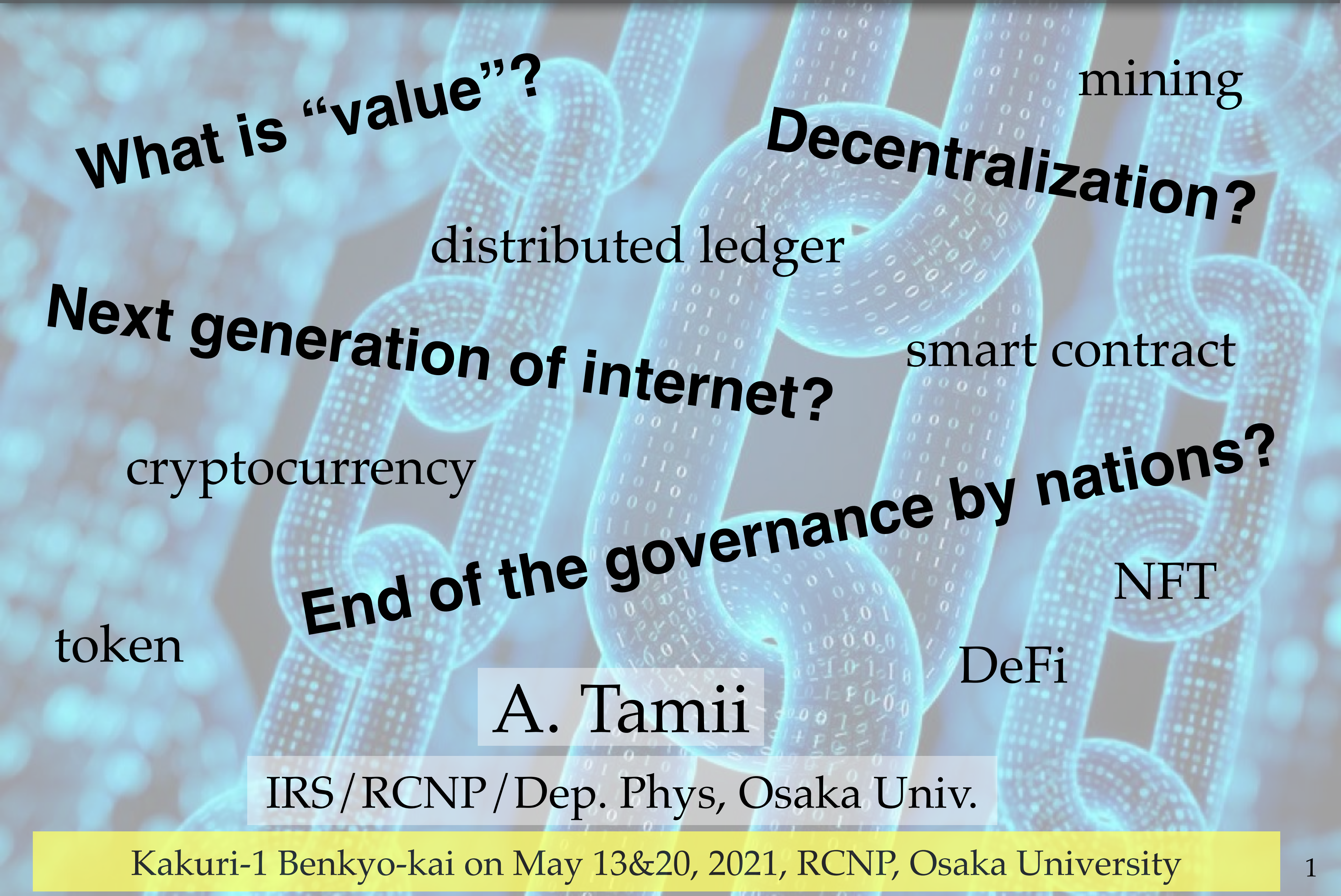
Blockchain Technology



mining

What is “value”?

Decentralization?

distributed ledger

Next generation of internet?

smart contract

cryptocurrency

End of the governance by nations?

NFT

token

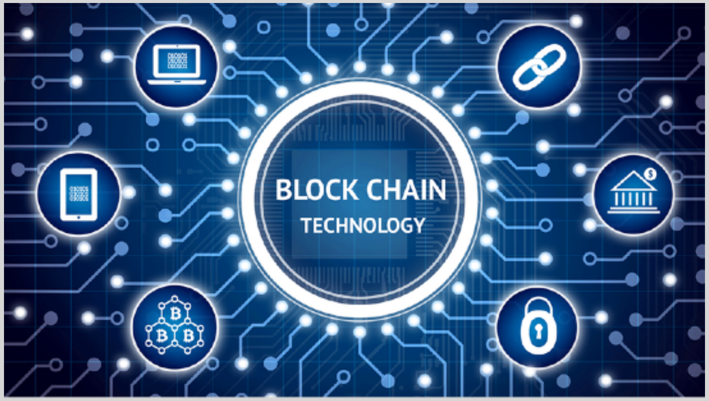
DeFi

A. Tamii

IRS / RCNP / Dep. Phys, Osaka Univ.

Kakuri-1 Benkyo-kai on May 13&20, 2021, RCNP, Osaka University

Blockchain Technology



Blockchain is a new revolutionary concept, originating from the information technology, that may bring a big impact on the human society in the coming ten years. It was innovated at the time of the birth of the cryptocurrency.

I plan to introduce the concept starting from its technological aspects up to a few real applications. Below I list two references but I will try to review the concept and the possible effects to the human society without following the contents of the references.

- S. Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, https://bitcoin.org/bitcoin.pdf

- *Ethereum White Paper*, https://ethereum.org/en/whitepaper/

Contents

I. Blockchain: a revolutionary technology

II. Technological background of a blockchain

Today

III. A second generation blockchain: Ethereum and smart contract

IV. Applications

V. Future and Summary

Next Week

I. Blockchain: a revolutionary technology

Blockchain: A Revolutionary Technology

Four Sacred Treasure (四種の神器) in the era of 5G.

IoT	Internet of Things	connecting everything via internet
Cloud	Cloud computing	software/platform/infrastructure *e.g.* AWS
AI	Artificial Intelligence	automation, optimization, etc
Blockchain	Distributed Ledger (分散台帳)	**decentralization** (非中央集権化)

Blockchain is regarded as the "last boss" of the new generation technologies that may bring a breaking transformation to the human society.

Blockchain was born with the cryptocurrency

Satoshi Nakamoto posted a concept of realizing a currency that was not controlled by the government (2008).

S. Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System

> "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**."

It allows people to exchange currency (or value) without giving commission to financial institutions.

no commission

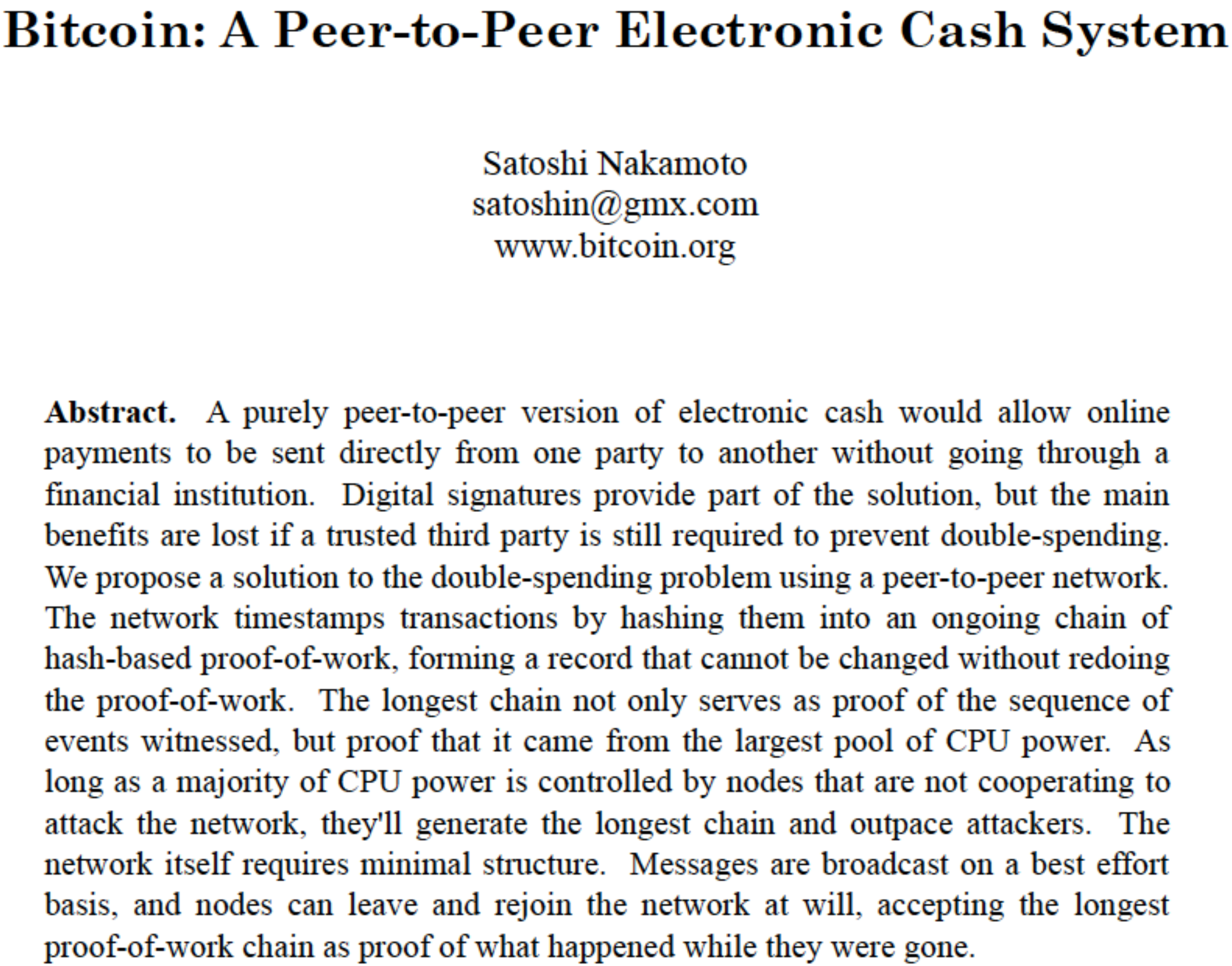
zero marginal cost

small latency

- Birth of the concept of the **blockchain**.
- **Cryptocurrency** as the first application.

仮想通貨/暗号資産

Bitcoin (2009)



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.

S. Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System

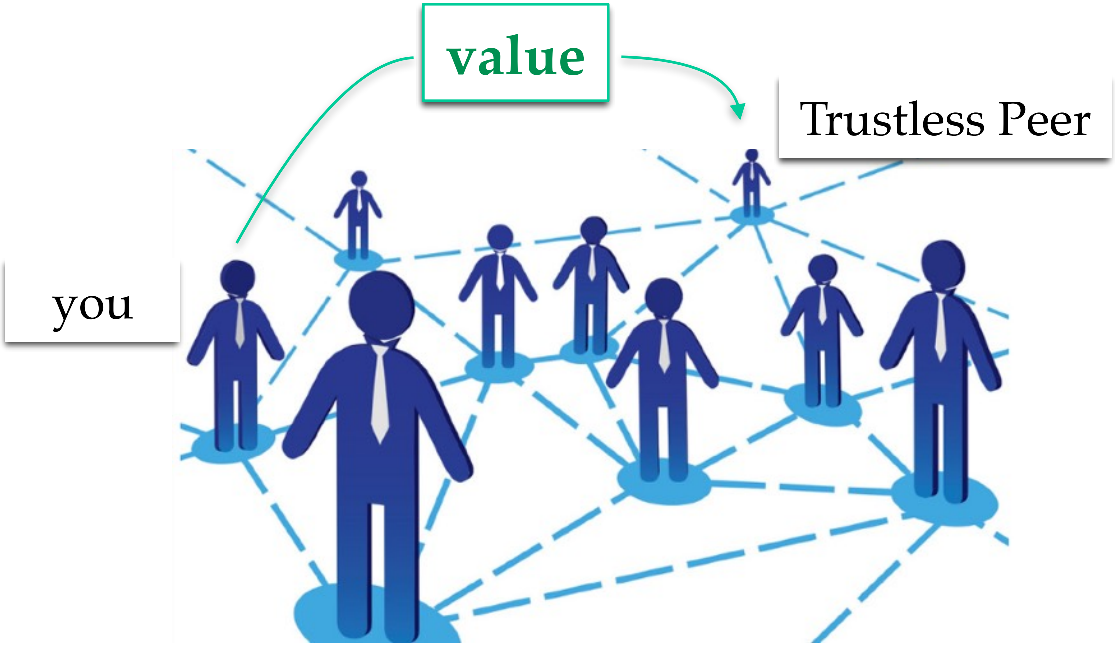
Blockchain: combined sophisticated concepts

Blockchain is sophisticatedly built up with the following information technologies.

- Prototype concept of **chained blocks**
- Cryptography: **Hash** and **Asymmetric Key**
- Game theorem: **Consensus** and **Incentives**
- **Proof of Work**
- **Distributed System**

Trust Protocol over Trustless Decentralized Network

The key innovation of the blockchain is a ***Trust Protocol***, realizing **reliable transaction** of value (currency) between **trustless peers** via a **trustless network** without an authorized institution (**decentralization**)



value

Trustless Peer

you

Decentralized Trustless Network

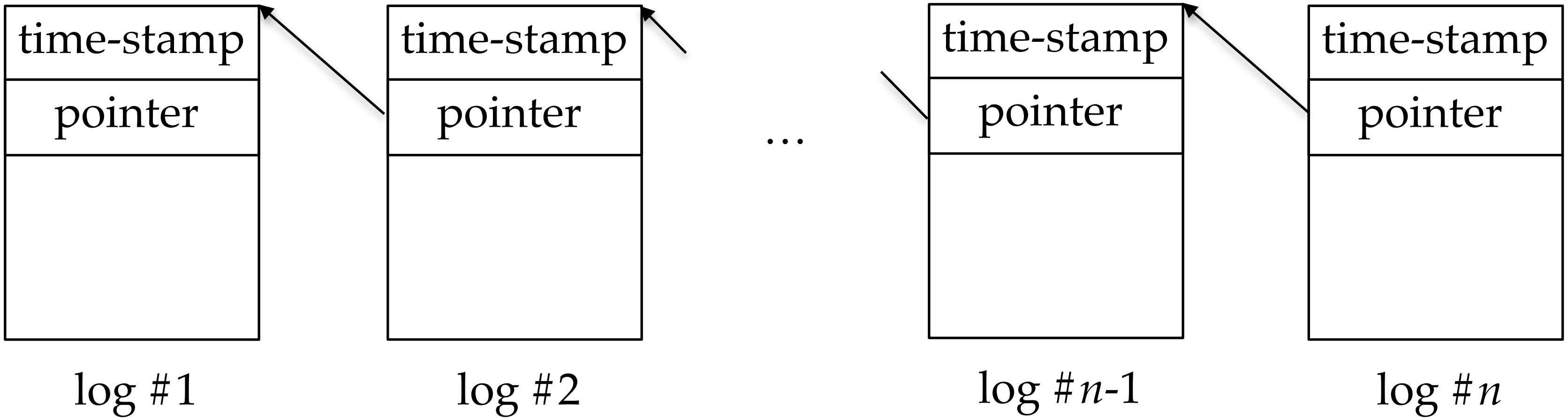
How can it be realized!

… Let’s see.

II. Technological background of a blockchain

Simplest Explanation of a Blockchain

A blockchain is **a chain of time-stamped append-only logs**

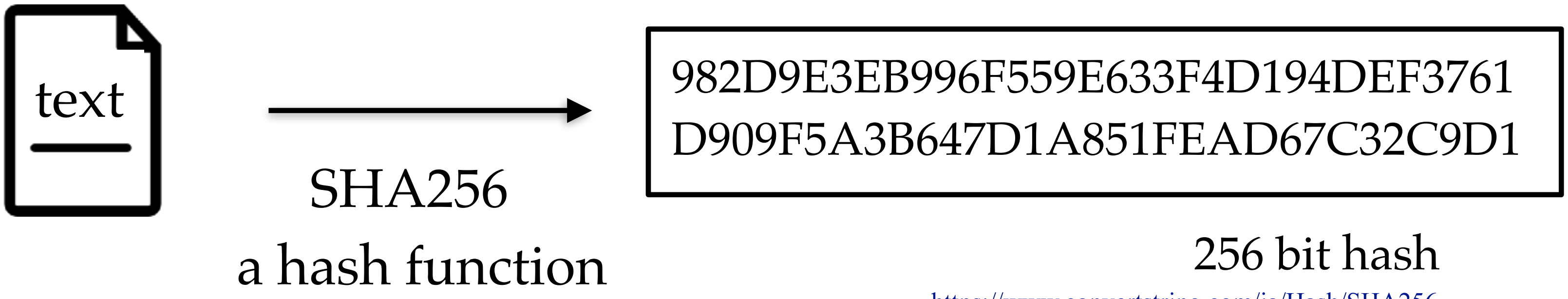


ordered by the time-stamp.

"Hash" of the previous block (log) is used as the pointer in the next block.

A *hash* is a fingerprint of a message of any length

A *Hash* is a fingerprint (digest) of a message of any length.



text

SHA256

a hash function

982D9E3EB996F559E633F4D194DEF3761
D909F5A3B647D1A851FEAD67C32C9D1

256 bit hash

https://www.convertstring.com/ja/Hash/SHA256

c.f. hash-table / message digest

- The hash transformation is **reproducible**.
- The hash transformation is **computationally efficient**.
- Any **small change** in the input results in a **complete change** in the output.
- Reverse transformation is impossible.

It is practically **impossible to create an input that has a specified hash output**.

How difficult is creating fake data with a specified hash value?

In the case of 256 bit has, the number of combinations is $2^{256} \sim 10^{77}$

The present *mining* factories of Bitcoin test, in total, $\sim 10^{20}$ hash/sec.

→ 10^{57} sec = $\sim 10^{49}$ years are required to create a fake input having a specified hash value.

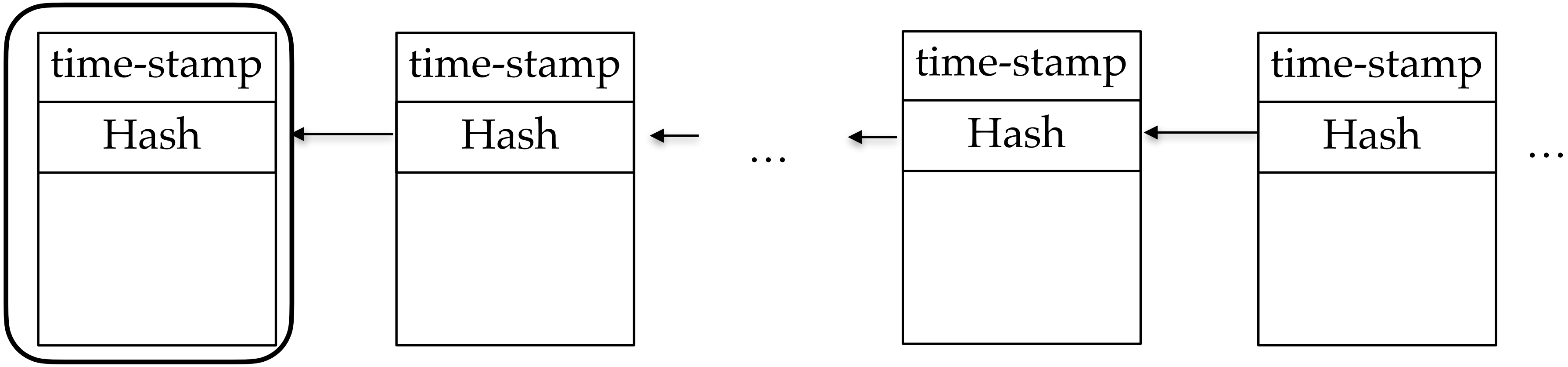
→ $\mathrm{sqrt}(10^{77})/10^{20}$ sec = $\sim 10^{18}$ years are required to have a collision in produced hashes.

