity on exchange business and initial coin offerings
  - Price manipulation practice
  - Taxation on profits
  - Use of real name in cryptocurrency transaction? Security becomes problem.

References

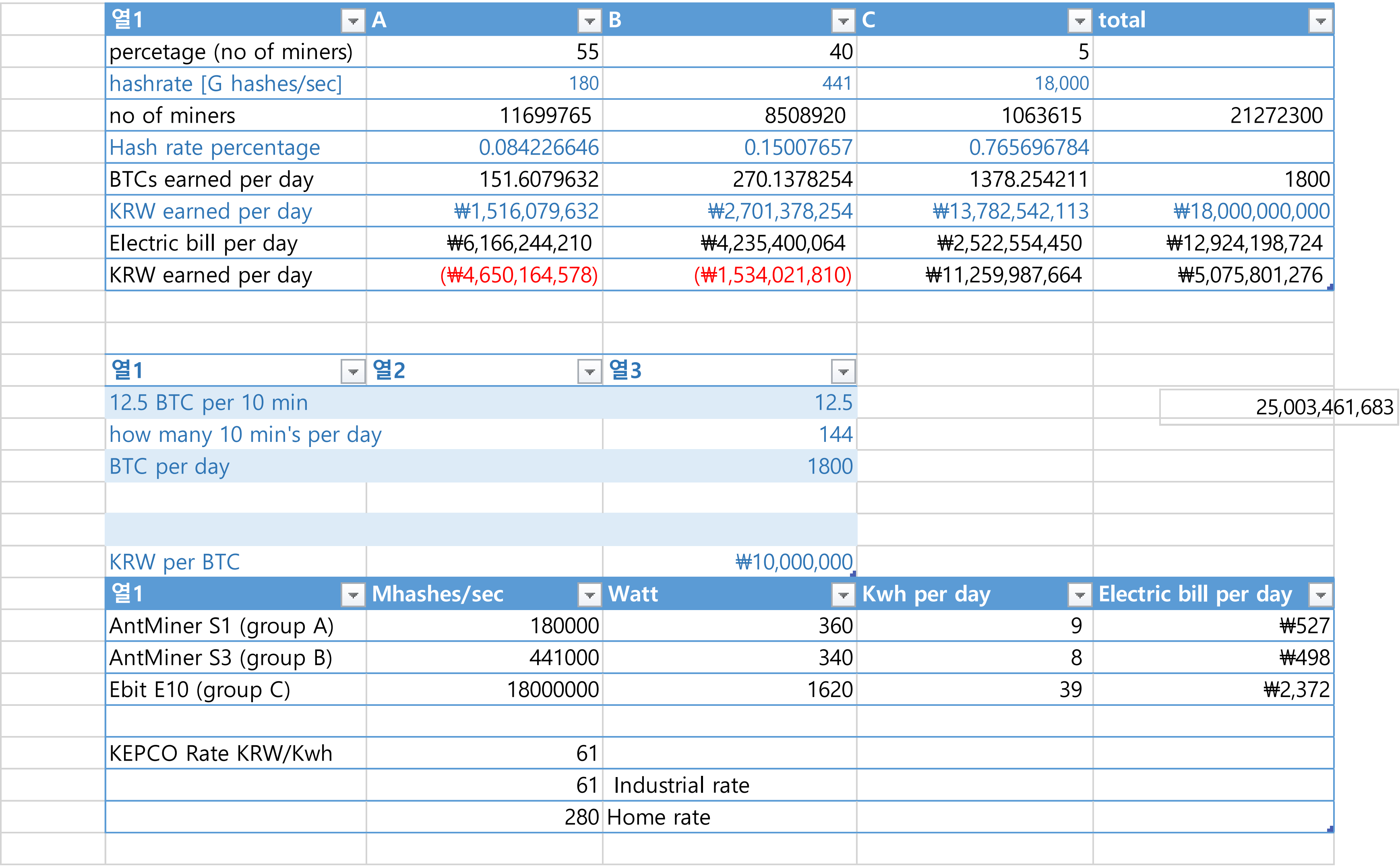
- 이흥노 교수 랩 블록체인페이지 https://infonet.gist.ac.kr/?page_id=6370.
- 박창기, “블록체인과 4차 산업혁명,” e-biz forum @Samsung Economy Research Institute, March 16, 2017.
- Blockchain.net
- Bitcoin.org
- Coursera course on Cryptocurrencies
- MIT Blockchain center
- Blockchain A beginner’s guide, Blockchain Hub
- Satoshi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