256 bit would be sufficiently large in the life of the present blockchains.

Hereafter, I simply use the word “impossible” to express “practically impossible”.

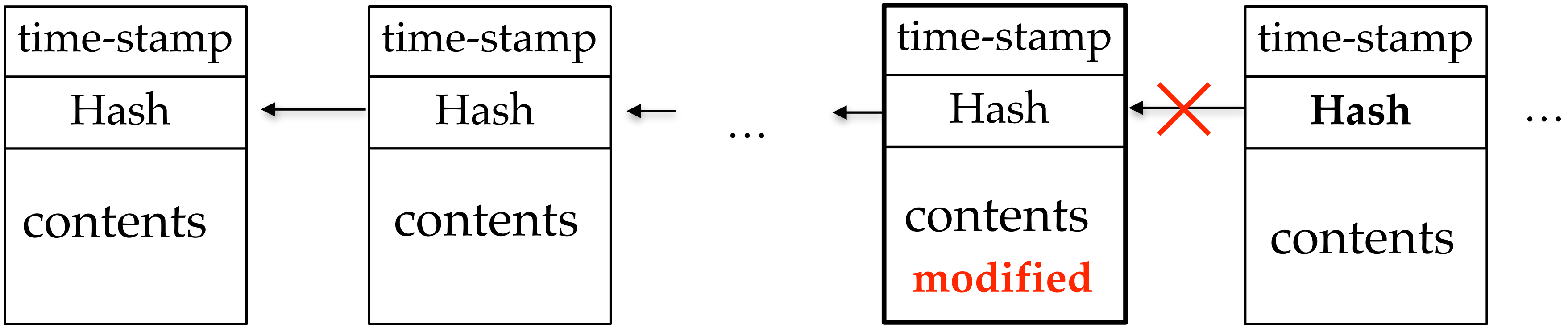
Blockchain with a hash pointer to the previous block

A blockchain with a hash as a pointer to the previous block.



What is the merit?

It is impossible to tamper a block that has a following block.



Any modification of a block produces inconsistency with the hash in the following block.

tamper resistance

How to get consensus when adding a block at the end?

How to get a consensus when adding a new block?

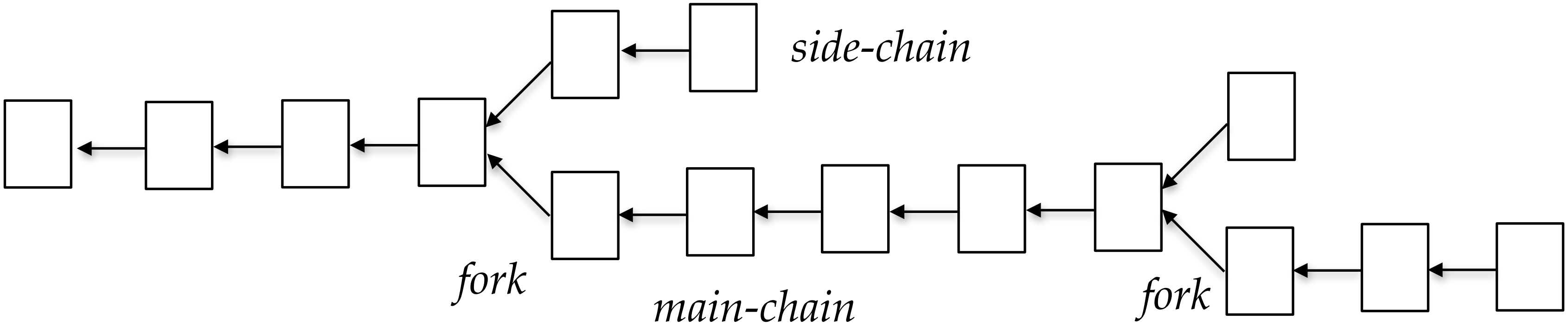
- The information on **the entire blockchain is shared by all the participants (nodes)**.

distributed ledger

- A new block is essentially added by ***first come***.
  However, **a computationally demanding puzzle** needs to be solved to add a block.

implementation of "Proof of Work"

- When two or more blocks are added to a block (***fork***), **the longest chain is regarded as the "true" chain**. Practically, a side-chain is terminated in 2-3 blocks and a fork is safely taken as the main-chain after having ~6 succeeding blocks.

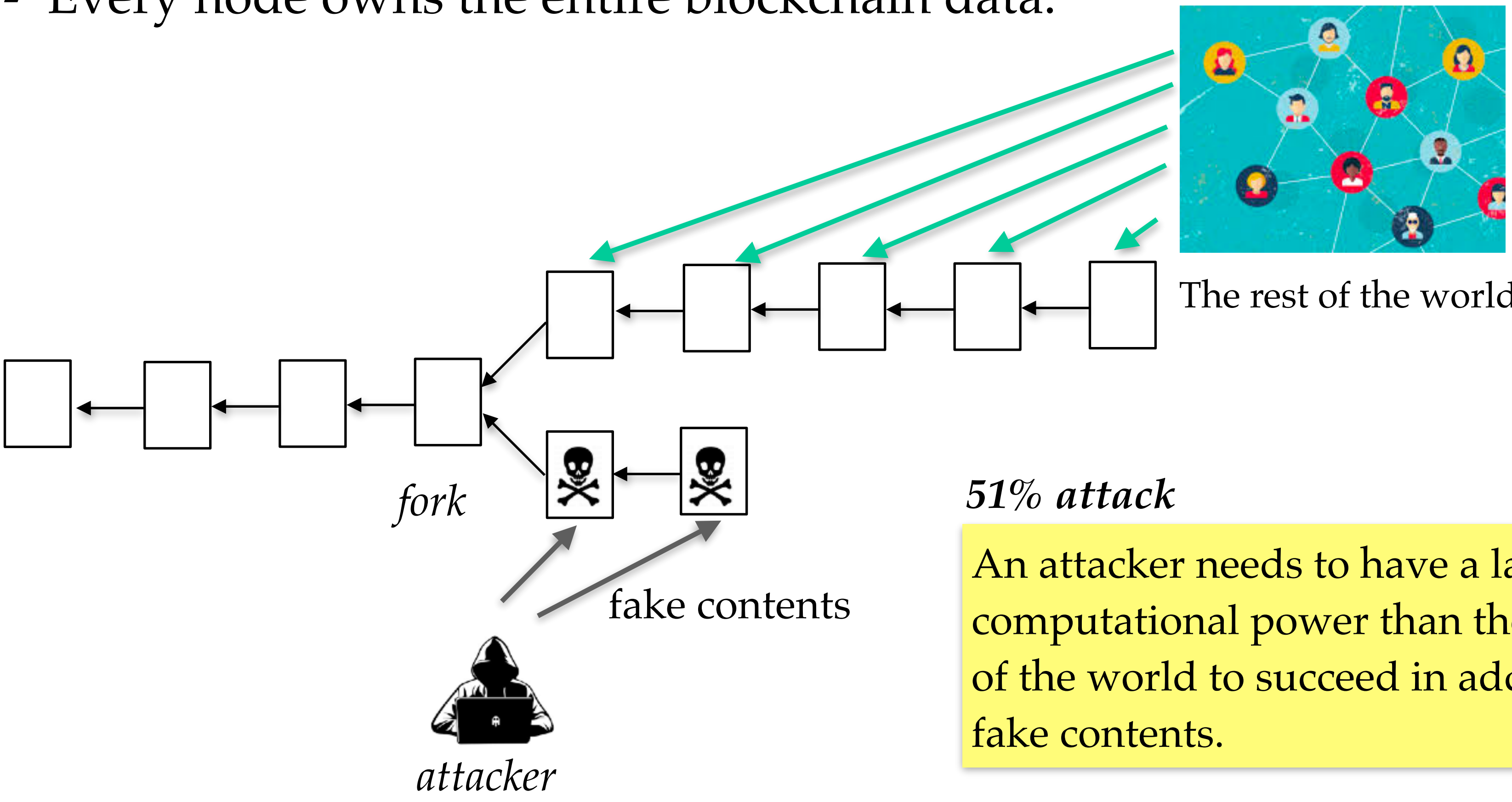


still not decisive which is the main chain

Resistance to Attacks

Key points

- Proof of Work: adding a block costs a significant computational power
- The longest chain is regarded as the main-chain
- Every node owns the entire blockchain data.



The rest of the world is faster.

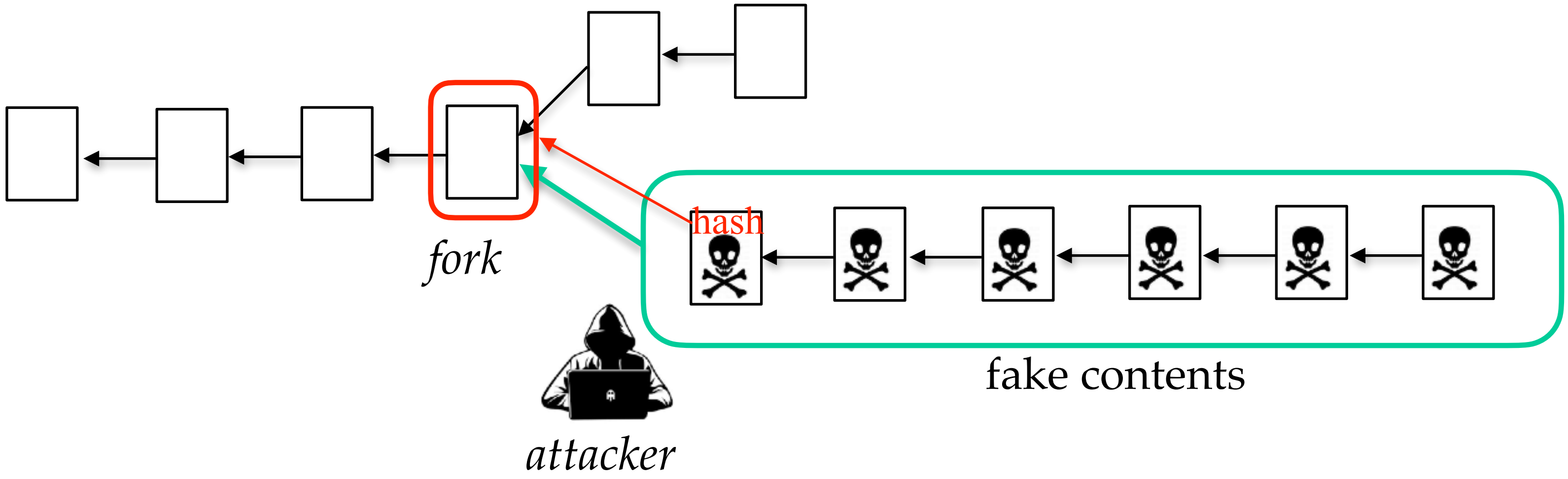
51% attack

An attacker needs to have a larger computational power than the rest of the world to succeed in adding fake contents.

Resistance to Attacks

Key points

- Proof of Work: adding a block costs a significant computational power
- The longest chain is regarded as the main-chain
- Every node owns the entire blockchain data.



An attacker might prepare many blocks and add them together to the blockchain.

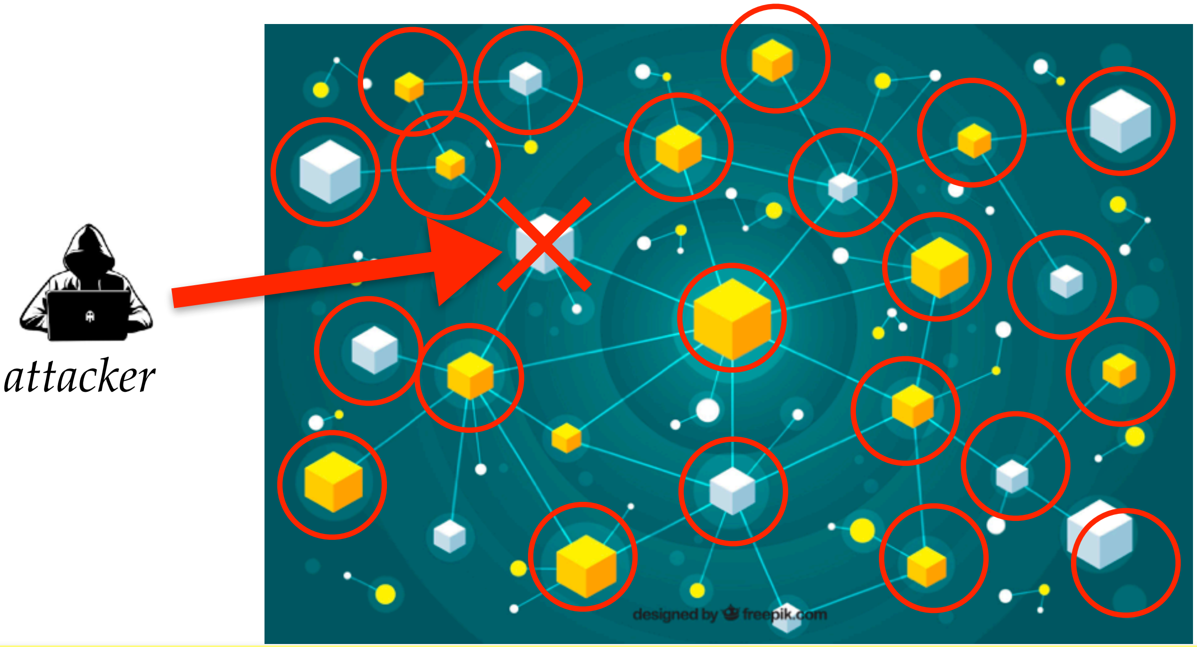
→ Fails ∵ The first prepared block needs to contain the hash of a block in the main chain.

Consequently, blocks can only be prepared by the order of the chain.

Resistance to Attacks

Key points

- Proof of Work: adding a block costs a significant computational power
- The longest chain is regarded as the main-chain
- Every node owns the entire blockchain data.



It means that the system is also resistive to the unexpected failure in any part of the system.

Resistance to system failure.

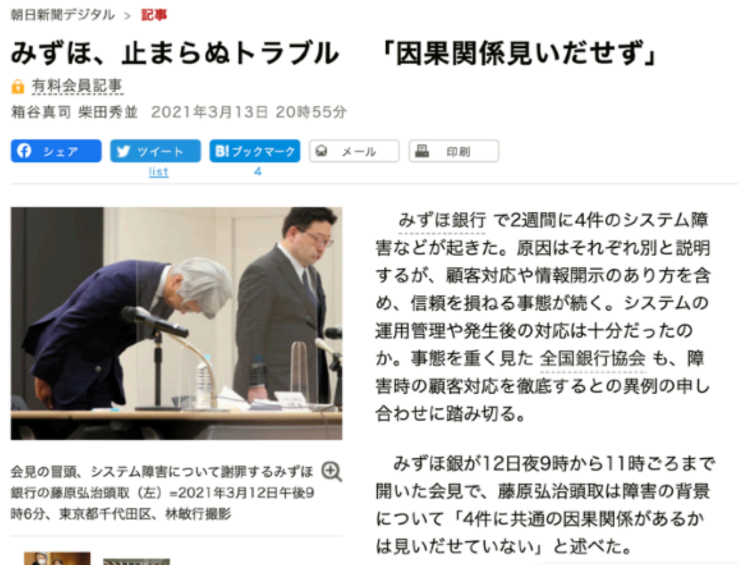
distributed ledger

An attacker might destroy a node and rewrite entirely the blockchain

→ Fails ∵ All the contents are distributed to all the nodes.
The attacker must rewrite the data simultaneously in more than half of the nodes.

Tolerance for System Failures

Mizuho ATM System Down
Asahi newspaper 2021.3.12



朝日新聞デジタル ＞ 記事

みずほ、止まらぬトラブル　「因果関係見いだせず」

有料会員記事

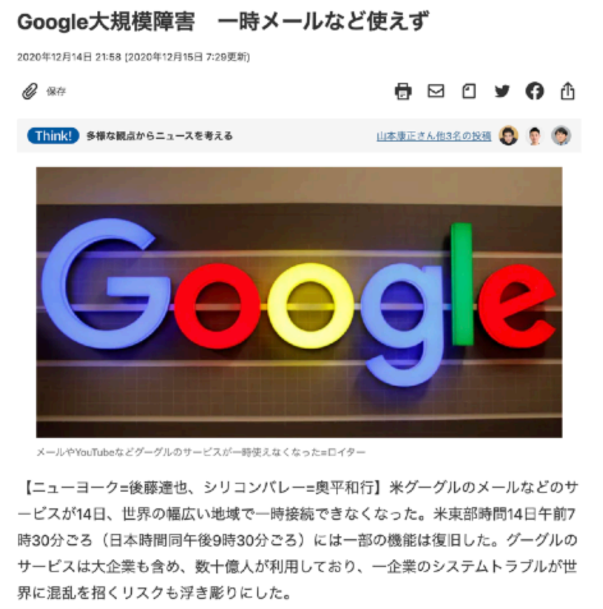
箱谷真司 柴田秀並　2021年3月13日 20時55分

会見の冒頭、システム障害について謝罪するみずほ銀行の藤原弘治頭取（左）＝2021年3月12日午後9時6分、東京都千代田区、林敏行撮影

みずほ銀行 で2週間に4件のシステム障害などが起きた。原因はそれぞれ別と説明するが、顧客対応や情報開示のあり方を含め、信頼を損ねる事態が続く。システムの運用管理や発生後の対応は十分だったのか。事態を重く見た 全国銀行協会 も、障害時の顧客対応を徹底するとの異例の申し合わせに踏み切る。

みずほ銀が12日夜9時から11時ごろまで開いた会見で、藤原弘治頭取は障害の背景について「4件に共通の因果関係があるかは見いだせていない」と述べた。

Google System Down
Nikkei newspaper 2020.12.14



Google大規模障害　一時メールなど使えず

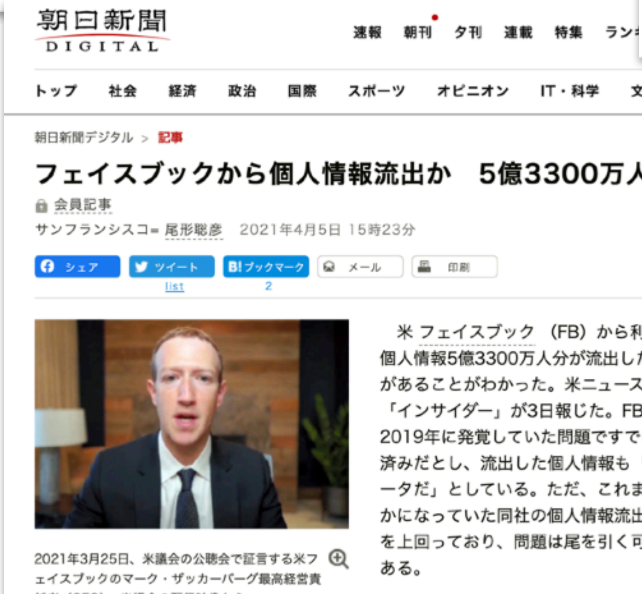
2020年12月14日 21:58 [2020年12月15日 7:29更新]

メールやYouTubeなどグーグルのサービスが一時使えなくなった＝ロイター

【ニューヨーク＝後藤達也、シリコンバレー＝奥平和行】米グーグルのメールなどのサービスが14日、世界の幅広い地域で一時接続できなくなった。米東部時間14日午前7時30分ごろ（日本時間同午後9時30分ごろ）には一部の機能は復旧した。グーグルのサービスは大企業も含め、数十億人が利用しており、一企業のシステムトラブルが世界に混乱を招くリスクも浮き彫りにした。

Information leakage
from Facebook

Asahi newspaper 2021.4.5



朝日新聞デジタル ＞ 記事

フェイスブックから個人情報流出か　5億3300万人分

会員記事

サンフランシスコ＝尾形聡彦　2021年4月5日 15時23分

2021年3月25日、米議会の公聴会で証言する米フェイスブックのマーク・ザッカーバーグ最高経営責

米 フェイスブック （FB）から利用者の個人情報5億3300万人分が流出した可能性があることがわかった。米ニュースサイト「インサイダー」が3日報じた。FBは2019年に発覚していた問題ですでに対処済みだとし、流出した個人情報も「古いデータだ」としている。ただ、これまで明らかになっていた同社の個人情報流出の規模を上回っており、問題は尾を引く可能性がある。

It is impossible to achieve complete tolerance by a centralized system

Information Security / Privacy

Blockchain, a genuine decentralized distributed system, can **achieve** a practically-**complete tolerance**.

No system down

No loss of data

No tamper

Blockchain is an **open system**, sharing all the data among the participating nodes.

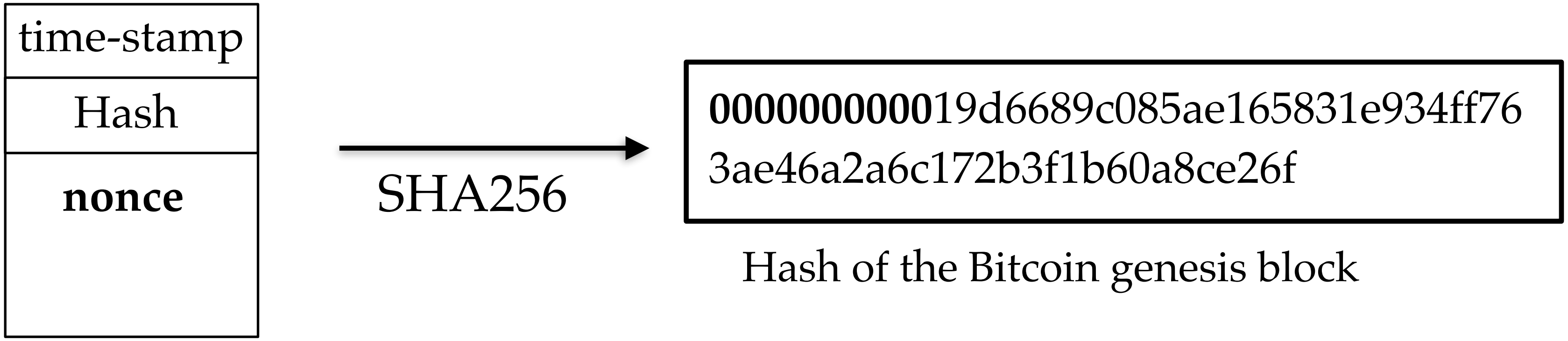
Privacy of the users is achieved by the ***anonymity* of each address or account**.
匿名性

The anonymity is not ensured by the blockchain itself.

Consensus Algorithm: *Proof of Work*

- *Proof of Work* is one of the consensus algorithms. It is applied in popular blockchains, *e.g.* Bitcoin and Ethereum 1.0.

Bitcoin Blockchain



000000000019d6689c085ae165831e934ff76
3ae46a2a6c172b3f1b60a8ce26f

Hash of the Bitcoin genesis block

A block is required to have **a hash starting from zeros of the specified length**.

In order to add a block, a **validator node (*miner*)** needs to find an appropriate ***nonce*** number to fulfill the requirement.

The length of the zeros, called ***difficulty***, is dynamically controlled to produce, on the average, a new block in 10 minutes depending on the available computational power.

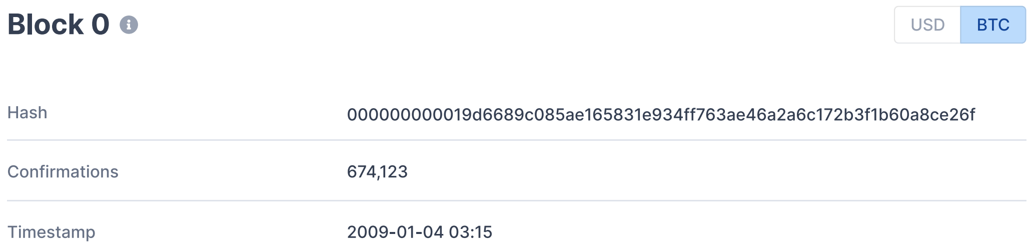
The difficulty is automatically adjusted after every 2016 blocks by comparing the averaged mining time with 10 minutes.

Proof of Work: Adam Back 1997

Bitcoin Genesis Block

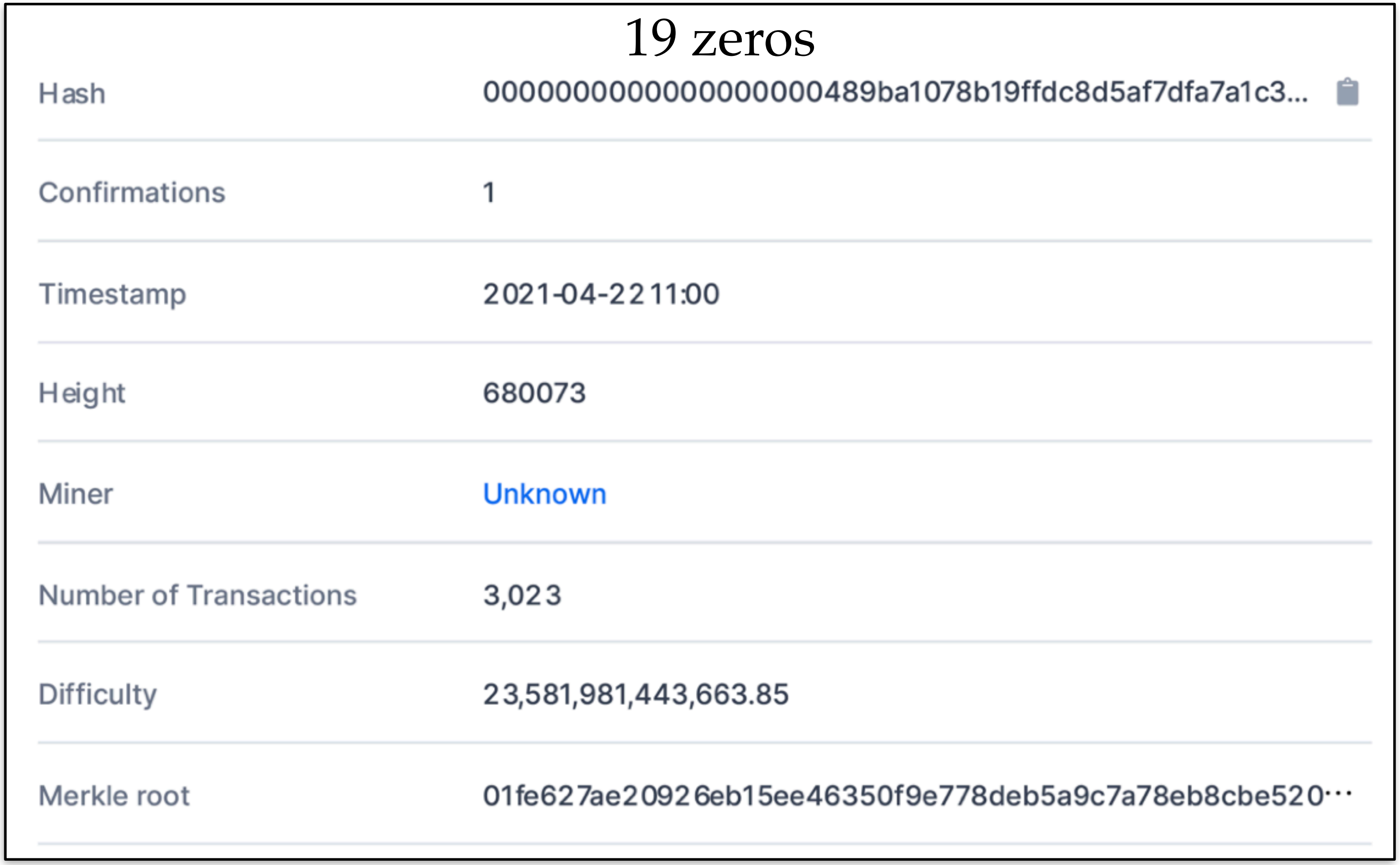
10 zeros

hash: 000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f



Block 0

Hash	000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f
Confirmations	674,123
Timestamp	2009-01-04 03:15



19 zeros

Hash	0000000000000000000489ba1078b19ffdc8d5af7dfa7a1c3...
Confirmations	1
Timestamp	2021-04-22 11:00
Height	680073
Miner	Unknown
Number of Transactions	3,023
Difficulty	23,581,981,443,663.85
Merkle root	01fe627ae20926eb15ee46350f9e778deb5a9c7a78eb8cbe520…

The Times 03/Jan/2009
Chancellor on brink of
second bailout for banks.

London Times

「財政担当大臣　二度目の銀行救済策目前」

Incentives: Stability of the Framework

Why do the validator nodes (miners) contribute to the computational work?

A blockchain produces a ***Token*** that is exchangeable among the participants.

A specified amount of **token is given** to the successful validators.

The token gives ***incentives*** (motivation) to the validators.

The Bitcoin blockchain uses the token as currency, that is the Bitcoin cryptocurrency.

The token value

- **Increases** as the participants **honestly contribute to** the blockchain framework.

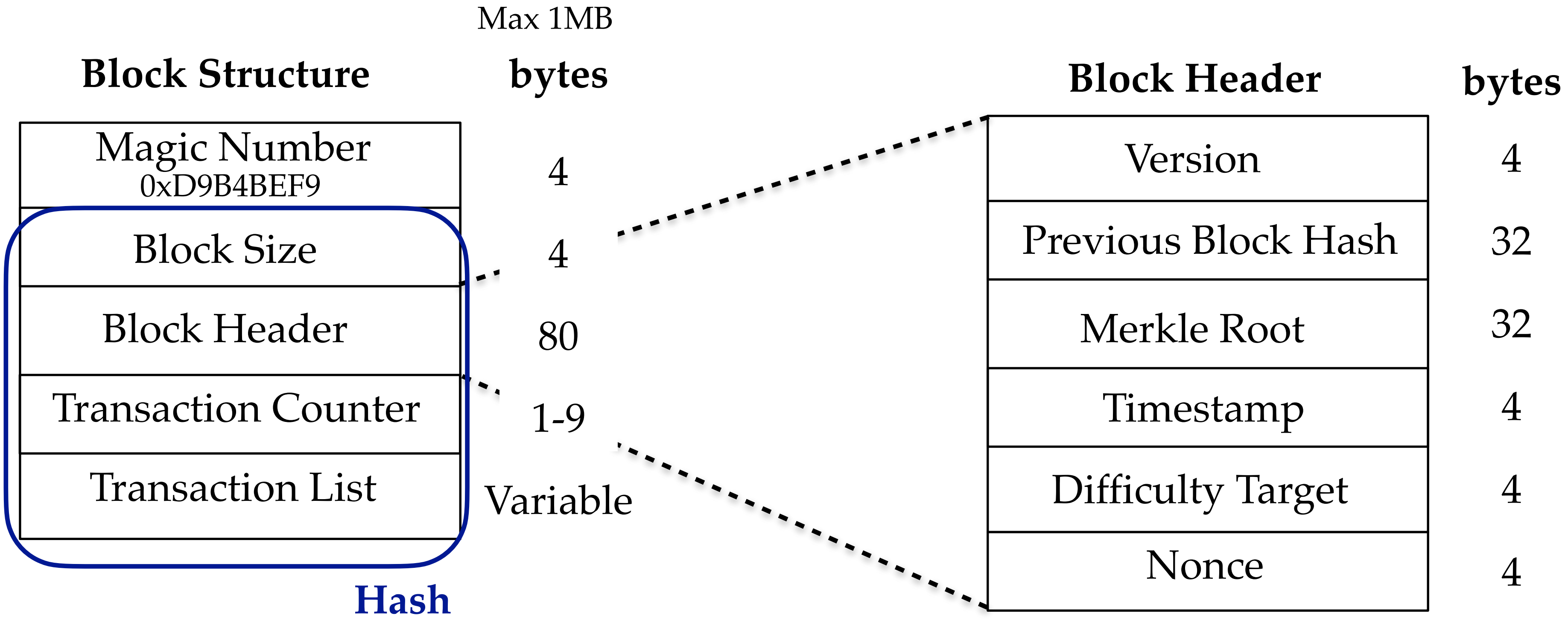
  Positive incentives for the supports

- **Decreases** if an attacker **destroys the framework** or its reliability.

  Negative incentives for the attacks

  No merit of destroying the token value that one has by wasting an enormous computational resource.

Bitcoin Block Structure



Block Structure	Max 1MB bytes
Magic Number 0xD9B4BEF9	4
Block Size	4
Block Header	80
Transaction Counter	1-9
Transaction List	Variable

Block Header	bytes
Version	4
Previous Block Hash	32
Merkle Root	32
Timestamp	4
Difficulty Target	4
Nonce	4

Bitcoin on April 2021

Average transactions per block: ~2,200

Total blockchain size: ~340 GB

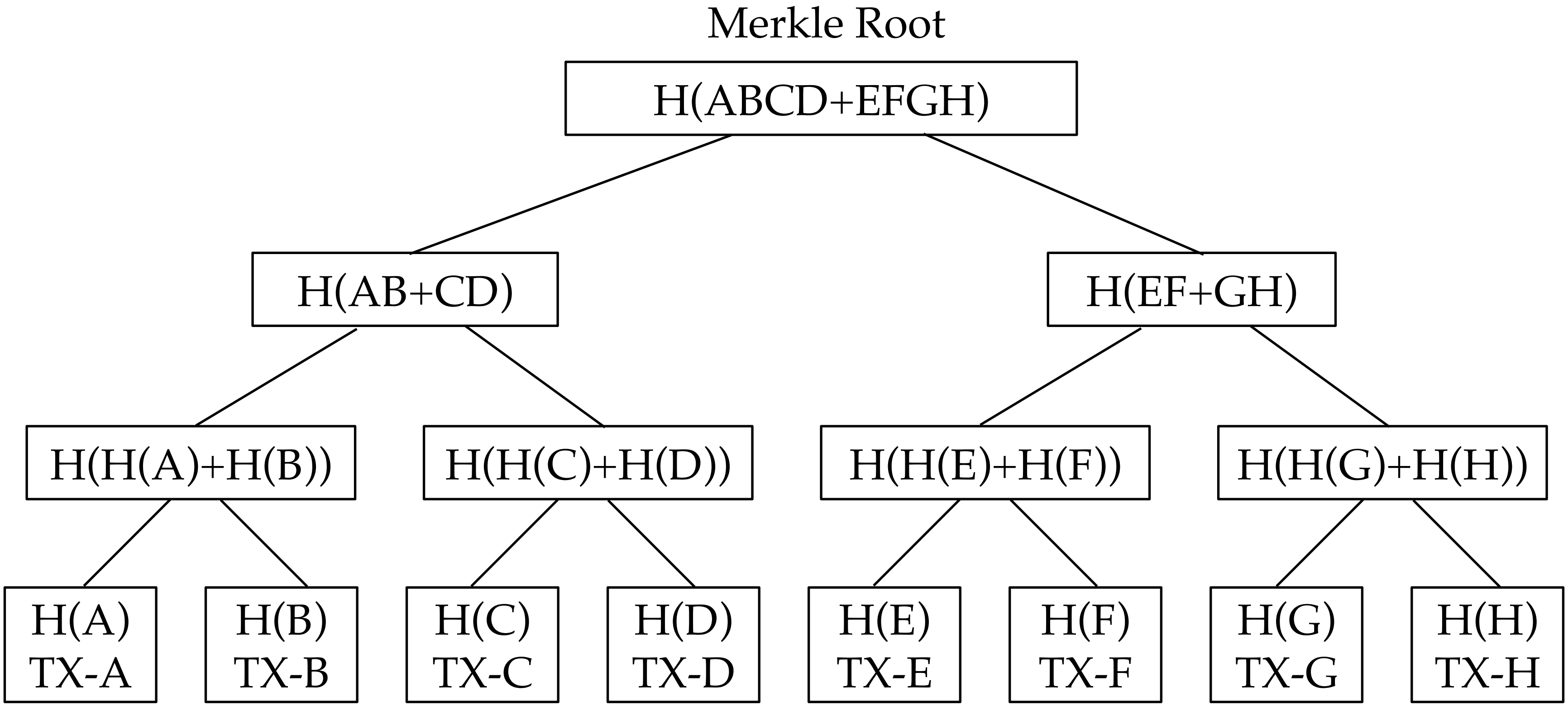
Total hash rate: 1.72×10^{20}/sec

Total number of blocks: 680,245

Total number of transactions: 6.36×10^{8}

Number of unused transactions (UTXO): 7.82×10^{7}

Merkle Root: Group of Transactions

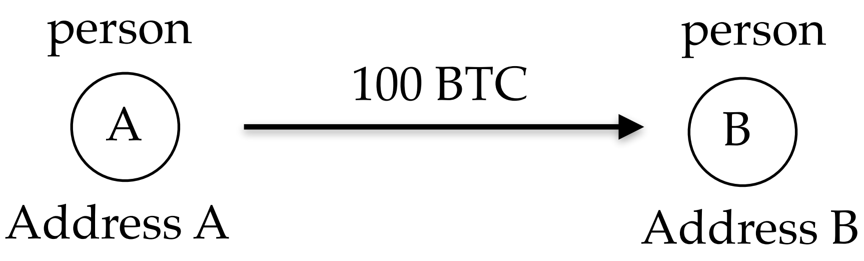


Merkle Root is the root hash of a binary (*trie*) tree of transactions.
Any modification in a transaction changes the value of Merkle Root

※Bitcoin uses Merkle tree while Ethereum uses Merkle-Patricia tree.