HW#1

- Problem 1: Suppose that there are only three groups of bitcoin miners in the bitcoin network.
- The first group A uses AntMiner S1 miners, second group B uses AntMiner S3, third group C uses Ebit E10.
- The percentage of each group is 1st 55%, 2nd 40%, and the third 5% in terms of numbers of miners.
- Provide an estimation on the total number of miners working in the bitcoin network today March 14th 2018.
- Give the number of miners in each group.
  - Use the reference for ASIC miners at https://en.bitcoin.it/wiki/Mining_hardware_comparison.
  - Use the estimated hashrate published at (https://bitcoinwisdom.com/bitcoin/difficulty).

- Problem 2: Use the setting from Problem 1. Find the probability of mining success per block or the percentage of the mining success per block of group C.
- What is the estimate amount of money the group C pays for electricity bill per day?
- What is the amount of money the group expects to earn for a day?
- Find the average rate at the on-line information post at Kepco and provide your source.
- Use this and give an estimate of the energy spent per day the bitcoin network consumes.

Solutions to Prob 1 & Prob 2



열1	A	B	C	total
percetage (no of miners)	55	40	5	
hashrate [G hashes/sec]	180	441	18,000	
no of miners	11699765	8508920	1063615	21272300
Hash rate percentage	0.084226646	0.15007657	0.765696784	
BTCs earned per day	151.6079632	270.1378254	1378.254211	1800
KRW earned per day	₩1,516,079,632	₩2,701,378,254	₩13,782,542,113	₩18,000,000,000
Electric bill per day	₩6,166,244,210	₩4,235,400,064	₩2,522,554,450	₩12,924,198,724
KRW earned per day	(₩4,650,164,578)	(₩1,534,021,810)	₩11,259,987,664	₩5,075,801,276

열1	열2	열3
12.5 BTC per 10 min		12.5
how many 10 min's per day		144
BTC per day		1800
KRW per BTC		₩10,000,000

25,003,461,683

열1	Mhashes/sec	Watt	Kwh per day	Electric bill per day
AntMiner S1 (group A)	180000	360	9	₩527
AntMiner S3 (group B)	441000	340	8	₩498
Ebit E10 (group C)	18000000	1620	39	₩2,372
KEPCO Rate KRW/Kwh	61			
	61	Industrial rate		
	280	Home rate		

HW#1

- Problem 3: (RSA Encryption/Decryption) Use the RSA Calculator on line. Suppose we use RSA for chain of signatures. Alice owns a Pizza shop. Bob wants to buy a Pizza (1000 Satoshi) from Alice using his bitcoin. (https://www.cs.drexel.edu/~introcs/Fa11/notes/10.1_Cryptography/RSAWorksheetv4d.html)

(a) Generate a private and public key pair for Bob. Show your answer.

(b) Do the same for Alice.

(c) Write down the sequences of events that must occur to complete the pizza ordering transaction. Start it with what Alice needs to do, and end it with the event that Alice sends the Pizza to Bob in delivery.

Answer to Prob 3

Please go to the Drexel web-site to create key pairs for both Bob and Alice.

I will use what Suwhan has found for the key generation parts.

- (a) Put in two prime numbers p=19 and q=41 to produce the key. Which gave me N=779 and r = 720. My candidate I chose for 1 mod r was 10081. The result for e and d were 17 and 593 each. Thus, public key for Bob is N=779 and e=17, and private key for Bob would be d=593.
- (b) This time the two prime numbers were p=71 and q=37. This time, N=2627, r=2520 and my candidate for 1 mod r was 22681, which then was factored into 37*613. The result for e and d was 37 and 613 each. Thus, public key for Alice is N=2627 and e=37, and private key for Alice is d=613.

Key Generation

- Pub-key is (*n*, *e*) and Pri-key is (*n*, *d*).
- With *p* and *q* not known public, it is very difficult to find what *d* is from public key (*n*, *e*).

1. Choose two primes $p = 61$ and $q = 53$.
2. Get $n = pq = 3233$.
3. Compute totient

$$\lambda(n{=}3233){=}\mathrm{lcm}(p\text{-}1, q\text{-}1)$$
$$=\mathrm{lcm}(60, 52)=780.$$

4. Choose a number e = 17, from 1 to 780, coprime to 780.
5. Compute d = 413, a multiplicative inverse of e mod $\lambda(n)$.

Key Generation

1. Choose two primes $p = 61$ and $q = 53$.

2. Get $n = pq = 3233$.

3. Compute totient

$$\lambda(n{=}3233){=}\mathrm{lcm}(p\text{-}1,\ q\text{-}1)$$
$$={\rm lcm}(60,\ 52){=}780.$$

4. Choose a number e = 17, from 1 to 780, coprime to 780.

5. Compute d = 413, a multiplicative inverse of e mod $\lambda(n)$.

- (c) Bob owns a 1K Satoshi at his public address. Now Bob wants to order a pizza from Alice who owns a pizza shop.

1. Alice advertises her public address (N=2627 and e=37) at her pizza shop.
2. Note that Bob's 1000 Satoshi has been stored to his public key in a previous transaction. Bob sends an e-mail to Alice in which an encrypted message is included. That is, he wants to order a pizza and he wants to pay for it with his 1000 Satoshi.
3. In the e-mail, Bob writes a message that says 1000 Satoshi stored in Bob's public key (N=779 and e=17) is transferred to Alice's public key (N=2627, e=37). Bob encrypts both the previous transaction and this message with Alice's public key (N=2627 and e=37). Bob also includes his digital sign. Digital sign is made by Bob who encrypts the encrypted message with his private key (d=593). Bob sends the encrypted message along with his digital sign to Alice in an e-mail.
4. The e-mail from Bob has arrived to Alice's e-mail box.
5. Alice decrypts the encrypted message with her private key (d=613). Alice finds Bob's public key (B=779, e=17) from the decrypted message and use it to verify Bob's digital sign. Verification is done by decrypting the digital sign by Bob's public key and making sure that the decrypted sign is the same as the encrypted message from Bob arrived in the e-mail.
6. After verification done, Alice sends Bob a pizza.

- The foregoing materials follows the suggestion of the Bitcoin white paper. Namely, a bitcoin is a chain of signature. But do you find any problem with this suggestion?

HW#1

- Problem 4: Use SHA-256. Bob has found that the input file x_0 has the hash value y_0.

(a) He select a file x_1 at random from his desktop computer and runs it thought SHA-256. What is the probability that this output is the same as the first output y_0?

(b) He does the experiment like (a) 10^6 times. What's the probability that he has found the same hash?

(c) How many repetition of experiments is required so that the probability he finds the same hash y_0 is greater than 1e-6.

(d) Repeating the question (c) but this time with a little change. Let us use a growing pool of all the produced hashes in previous experiments for comparison. That is, at the n-th experiment, the new hash y_n is to be compared with all the previously produced hashes that are distinct with each other, i.e., $\{y_0, y_1, y_2, \ldots, y_{n-1}\}$.

$$\boxed{\Pr(S > t) = e^{-\lambda t} \qquad \text{where } \lambda := \frac{p}{T}}$$