Transactions in the Bitcoin blockchain

A transaction of Bitcoin



Items needs to be ensured:

1) 100 BTC **has been sent from** the Bitcoin address **A**.

2) The sent 100 BTC **can** only **be used by** the owner of the address **B**.

For 1), the transaction is signed by the owner of the address A.

The owner of the address A cannot deny the usage of the money.

For 2), the transaction input has

- the public key of A that can validate the digital signature of A
- the receiver address B is signed by A.

Digital Signature

※Bitcoin has only transactions without accounts.

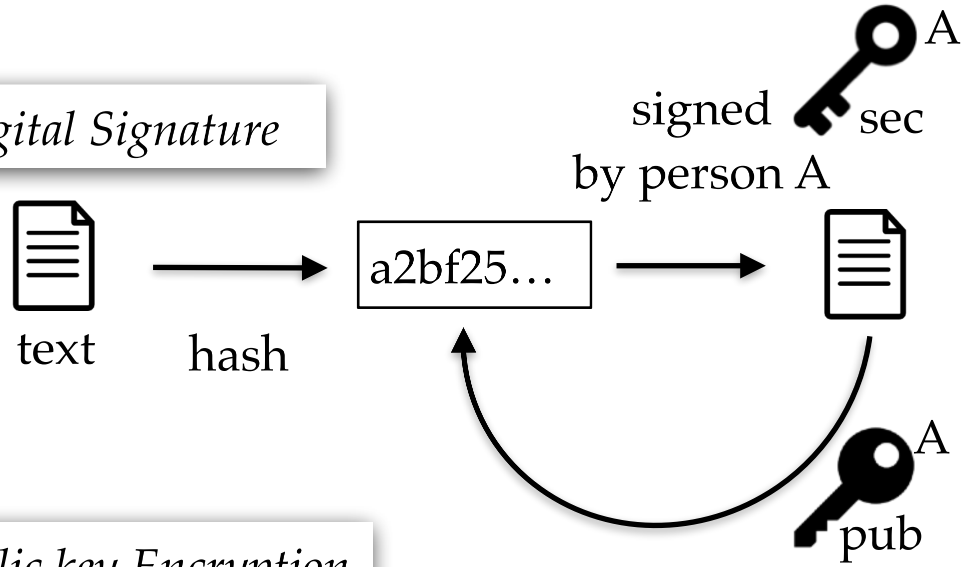
Asymmetric Key Cryptography

Each person produces a pair of a secret key and a public key.

sec Only the owner knows

pub Open to the public

Digital Signature



text

hash

a2bf25…

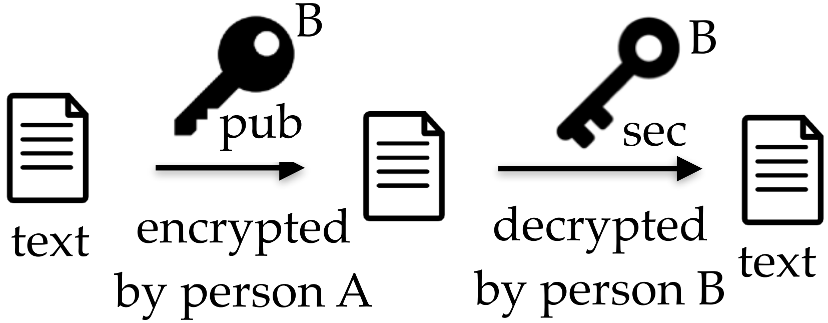
signed by person A

A sec

A pub

Anyone can check that the person A has agreed with the text by using the public key of A.

Public key Encryption



text

B pub

encrypted by person A

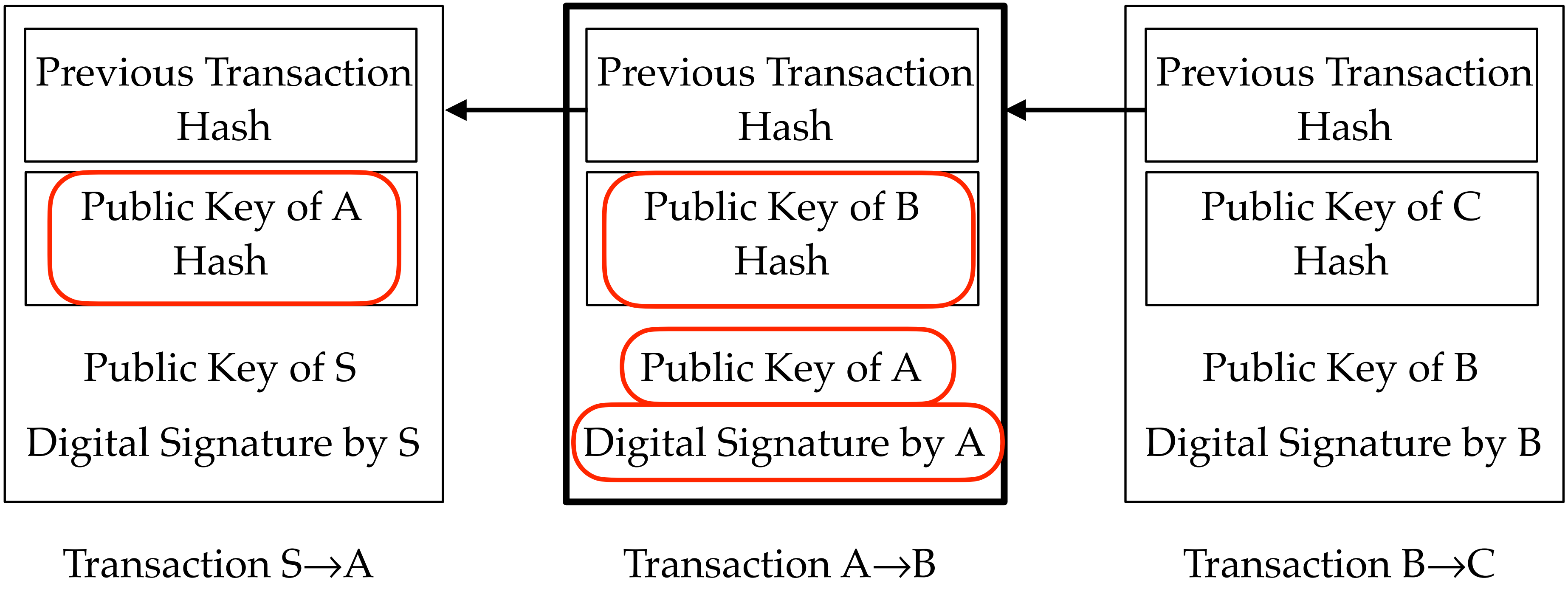
B sec

decrypted by person B

text

Only the person B can read the text by using the secret key B.

A transaction in the Bitcoin blockchain: essence



Previous Transaction Hash

Public Key of A Hash

Public Key of S

Digital Signature by S

Transaction S→A

Previous Transaction Hash

Public Key of B Hash

Public Key of A

Digital Signature by A

Transaction A→B

Previous Transaction Hash

Public Key of C Hash

Public Key of B

Digital Signature by B

Transaction B→C

“Digital signature by A” ensures that

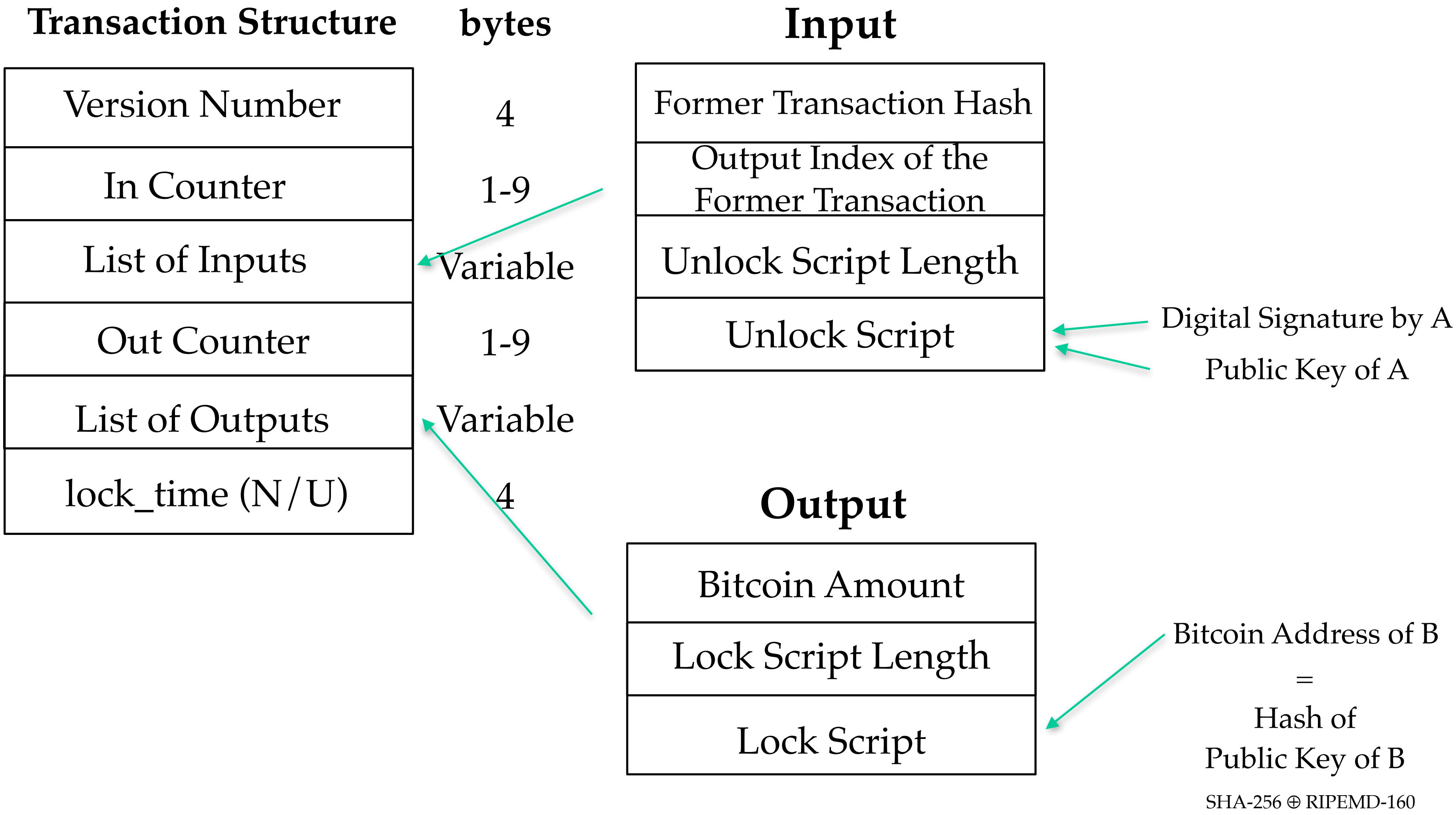
- The owner A has the authorized right of using the output of the previous transaction (correspondence to the “Public Key of A”)
- The owner A authorizes that the owner of the “Public Key of B” has the right to use the output.

※A transaction of Bitcoin can have multiple inputs and multiple outputs.

※Each transaction uses up all the inputs. Each time the receiver address (hash of the public key of the receiver) is newly created and not recycled.

Bitcoin Transaction Structure

Transaction from A to B



Transaction Structure	bytes
Version Number	4
In Counter	1-9
List of Inputs	Variable
Out Counter	1-9
List of Outputs	Variable
lock_time (N/U)	4

Input

Input
Former Transaction Hash
Output Index of the Former Transaction
Unlock Script Length
Unlock Script

Digital Signature by A

Public Key of A

Output

Output
Bitcoin Amount
Lock Script Length
Lock Script

Bitcoin Address of B
=
Hash of
Public Key of B

SHA-256 ⊕ RIPEMD-160

※Bitcoin Script Language

Mining

Miners (採掘者) validates a new block int the following way.

- A miner node has **a copy of all the blocks and transactions**.
- New transactions are distributed to each node.
- A miner **verifies each transaction**, *e.g.* for signature, token amount, availability of the inputs.
- A miner packs a set of valid transactions in the structure of a block to be added at the present end of the blockchain.
- A miner **tries to find a solution of the Proof of Work** by changing the nonce number. If successful, it distributes the block to every node. The miner gets reward of **newly generated Bitcoin** (with possible reward from the transaction requester).
- Meanwhile, **if a successful block arrives**, a miner add it to the blockchain (with updating the transaction database) and **gives up the present trial**. For each fork the longest chain is regarded as the main-chain

New bitcoin can only be generated at the time of block validation (mining).

Thus the amount of the bitcoin is not controlled by an authority.

The amount of generated bitcoin per block is scheduled to decrease.

Mining Cost

Mining power is rapidly increasing from 10^9 has/sec (2009) to ~10^{20}(2021).

The electric power used for the mining is becoming problematic.

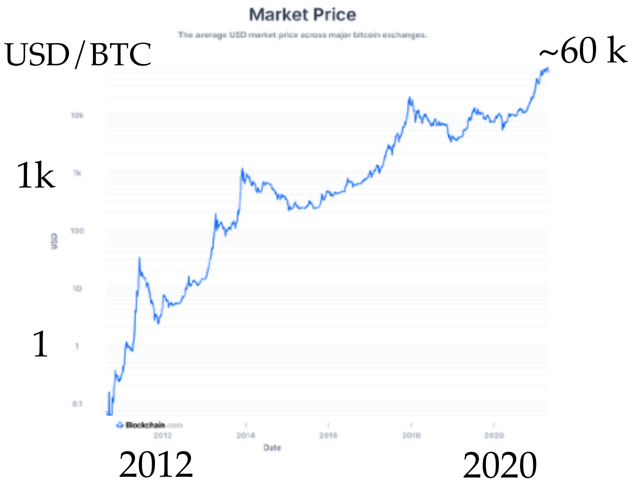
Mining cost: ~18.2 kUSD/BTC (2021.2.17)

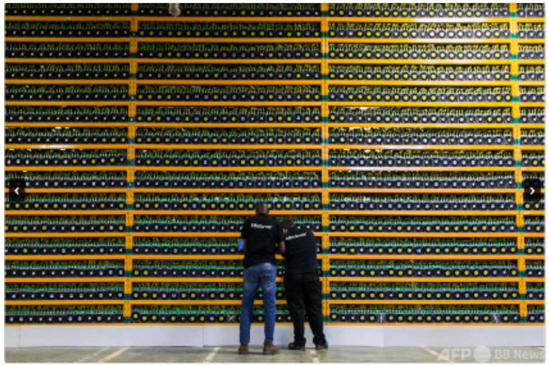
Electricity: ~ 100 TW (2021)

0.6% of the world consumption

Electricity at RCNP (RING+GR) =1.7 MW = 680 kJpY /day

~1 BTC / 3 day





Rapid increase of the BTC price

since BTC is regarded as a speculative target by capitalists

Bitcoin Controlled Supply

- The average time of producing a block is controlled to 10 minute.

- Newly produced Bitcoin as a reward for validating a block is scheduled to reduce by half for every 210,000 blocks (~4 years).

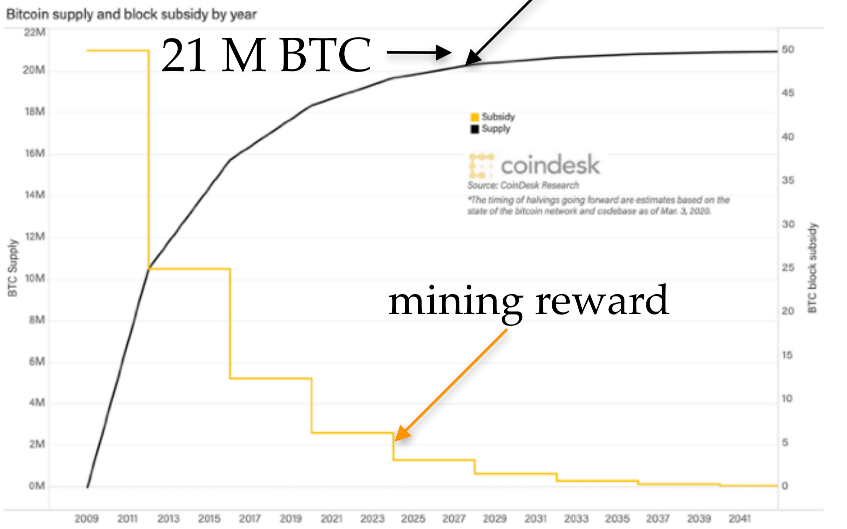
protection from inflation

→ The total supply of Bitcoin is limited.

	reward
2019.1.3	50 BTC/block
2012.11.28	25
2016.7.9	12.5
2020.5.11	6.25

The controlled supply ensures the rarity of the currency and a nearly regular increase of the price.

total amount of BTC



Source: CoinDesk Research

*The timing of halvings going forward are estimates based on the state of the bitcoin network and codebase as of Mar. 3, 2020.

21 M BTC →

mining reward

2009 2021 2041

1 BTC = 10^8 Satoshi

History of Bitcoin

2008.10.31	White paper by Satoshi Nakamoto
2009.1.3	Bitcoin blockchain started
2010.5.22	The first payment: 2 pizzas by 10,000BTC in Florida
2010	Mt. Gox, the first cryptocurrency exchange
2014	Mt. Gox incident: 750 kBTC (~48 GJpY) was stolen
2017.8.1	Hard-fork of Bitcoin Cash (BCH)
2018.1.26	Coincheck incident: 523 M XEM (~58 GJpY) was stolen.
2021.3.14	The Bitcoin price exceeded 60 kUSD/BTC.
2021.4.14	Coinbase IPO in USA
2019-	9 Bitcoin ETF applications to SEC in USA (no accept yet)

Cryptocurrency 3.0
Mark Karpelès

Currency leaks were due to the insecure management of the exchange companies.

The **blockchain protocol has never been broken** in spite of the several incidents of the currency leak.

Validity of the **blockchain** concept and **proof of work** mechanism has been proven by the operation of more than 10 years!

What is “value”?

Blockchain has realized **decentralized exchange of *value***.

Bitcoin was its application using the *value* as *currency*.

One may regard the cryptocurrency as just a digital information holding empty value.

It looks that the miners just waste electricity for finding useless mathematical solutions.

The opinion might be correct. Before judging, however, we need to remind us *what is “value”* and *what is the value of conventional currencies*.

History of money

…

Gold	金	
Convertible Money	兌換紙幣	
Fiat Money	不換紙幣	Nixon Shock (1971)
Cryptocurrency	仮想通貨/暗号資産	

The value of gold is not at all the cost of the mining.

The value of fiat money is only authorized by the government.

What is "value"?

Marxian Economy

Karl Marx, *Capital: Critique of Political Economy* 資本論

Goods (商品) have two values

- use value 使用価値
- exchange value 交換価値

The exchange value is mediated by money (price).