$$1 - p_k = 1 - \sum_{j=1}^{k} (1-p)^{j-1} p$$

$$= \sum_{j=k+1}^{\infty} (1-p)^{j-1} p$$

$$= (1-p)^k$$

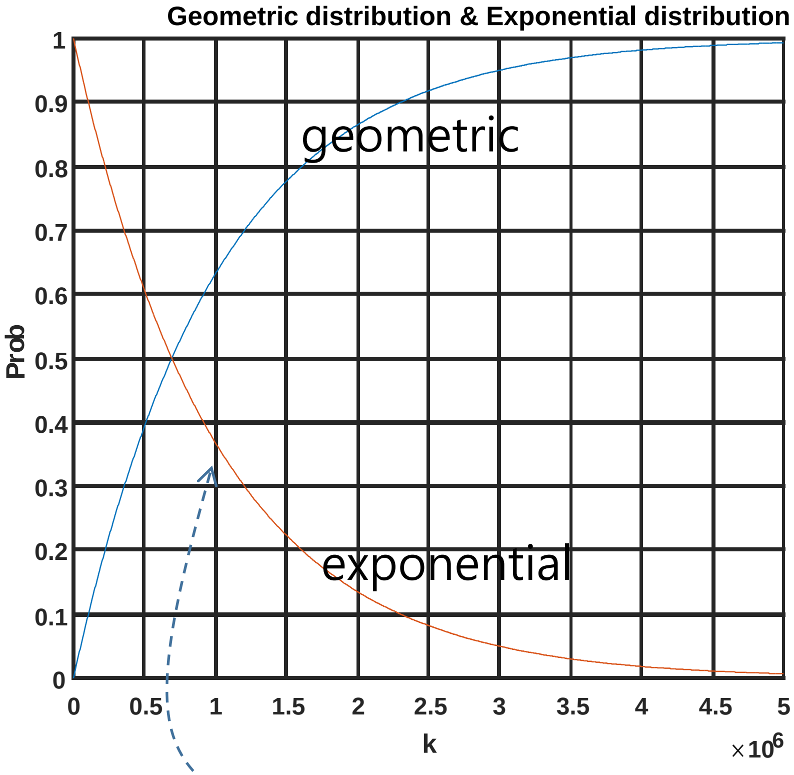
$$(1-p)^k = (1-p)^{\frac{1}{T}kT}$$

$$= (1-p)^{\frac{1}{p}\frac{p}{T}kT}$$

$$= \left\{(1-p)^{\frac{1}{p}}\right\}^{\frac{p}{T}kT}$$

$$= e^{-\frac{p}{T}kT}$$

$$= e^{-\lambda t}\Big|_{t=kT} \qquad \text{where } \lambda := \frac{p}{T}$$



$$e^{-\lambda t}\Big|_{t=kT} \qquad T = 1 \qquad p = 10^{-6}$$

HW#1

- Problem 5. Use Satoshi's paper and my lecture note #1 for these answers. Two or three line answers for each shall be enough.

(a) What is the definition of bitcoin?

(b) What is the double spending problem? How is it resolved in bitcoin network?

(c) What is the timestamp server?

(d) Write down your reasoning why blockchain provides data immutability.

(e) Is the data stored in blockchain really immutable?

(f) What is the kind of attack the bitcoin paper says is possible?

(g) Write down the sequence of events to mine a block?

(h) List the field types that needs to be recorded inside the blockheader?

(i) What is the byte size of the private and that of the public key used in Bitcoin?

(j) What is the meaning of signature in Satoshi's paper?

(k) Bob wants to send Alice a bitcoin. What are the three basic things that must be done to complete this transaction?

(l) Why do we need proof-of-work in bitcoin network?

(m) What is the benefit of eliminating the third party according to Satoshi?

(n) Who is doing the proof-of-work in bitcoin network?

(o) What is a hash cycle?

HW#1

- Problem 6

a. Define what a money is. Provide your source.

b. Define what currency is. Provide your source.

c. What is the current market price of a bitcoin? Is it expensive or cheap? Justify your answer.

d. Bitcoin intends to get rid of the bank and uses P2P network instead. What are the possible benefits of using P2P network, instead of a bank? What are the possible drawbacks? Justify your answer.

e. Does the fiat money such as KRW and USD have any intrinsic value? Why do you think they have a market value? Who or what decides their values?

Quiz #1

- Problem 1 (5pts) What is nonce in bitcoin? How is it used? Why do you need it?

- Problem 2 (5pts) In the bitcoin system, what do we mean by data immutability? Is it really immutable? If yes, how is it done? Justify your answer.

Quiz #1

- Problem 3 (10pts) The hashrate is 20Exa in bitcoin network. Use your hand calculation to provide an approximate answer to the following question. Just follow the order of magnitude. Let the first 20 hexadecimals be zeros for good block summary (the target hash).
- (a) The size of good hash output set $\mathcal{Y}$ in decimal number (cf 2^256 = 1.16e77).
  - Ny=2^(256-20*4)=9.6e52.
- (b) The size of the set of all the produced hashes in a month.
  - N1=Num_hashes_month = hashrate * 60* 60*24*30 = 5.18e22.
- (c) Now draw an input x at random and calculate the hash of x and compare with all the produced hashes. What is the probability that hash collision occurs?

Use the result in HW#1 solution for Prob. 4.

$$p = \frac{N_1\left(N_{x/y} - 1\right)}{N_x - N_1} \approx \frac{N_1 N_{x/y}}{N_x} = \frac{N_1}{N_y} = \frac{5.18e22}{1.16e77} \sim O(1e-55)$$