The exchange value originates from the required amount of labor. 労働量

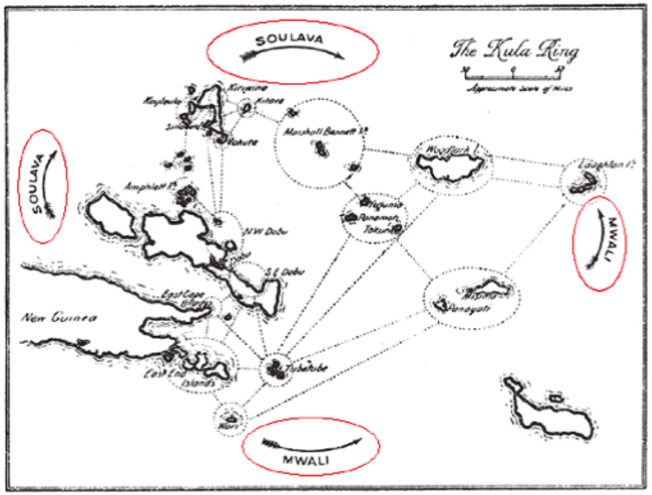
It implies that the value of cryptocurrency is based on the work of mining.

Kula Exchange in Papua Niugini

Bronisław Malinowski *Argonauts of the Western Pacific*

People in the inlands exchanged their treasures taking a risk of life even though they looked to have no value!

Exchange creates the value.



Map V—The Kula Ring.

©National Museum of Ethnology

What is “value”?

It would be difficult to define **the value of the cryptocurrency**.

In my opinion, the value of the cryptocurrency **should be defined according to its original purpose**: **realization of decentralized peer-to-peer currency**

Present speculative investment and excessive value creation are obstructing the realization of the purpose.

Today's Summary

Blockchain Technology

is a ***Trust Protocol*** that realizes ***decentralized*** exchange of value.

The validity of the concept has been proved by more than 10 years of operation of the Bitcoin.

Next week, I will introduce

A second generation blockchain operated from 2015, that is

a **distributed world computer** working on a blockchain.

Smart contract, Web3.0, dApps, NFT, DeFi, …

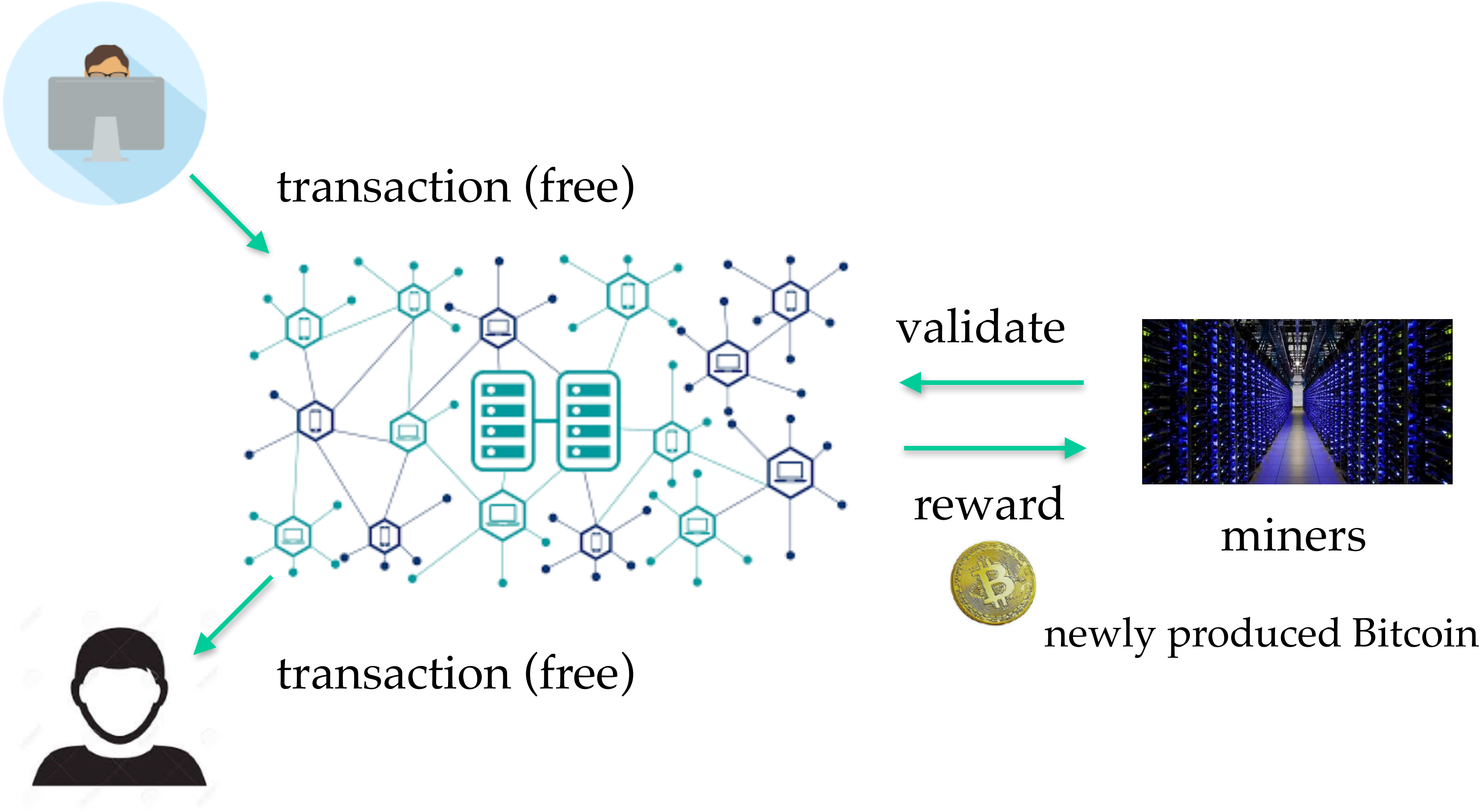
III. A second generation blockchain:

Ethereum and smart contract

Notes on the previous presentation

Notes

- The transaction fee of Bitcoin is essentially free. Newly produced Bitcoins are given to the miners.



transaction (free)

validate

reward

miners

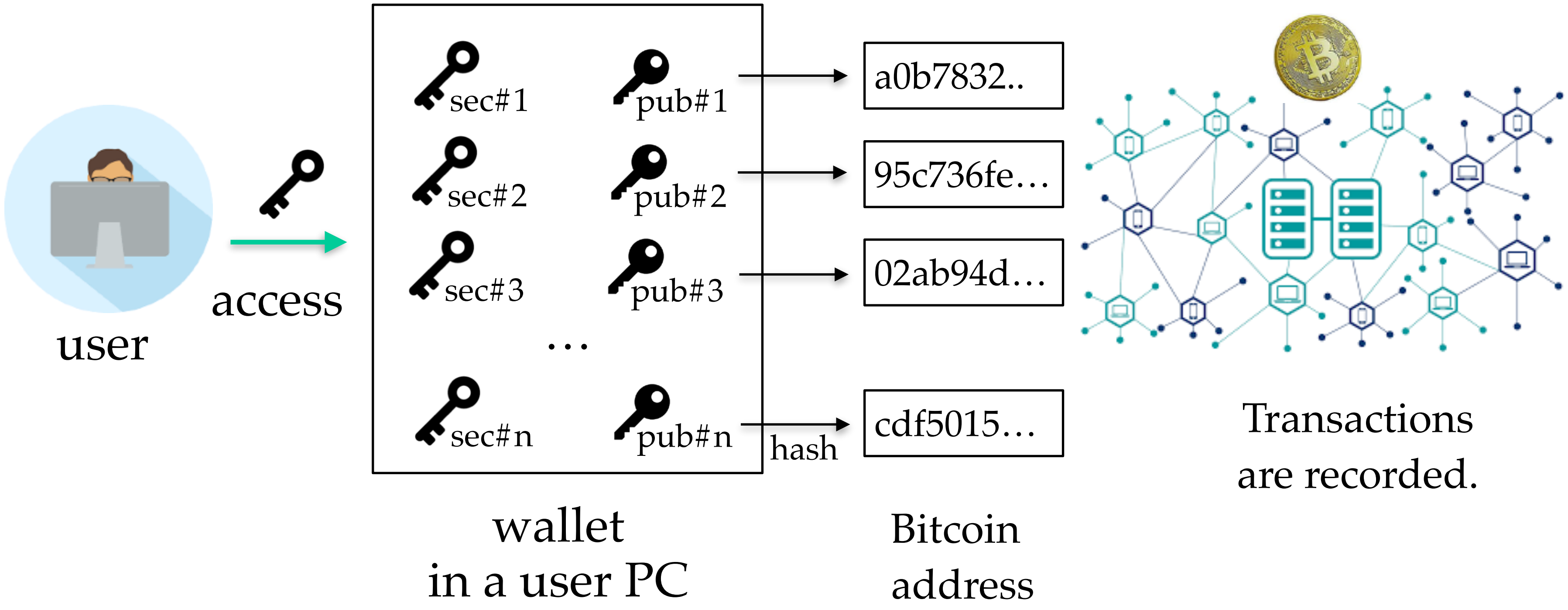
newly produced Bitcoin

transaction (free)

Notes on the previous presentation

Notes

- Digital wallet

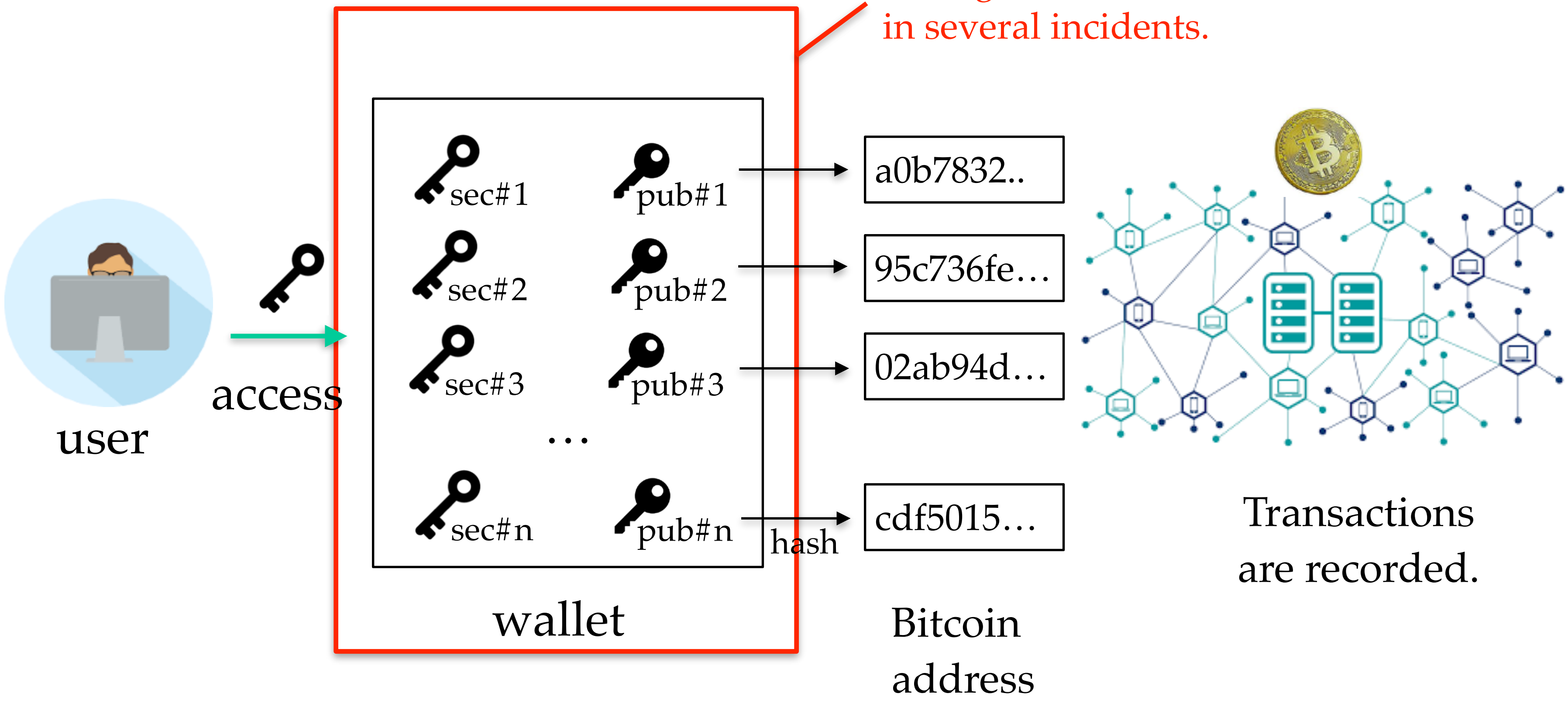


A pair of secret and public keys are generated for each transaction without recycling.
There is no way to get your money back if you lose the access to your secret keys!

Notes on the previous presentation

Notes

- Digital wallet



Cryptocurrency exchange companies manage user wallets, that were stollen in several incidents.

user

access

sec#1

pub#1

sec#2

pub#2

sec#3

pub#3

…

sec#n

pub#n

wallet

hash

a0b7832..

95c736fe…

02ab94d…

cdf5015…

Bitcoin address

Transactions are recorded.

Cryptocurrency exchange companies get commission from the *spread* between sell and buy.

Previous presentation to Today’s

Blockchain Technology

is a ***Trust Protocol*** that realizes ***decentralized*** exchange of value.

Last week, the **first generation blockchain** and its first application, Bitcoin **cryptocurrency**, was introduced.

Today, I will introduce a **second generation blockchain**, Ethereum, realization of **smart contract** and its applications.

	similar to
Bitcoin:	gold
Ethereum:	computer

Ethereum is a *decentralized wold computer* working on a blockchain that can accommodate applications on it.

Ethereum: a second generation blockchain

Vitalik Buterin

2013.12	Ethereum white paper by Vitalik Buterin
2015.7.30	Ethereum blockchain started
2016.6.18	The DAO Incident, 3.6 M ETH was stolen.
2016.7.23	Hard-fork of Ethereum Classic

15 seconds for a block validation

No limit of supply

Ethereum blockchain:

- a general blockchain platform that implements **smart contract**.
- a **state machine** equipped with an **internal storage**.
- concept of **accounts**
- **Ethereum Virtual Machine** (EVM), Turing-complete.
- *gas* for paying the cost of calculation and storage
- Scheduled update from *Proof of Work* to ***Proof of Stake***.

Ethereum is a "decentralized world computer" based on a blockchain.

Turing Completeness

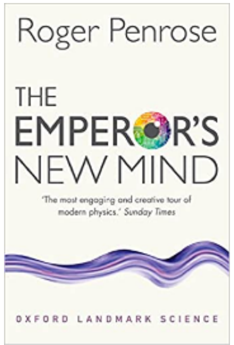
計算可能性

A.M. Turing

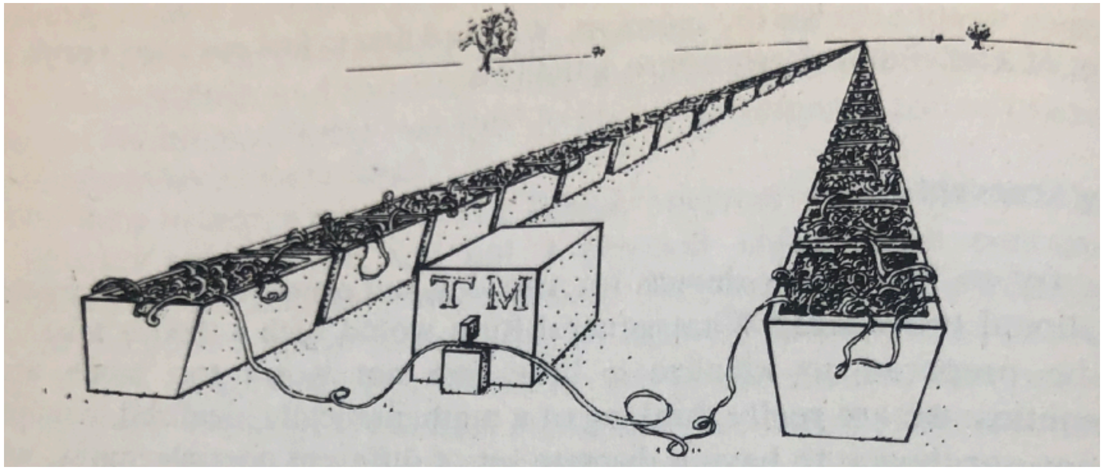
A **Turing machine** is a mathematical model of **computational possibility** (algorithm) defined with an abstract machine that manipulates symbols on a strip of an infinitely long tape according to a table of rules.

The word ***Turing completeness*** expresses an ability of simulating the Turing machine. **Many popular programming languages** working on a von-Neumann architecture computer are **Turing complete** if the limitation of the memory size is ignored, i.e. **they are equivalent** in terms of the computational possibility.

I suggest you read *the emperor's new mind* by Roger Penrose if you are interested in this subject.


Roger Penrose
THE EMPEROR'S NEW MIND
'The most engaging and creative tour of modern physics.' Sunday Times
OXFORD LANDMARK SCIENCE

Turing Machine: A.M. Turing (1936)



c.f. Turing test

Smart Contract

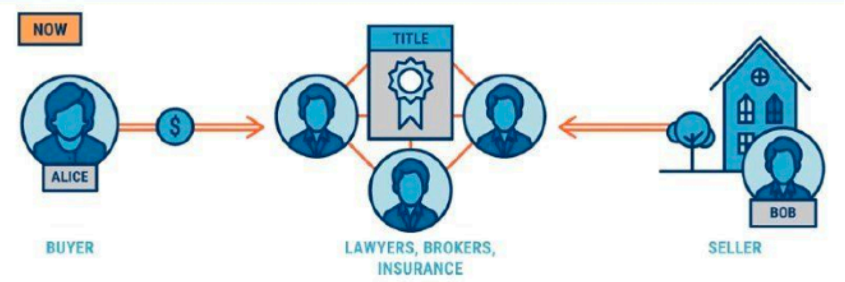
A contract between peers is concluded without centralized authorization.
契約

A **contract account** is created in the blockchain for each type of the work.

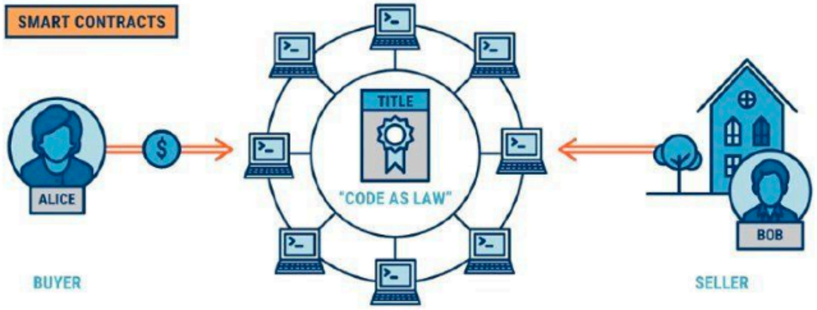
A contract contains **a code that automates the work** between the peers.

All the nodes witness the work and accept only valid results.

contact under authorization



decentralized automated contact



Smart Contracts: Nick Szabo (1996)

Contract Account

A contract works on the Ethereum Virtual Machine (EVM).

- **A contract account is created** by a message from an externally owned account (EOA). It costs “**gas**” for storing the code and for initialization.
- An EOA uses a contract by sending a message to a contract account. It costs “**gas**” to accomplish the work for the contract. The contact **fails** if the supplied gas is used up before completion with rolling back all the transactions.
- The contract account can send a reply to the EOA and messages to other accounts including contract accounts.

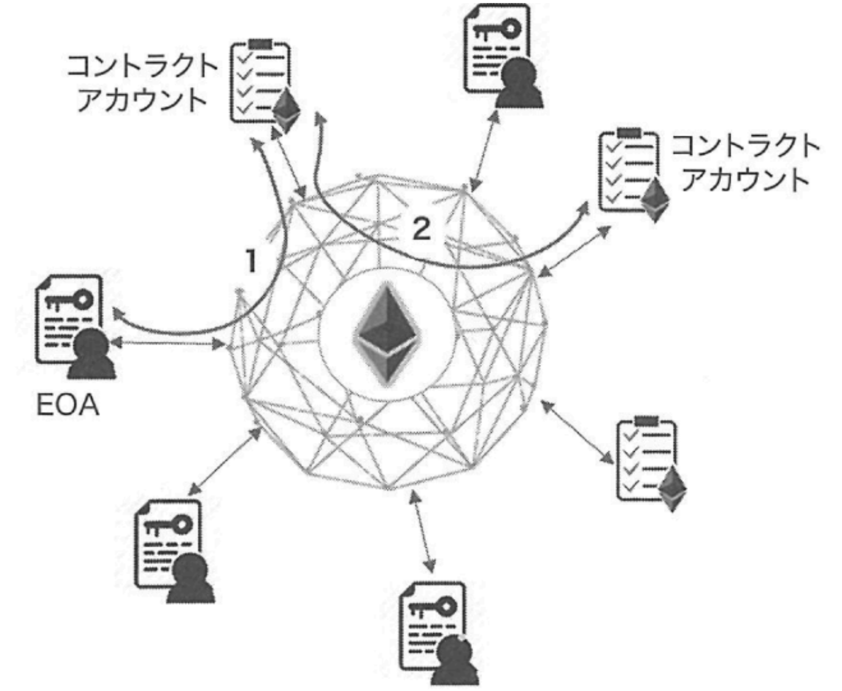


図4.5　EOAからコントラクトアカウントへ、さらにコントラクトアカウントへと発行されるトランザクション

Payment by the sender

Cost in ETH = (gas amount)× (gas price)

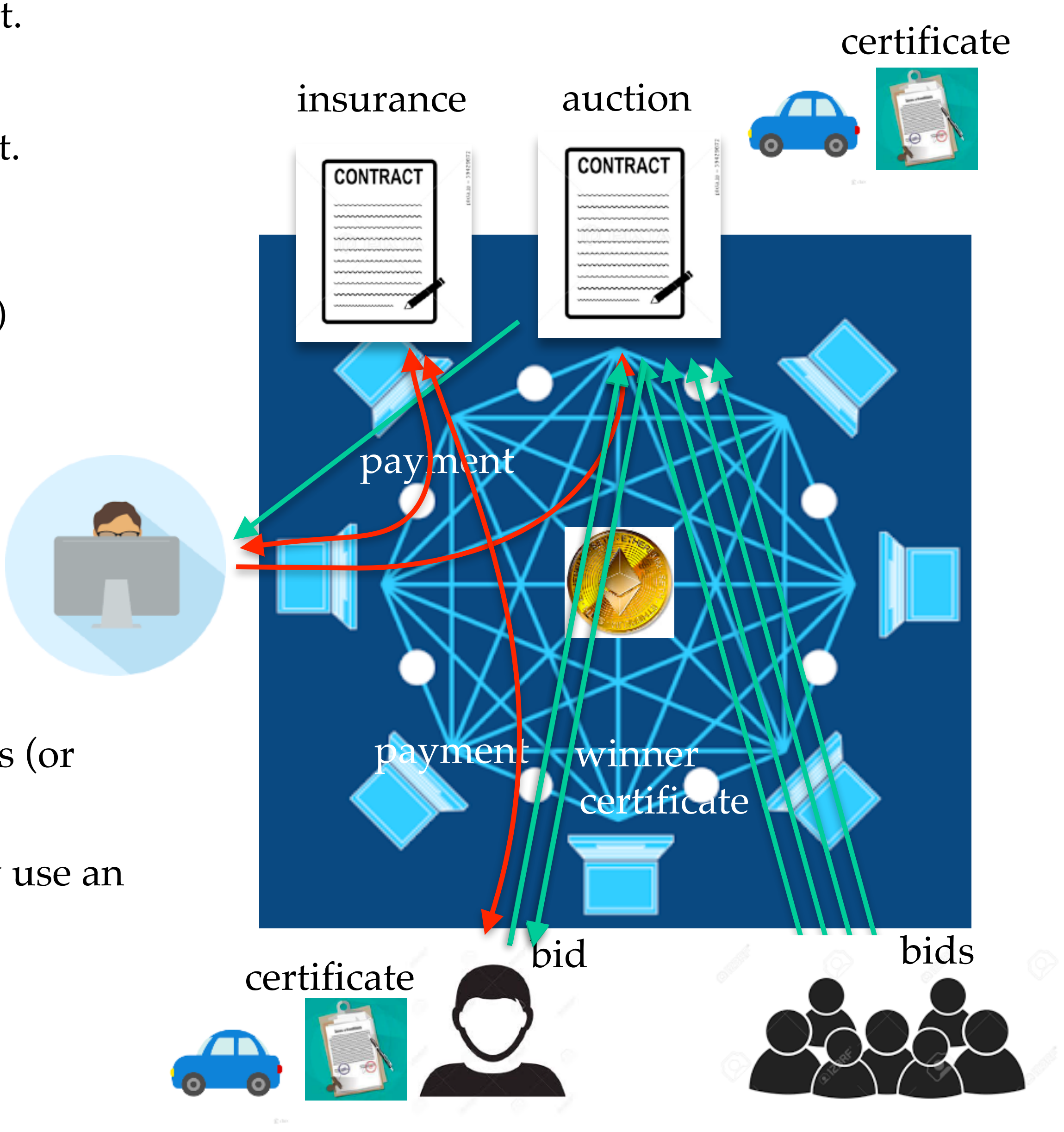
Gas price is determined by the balance between supply and demand.

Gas amount is the maximum that can be user for calculation and storage.

Smart Contract: An Example

An example: auction smart contract.

- Creation of auction smart contract.
- Register goods for the auction.
  digital certificate
  details (deadline, initial price, etc)
- People bid for the goods.
- A message is sent to the winner
- Payment from the winner.
- Transfer of the certificate.



- Fine is taken from the illegal users (or provider). Their rating decreases.
- The provider (and the users) may use an insurance contract for risks.

Ethereum Block Structure

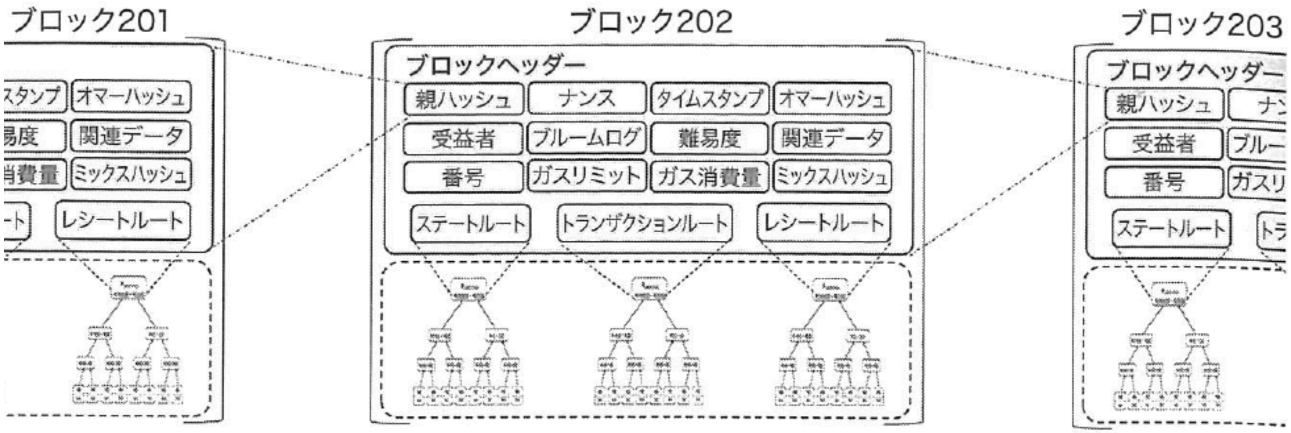


図4.2　イーサリアムブロックチェーンのデータ構造

Merkle-Patricia trees are used for recording the states, transactions, and receipts.

Ethereum on May 2021

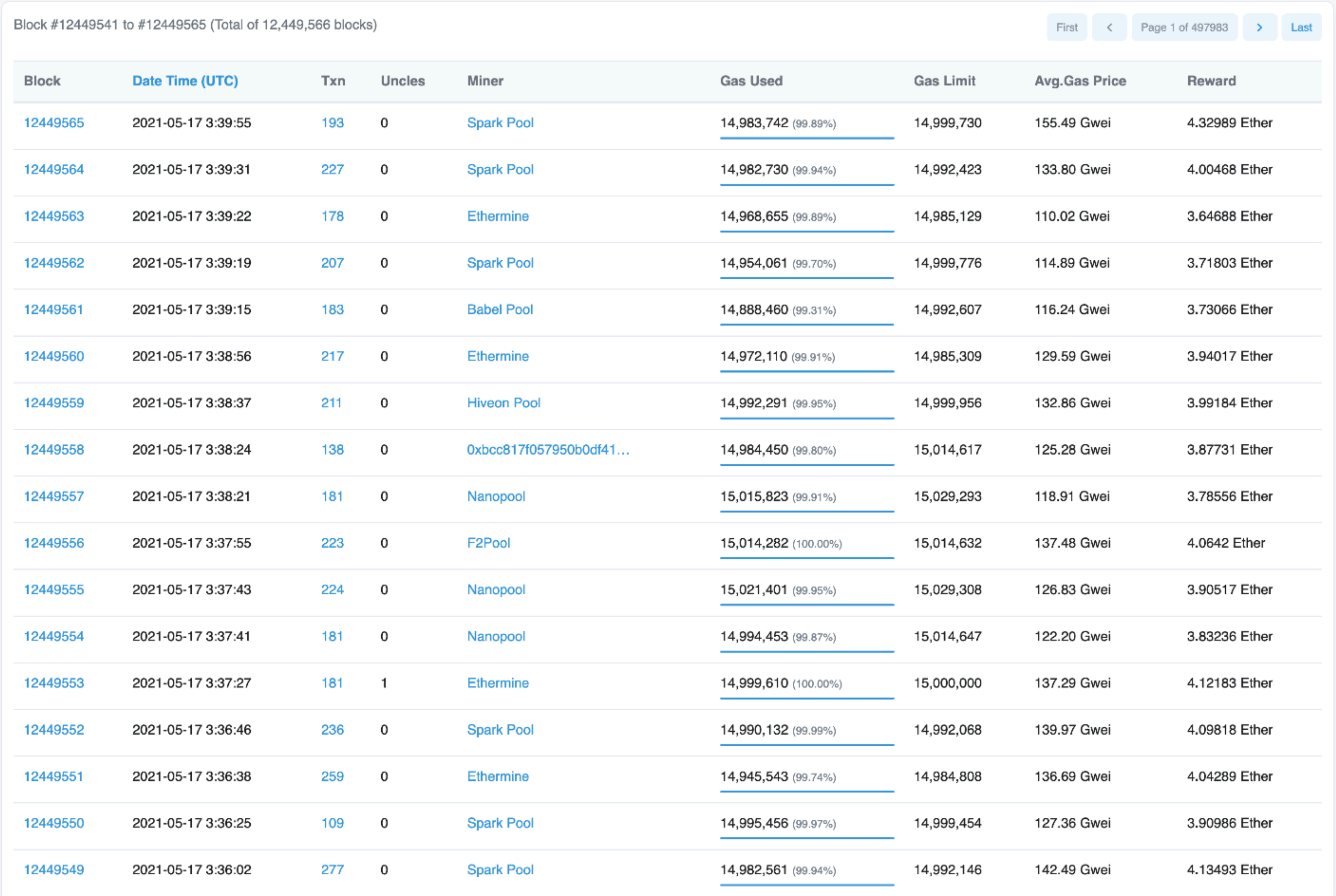
- Average transactions per block: ~250
- Total blockchain size: ~234 GB
- Average block size: ~56 kB
- Average time for a block: 15 sec
- Total number of blocks: 1.24×10^7
- Total number of transactions: 1.14×10^9
- Average Transaction Fee: ~0.01 ETH

https://etherscan.io/

https://blockchair.com/ethereum/charts

Ethereum Blocks

https://etherscan.io/blocks



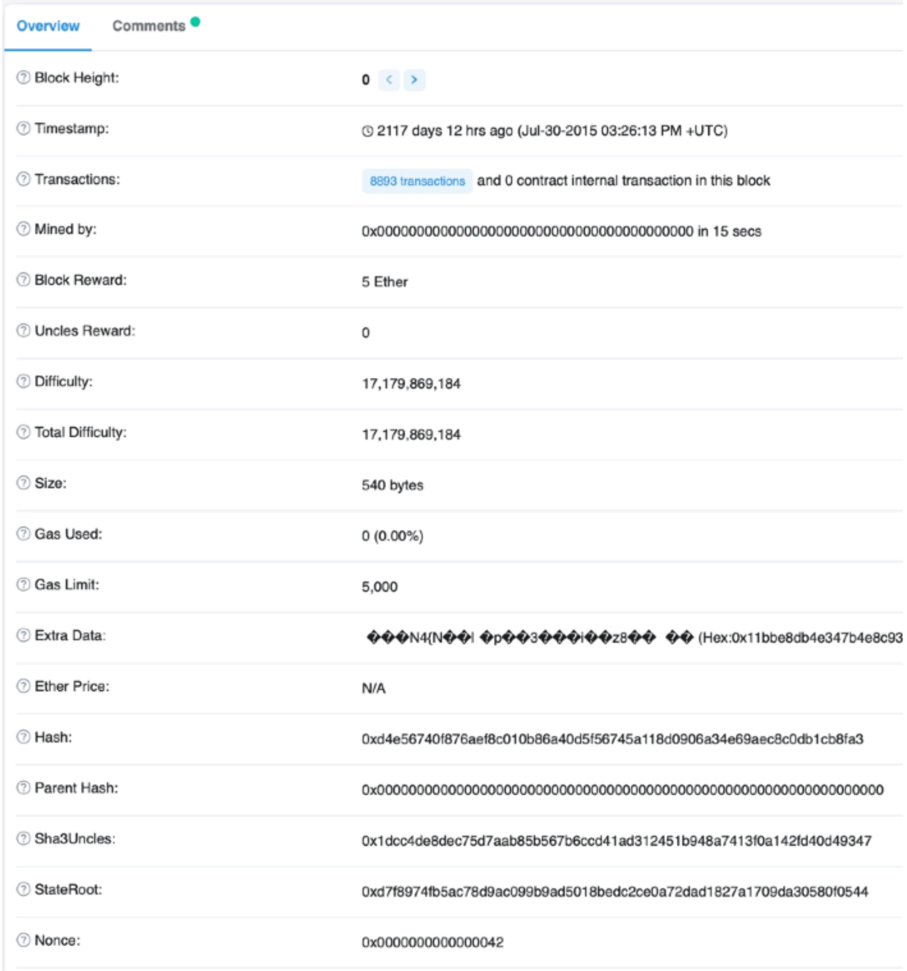
Block #12449541 to #12449565 (Total of 12,449,566 blocks)

Block	Date Time (UTC)	Txn	Uncles	Miner	Gas Used	Gas Limit	Avg.Gas Price	Reward
12449565	2021-05-17 3:39:55	193	0	Spark Pool	14,983,742 (99.89%)	14,999,730	155.49 Gwei	4.32989 Ether
12449564	2021-05-17 3:39:31	227	0	Spark Pool	14,982,730 (99.94%)	14,992,423	133.80 Gwei	4.00468 Ether
12449563	2021-05-17 3:39:22	178	0	Ethermine	14,968,655 (99.89%)	14,985,129	110.02 Gwei	3.64688 Ether
12449562	2021-05-17 3:39:19	207	0	Spark Pool	14,954,061 (99.70%)	14,999,776	114.89 Gwei	3.71803 Ether
12449561	2021-05-17 3:39:15	183	0	Babel Pool	14,888,460 (99.31%)	14,992,607	116.24 Gwei	3.73066 Ether
12449560	2021-05-17 3:38:56	217	0	Ethermine	14,972,110 (99.91%)	14,985,309	129.59 Gwei	3.94017 Ether
12449559	2021-05-17 3:38:37	211	0	Hiveon Pool	14,992,291 (99.95%)	14,999,956	132.86 Gwei	3.99184 Ether
12449558	2021-05-17 3:38:24	138	0	0xbcc817f057950b0df41...	14,984,450 (99.80%)	15,014,617	125.28 Gwei	3.87731 Ether
12449557	2021-05-17 3:38:21	181	0	Nanopool	15,015,823 (99.91%)	15,029,293	118.91 Gwei	3.78556 Ether
12449556	2021-05-17 3:37:55	223	0	F2Pool	15,014,282 (100.00%)	15,014,632	137.48 Gwei	4.0642 Ether
12449555	2021-05-17 3:37:43	224	0	Nanopool	15,021,401 (99.95%)	15,029,308	126.83 Gwei	3.90517 Ether
12449554	2021-05-17 3:37:41	181	0	Nanopool	14,994,453 (99.87%)	15,014,647	122.20 Gwei	3.83236 Ether
12449553	2021-05-17 3:37:27	181	1	Ethermine	14,999,610 (100.00%)	15,000,000	137.29 Gwei	4.12183 Ether
12449552	2021-05-17 3:36:46	236	0	Spark Pool	14,990,132 (99.99%)	14,992,068	139.97 Gwei	4.09818 Ether
12449551	2021-05-17 3:36:38	259	0	Ethermine	14,945,543 (99.74%)	14,984,808	136.69 Gwei	4.04289 Ether
12449550	2021-05-17 3:36:25	109	0	Spark Pool	14,995,456 (99.97%)	14,999,454	127.36 Gwei	3.90986 Ether
12449549	2021-05-17 3:36:02	277	0	Spark Pool	14,982,561 (99.94%)	14,992,146	142.49 Gwei	4.13493 Ether

Ethereum Blocks

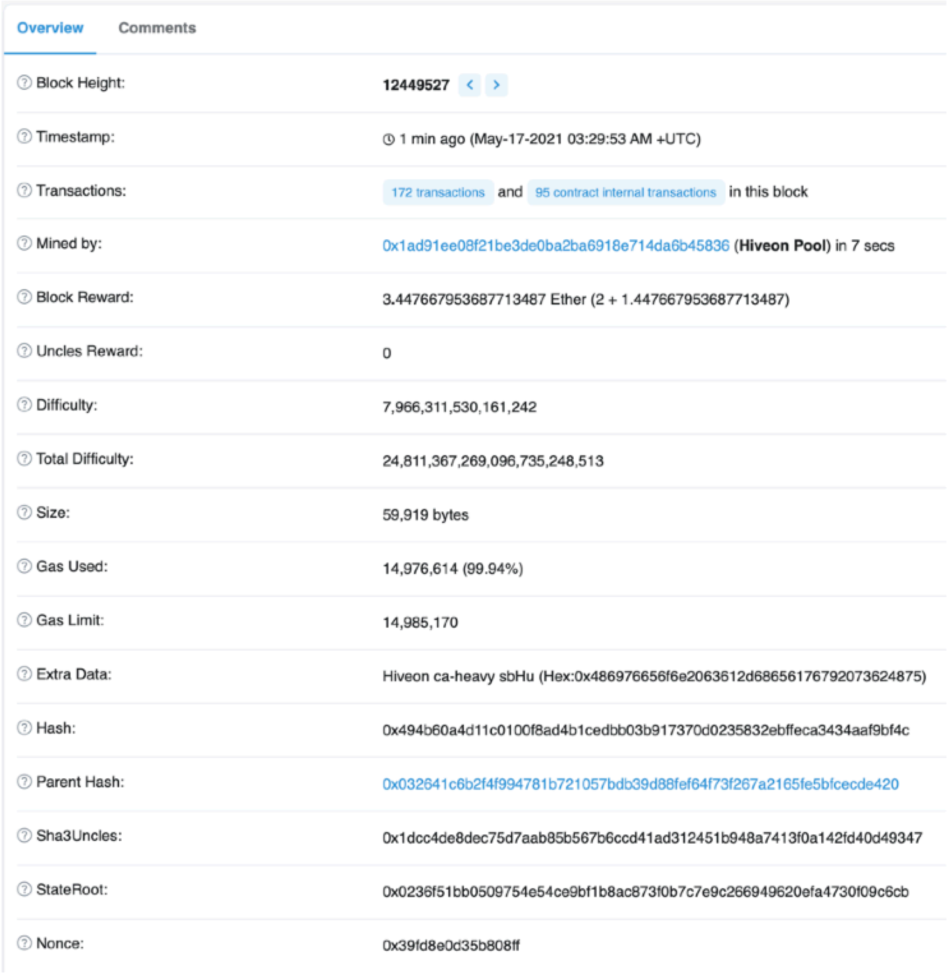
https://etherscan.io/blocks

Genesis Block



Block Height:	**0** < >
Timestamp:	2117 days 12 hrs ago (Jul-30-2015 03:26:13 PM +UTC)
Transactions:	8893 transactions and 0 contract internal transaction in this block
Mined by:	0x0000000000000000000000000000000000000000 in 15 secs
Block Reward:	5 Ether
Uncles Reward:	0
Difficulty:	17,179,869,184
Total Difficulty:	17,179,869,184
Size:	540 bytes
Gas Used:	0 (0.00%)
Gas Limit:	5,000
Extra Data:	���N4{N��I �p��3���i��z8�� �� (Hex:0x11bbe8db4e347b4e8c93
Ether Price:	N/A
Hash:	0xd4e56740f876aef8c010b86a40d5f56745a118d0906a34e69aec8c0db1cb8fa3
Parent Hash:	0x0000000000000000000000000000000000000000000000000000000000000000
Sha3Uncles:	0x1dcc4de8dec75d7aab85b567b6ccd41ad312451b948a7413f0a142fd40d49347
StateRoot:	0xd7f8974fb5ac78d9ac099b9ad5018bedc2ce0a72dad1827a1709da30580f0544
Nonce:	0x0000000000000042

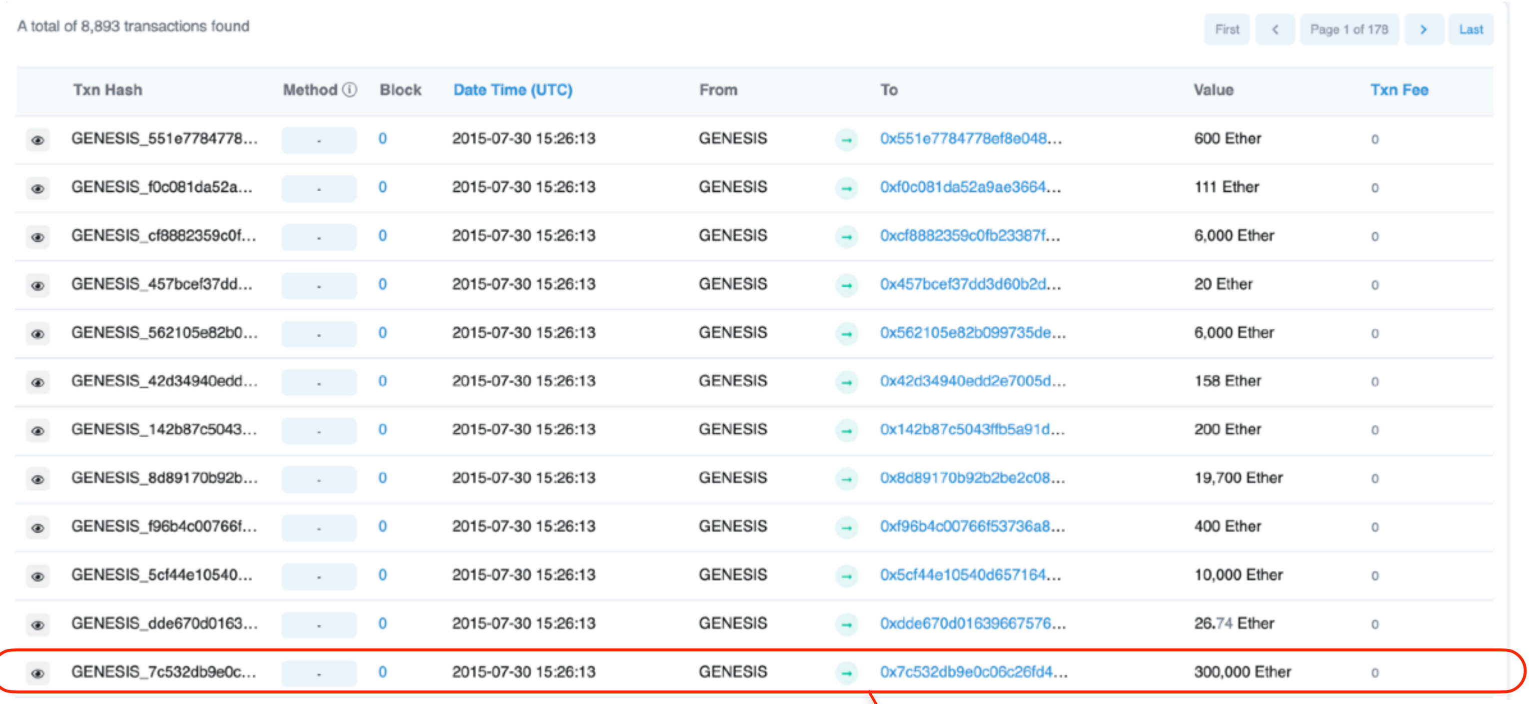
2021.5.17



Block Height:	**12449527** < >
Timestamp:	1 min ago (May-17-2021 03:29:53 AM +UTC)
Transactions:	172 transactions and 95 contract internal transactions in this block
Mined by:	0x1ad91ee08f21be3de0ba2ba6918e714da6b45836 (**Hiveon Pool**) in 7 secs
Block Reward:	3.447667953687713487 Ether (2 + 1.447667953687713487)
Uncles Reward:	0
Difficulty:	7,966,311,530,161,242
Total Difficulty:	24,811,367,269,096,735,248,513
Size:	59,919 bytes
Gas Used:	14,976,614 (99.94%)
Gas Limit:	14,985,170
Extra Data:	Hiveon ca-heavy sbHu (Hex:0x486976656f6e2063612d6865617679207362487 5)
Hash:	0x494b60a4d11c0100f8ad4b1cedbb03b917370d0235832ebffeca3434aaf9bf4c
Parent Hash:	0x032641c6b2f4f994781b721057bdb39d88fef64f73f267a2165fe5bfcecde420
Sha3Uncles:	0x1dcc4de8dec75d7aab85b567b6ccd41ad312451b948a7413f0a142fd40d49347
StateRoot:	0x0236f51bb0509754e54ce9bf1b8ac873f0b7c7e9c266949620efa4730f09c6cb
Nonce:	0x39fd8e0d35b808ff

Ethereum Transactions

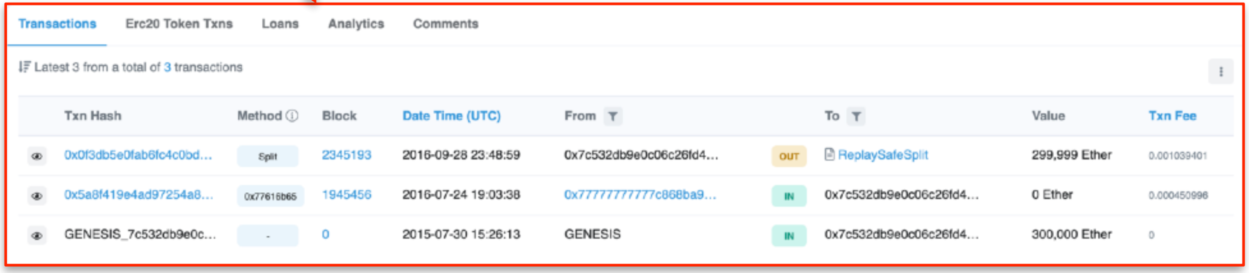
https://etherscan.io/blocks



A total of 8,893 transactions found

First < Page 1 of 178 > Last

Txn Hash	Method ⓘ	Block	Date Time (UTC)	From		To	Value	Txn Fee
GENESIS_551e7784778...	-	0	2015-07-30 15:26:13	GENESIS	→	0x551e7784778ef8e048...	600 Ether	0
GENESIS_f0c081da52a...	-	0	2015-07-30 15:26:13	GENESIS	→	0xf0c081da52a9ae3664...	111 Ether	0
GENESIS_cf8882359c0f...	-	0	2015-07-30 15:26:13	GENESIS	→	0xcf8882359c0fb23387f...	6,000 Ether	0
GENESIS_457bcef37dd...	-	0	2015-07-30 15:26:13	GENESIS	→	0x457bcef37dd3d60b2d...	20 Ether	0
GENESIS_562105e82b0...	-	0	2015-07-30 15:26:13	GENESIS	→	0x562105e82b099735de...	6,000 Ether	0
GENESIS_42d34940edd...	-	0	2015-07-30 15:26:13	GENESIS	→	0x42d34940edd2e7005d...	158 Ether	0
GENESIS_142b87c5043...	-	0	2015-07-30 15:26:13	GENESIS	→	0x142b87c5043ffb5a91d...	200 Ether	0
GENESIS_8d89170b92b...	-	0	2015-07-30 15:26:13	GENESIS	→	0x8d89170b92b2be2c08...	19,700 Ether	0
GENESIS_f96b4c00766f...	-	0	2015-07-30 15:26:13	GENESIS	→	0xf96b4c00766f53736a8...	400 Ether	0
GENESIS_5cf44e10540...	-	0	2015-07-30 15:26:13	GENESIS	→	0x5cf44e10540d657164...	10,000 Ether	0
GENESIS_dde670d0163...	-	0	2015-07-30 15:26:13	GENESIS	→	0xdde670d01639667576...	26.74 Ether	0
GENESIS_7c532db9e0c...	-	0	2015-07-30 15:26:13	GENESIS	→	0x7c532db9e0c06c26fd4...	300,000 Ether	0



Transactions | Erc20 Token Txns | Loans | Analytics | Comments

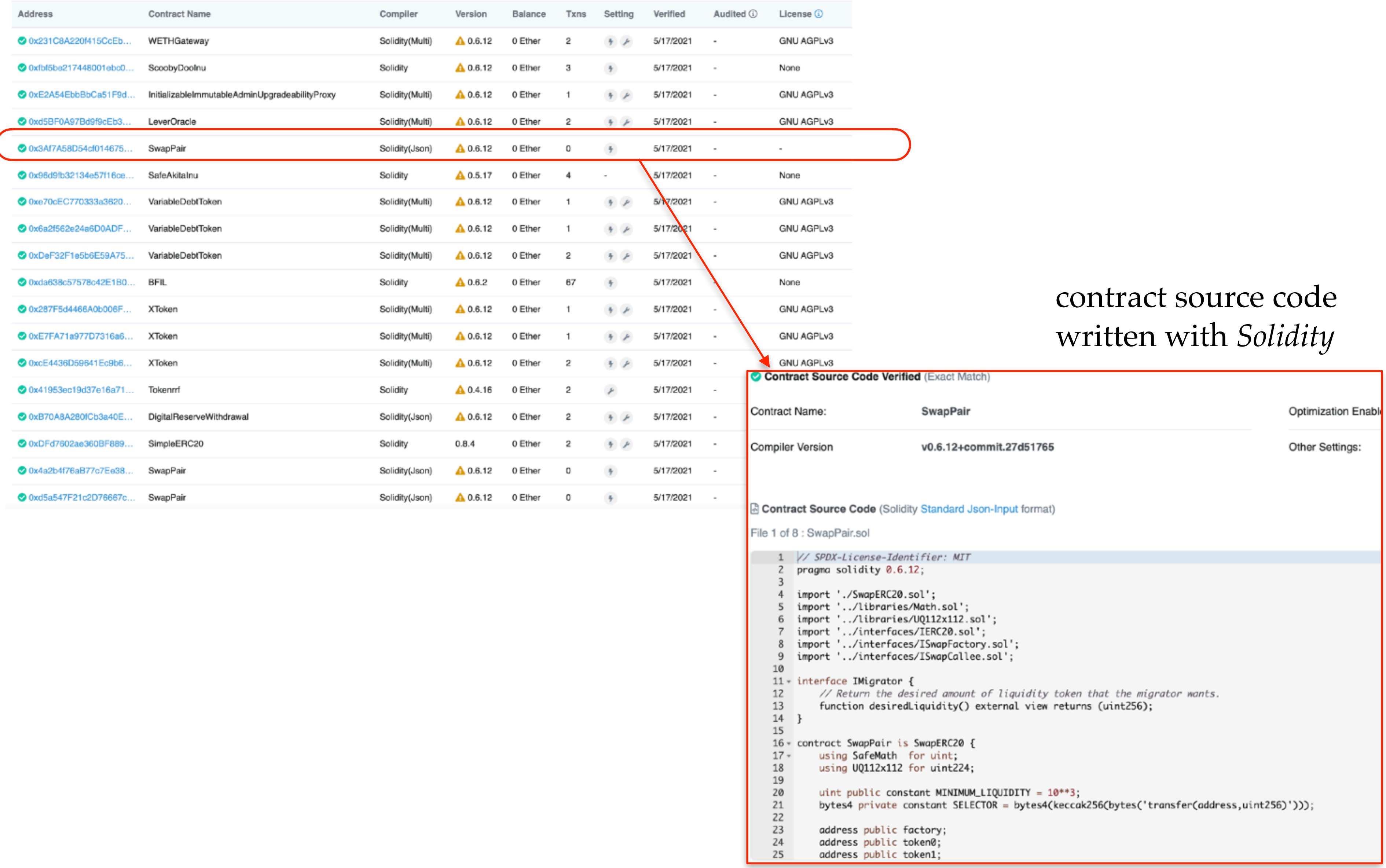
Latest 3 from a total of 3 transactions

Txn Hash	Method ⓘ	Block	Date Time (UTC)	From		To	Value	Txn Fee
0x0f3db5e0fab6fc4c0bd...	Split	2345193	2016-09-28 23:48:59	0x7c532db9e0c06c26fd4...	OUT	ReplaySafeSplit	299,999 Ether	0.001039401
0x5a8f419e4ad97254a8...	0x77616b65	1945456	2016-07-24 19:03:38	0x77777777777c868ba9...	IN	0x7c532db9e0c06c26fd4...	0 Ether	0.000450996
GENESIS_7c532db9e0c...	-	0	2015-07-30 15:26:13	GENESIS	IN	0x7c532db9e0c06c26fd4...	300,000 Ether	0

Ethereum Contracts

https://etherscan.io/contractsVerified

registered smart contracts



Address	Contract Name	Compiler	Version	Balance	Txns	Setting	Verified	Audited ⓘ	License ⓘ
✓ 0x231C8A220f415CcEb...	WETHGateway	Solidity(Multi)	⚠ 0.6.12	0 Ether	2	⚡ 🔧	5/17/2021	-	GNU AGPLv3
✓ 0xfbf5ba217448001ebc0...	ScoobyDooInu	Solidity	⚠ 0.6.12	0 Ether	3	⚡	5/17/2021	-	None
✓ 0xE2A54EbbBbCa51F9d...	InitializableImmutableAdminUpgradeabilityProxy	Solidity(Multi)	⚠ 0.6.12	0 Ether	1	⚡ 🔧	5/17/2021	-	GNU AGPLv3
✓ 0xd5BF0A97Bd9f9cEb3...	LeverOracle	Solidity(Multi)	⚠ 0.6.12	0 Ether	2	⚡ 🔧	5/17/2021	-	GNU AGPLv3
✓ 0x3Af7A58D54cf014675...	SwapPair	Solidity(Json)	⚠ 0.6.12	0 Ether	0	⚡	5/17/2021	-	-
✓ 0x96d9fb32134e57f16ce...	SafeAkitaInu	Solidity	⚠ 0.5.17	0 Ether	4	-	5/17/2021	-	None
✓ 0xe70cEC770333a3620...	VariableDebtToken	Solidity(Multi)	⚠ 0.6.12	0 Ether	1	⚡ 🔧	5/17/2021	-	GNU AGPLv3
✓ 0x6a2f562e24a6D0ADF...	VariableDebtToken	Solidity(Multi)	⚠ 0.6.12	0 Ether	1	⚡ 🔧	5/17/2021	-	GNU AGPLv3
✓ 0xDeF32F1e5b6E59A75...	VariableDebtToken	Solidity(Multi)	⚠ 0.6.12	0 Ether	2	⚡ 🔧	5/17/2021	-	GNU AGPLv3
✓ 0xda638c57578c42E1B0...	BFIL	Solidity	⚠ 0.6.2	0 Ether	67	⚡	5/17/2021	-	None
✓ 0x287F5d4466A0b006F...	XToken	Solidity(Multi)	⚠ 0.6.12	0 Ether	1	⚡ 🔧	5/17/2021	-	GNU AGPLv3
✓ 0xE7FA71a977D7316a6...	XToken	Solidity(Multi)	⚠ 0.6.12	0 Ether	1	⚡ 🔧	5/17/2021	-	GNU AGPLv3
✓ 0xcE4436D59841Ec9b6...	XToken	Solidity(Multi)	⚠ 0.6.12	0 Ether	2	⚡ 🔧	5/17/2021	-	GNU AGPLv3
✓ 0x41953ec19d37e16a71...	Tokenrrf	Solidity	⚠ 0.4.16	0 Ether	2	🔧	5/17/2021	-	
✓ 0xB70A8A280fCb3a40E...	DigitalReserveWithdrawal	Solidity(Json)	⚠ 0.6.12	0 Ether	2	⚡ 🔧	5/17/2021	-	
✓ 0xDFd7602ae360BF889...	SimpleERC20	Solidity	0.8.4	0 Ether	2	⚡ 🔧	5/17/2021	-	
✓ 0x4a2b4f76aB77c7Ee38...	SwapPair	Solidity(Json)	⚠ 0.6.12	0 Ether	0	⚡	5/17/2021	-	
✓ 0xd5a547F21c2D76667c...	SwapPair	Solidity(Json)	⚠ 0.6.12	0 Ether	0	⚡	5/17/2021	-	

✓ **Contract Source Code Verified** (Exact Match)

Contract Name:	**SwapPair**	Optimization Enabl
Compiler Version	**v0.6.12+commit.27d51765**	Other Settings:

Contract Source Code (Solidity Standard Json-Input format)

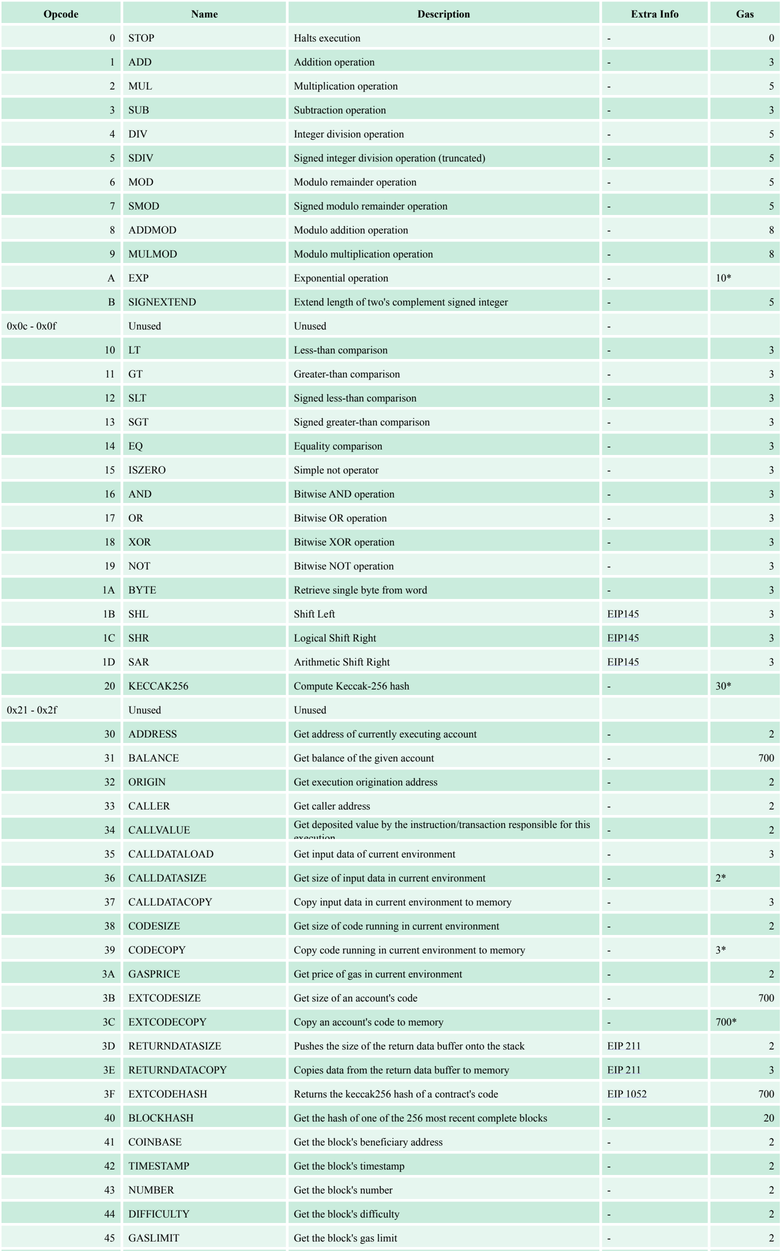
File 1 of 8 : SwapPair.sol

```
// SPDX-License-Identifier: MIT
pragma solidity 0.6.12;

import './SwapERC20.sol';
import '../libraries/Math.sol';
import '../libraries/UQ112x112.sol';
import '../interfaces/IERC20.sol';
import '../interfaces/ISwapFactory.sol';
import '../interfaces/ISwapCallee.sol';

interface IMigrator {
    // Return the desired amount of liquidity token that the migrator wants.
    function desiredLiquidity() external view returns (uint256);
}

contract SwapPair is SwapERC20 {
    using SafeMath  for uint;
    using UQ112x112 for uint224;

    uint public constant MINIMUM_LIQUIDITY = 10**3;
    bytes4 private constant SELECTOR = bytes4(keccak256(bytes('transfer(address,uint256)')));

    address public factory;
    address public token0;
    address public token1;
```

contract source code
written with *Solidity*

EVM Opcodes and Gas

https://github.com/crytic/evm-opcodes



Opcode	Name	Description	Extra Info	Gas
0	STOP	Halts execution	-	0
1	ADD	Addition operation	-	3
2	MUL	Multiplication operation	-	5
3	SUB	Subtraction operation	-	3
4	DIV	Integer division operation	-	5
5	SDIV	Signed integer division operation (truncated)	-	5
6	MOD	Modulo remainder operation	-	5
7	SMOD	Signed modulo remainder operation	-	5
8	ADDMOD	Modulo addition operation	-	8
9	MULMOD	Modulo multiplication operation	-	8
A	EXP	Exponential operation	-	10*
B	SIGNEXTEND	Extend length of two's complement signed integer	-	5
0x0c - 0x0f	Unused	Unused	-	
10	LT	Less-than comparison	-	3
11	GT	Greater-than comparison	-	3
12	SLT	Signed less-than comparison	-	3
13	SGT	Signed greater-than comparison	-	3
14	EQ	Equality comparison	-	3
15	ISZERO	Simple not operator	-	3
16	AND	Bitwise AND operation	-	3
17	OR	Bitwise OR operation	-	3
18	XOR	Bitwise XOR operation	-	3
19	NOT	Bitwise NOT operation	-	3
1A	BYTE	Retrieve single byte from word	-	3
1B	SHL	Shift Left	EIP145	3
1C	SHR	Logical Shift Right	EIP145	3
1D	SAR	Arithmetic Shift Right	EIP145	3
20	KECCAK256	Compute Keccak-256 hash	-	30*
0x21 - 0x2f	Unused	Unused		
30	ADDRESS	Get address of currently executing account	-	2
31	BALANCE	Get balance of the given account	-	700
32	ORIGIN	Get execution origination address	-	2
33	CALLER	Get caller address	-	2
34	CALLVALUE	Get deposited value by the instruction/transaction responsible for this execution	-	2
35	CALLDATALOAD	Get input data of current environment	-	3
36	CALLDATASIZE	Get size of input data in current environment	-	2*
37	CALLDATACOPY	Copy input data in current environment to memory	-	3
38	CODESIZE	Get size of code running in current environment	-	2
39	CODECOPY	Copy code running in current environment to memory	-	3*
3A	GASPRICE	Get price of gas in current environment	-	2
3B	EXTCODESIZE	Get size of an account's code	-	700
3C	EXTCODECOPY	Copy an account's code to memory	-	700*
3D	RETURNDATASIZE	Pushes the size of the return data buffer onto the stack	EIP 211	2
3E	RETURNDATACOPY	Copies data from the return data buffer to memory	EIP 211	3
3F	EXTCODEHASH	Returns the keccak256 hash of a contract's code	EIP 1052	700
40	BLOCKHASH	Get the hash of one of the 256 most recent complete blocks	-	20
41	COINBASE	Get the block's beneficiary address	-	2
42	TIMESTAMP	Get the block's timestamp	-	2
43	NUMBER	Get the block's number	-	2
44	DIFFICULTY	Get the block's difficulty	-	2
45	GASLIMIT	Get the block's gas limit	-	2

1 ETH = 10^9 Gwei = 10^{18} wei

2021.5

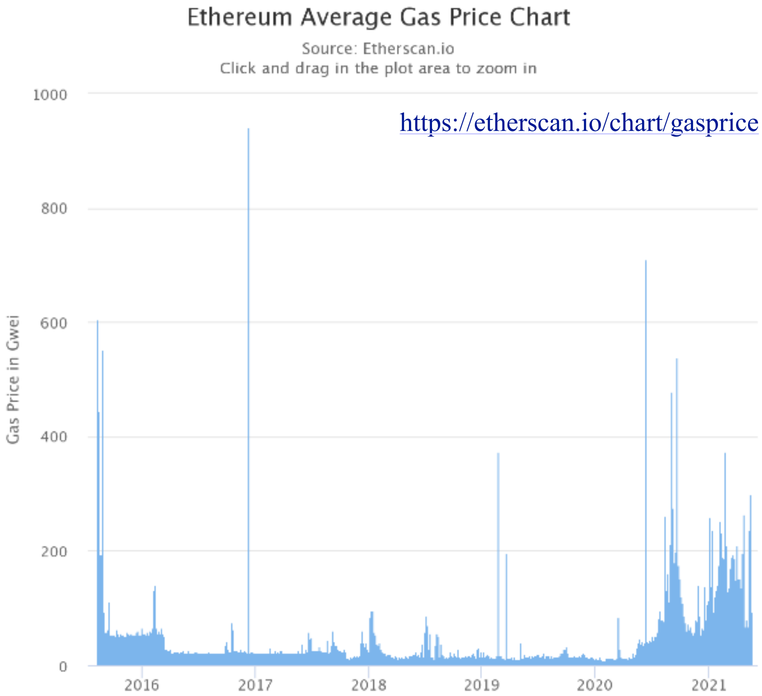
1 transaction = 21,000 gas ~ 0.0021 ETH ~ $6

opcode = 3 (ADD) - 30 (hash) gas

transaction data = 68 gas/byte

storage (SSTORE) = 20,000 gas/word

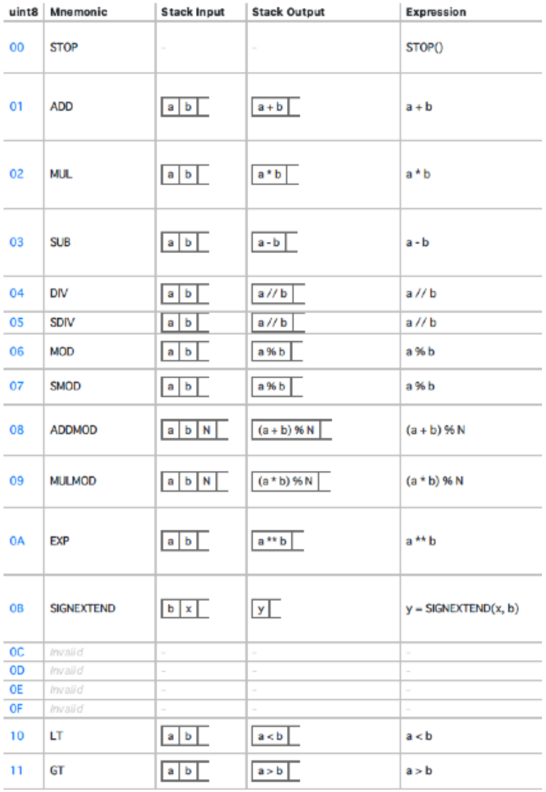
gas price = ~100 Gwei



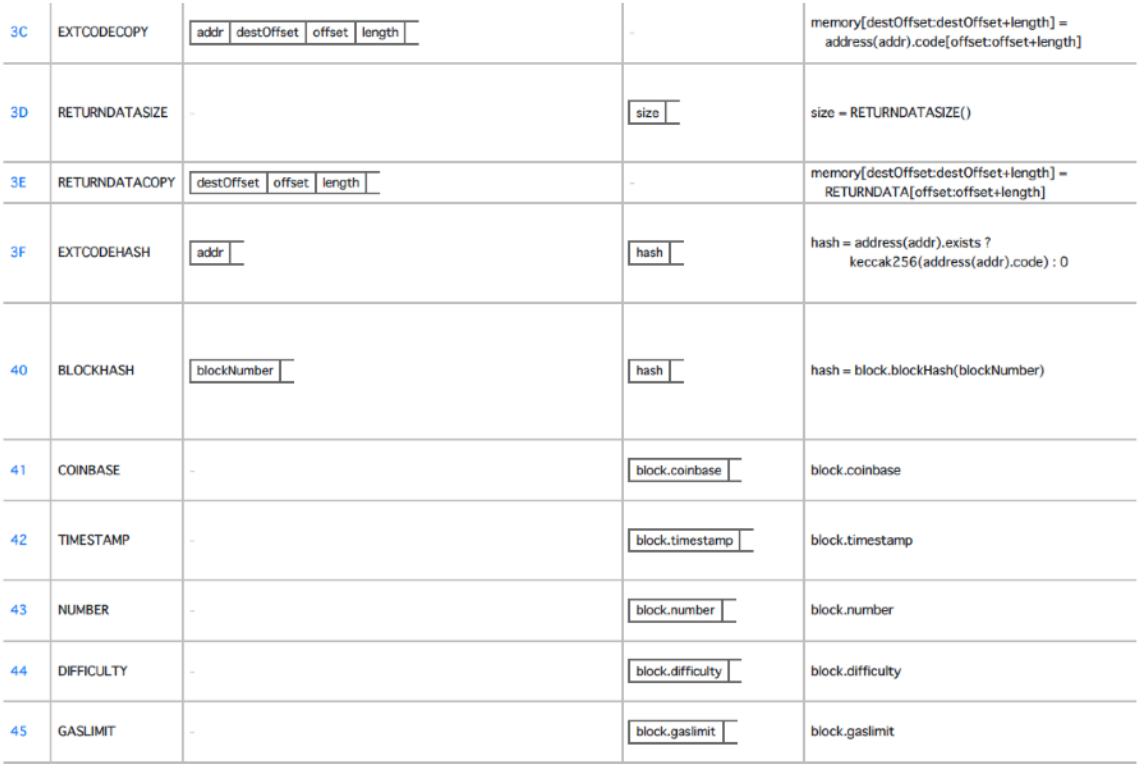
https://etherscan.io/chart/gasprice

EVM Opcodes

https://ethervm.io/#opcodes



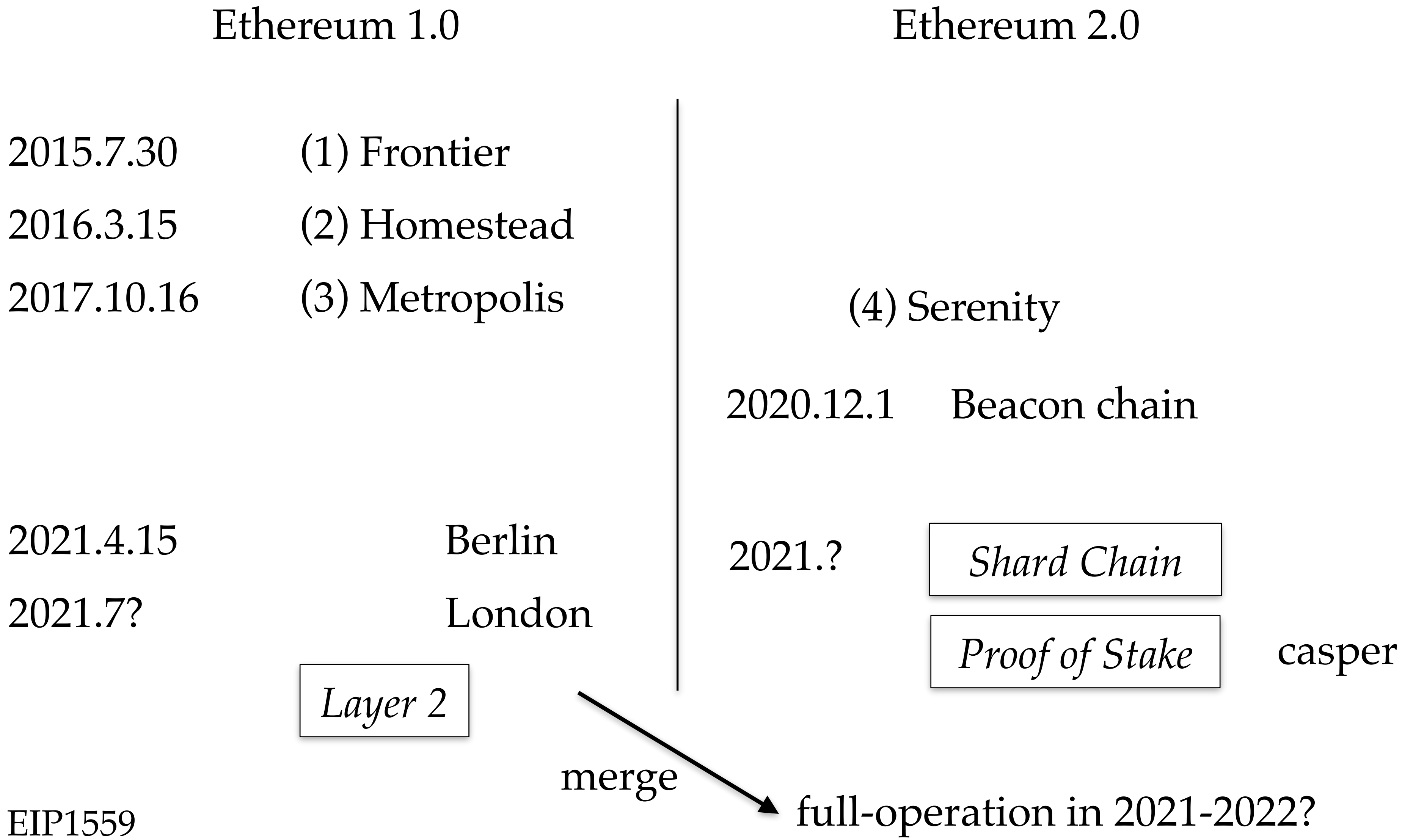
uint8	Mnemonic	Stack Input	Stack Output	Expression
00	STOP	-	-	STOP()
01	ADD	a b	a + b	a + b
02	MUL	a b	a * b	a * b
03	SUB	a b	a - b	a - b
04	DIV	a b	a // b	a // b
05	SDIV	a b	a // b	a // b
06	MOD	a b	a % b	a % b
07	SMOD	a b	a % b	a % b
08	ADDMOD	a b N	(a + b) % N	(a + b) % N
09	MULMOD	a b N	(a * b) % N	(a * b) % N
0A	EXP	a b	a ** b	a ** b
0B	SIGNEXTEND	b x	y	y = SIGNEXTEND(x, b)
0C	*Invalid*	-	-	-
0D	*Invalid*	-	-	-
0E	*Invalid*	-	-	-
0F	*Invalid*	-	-	-
10	LT	a b	a < b	a < b
11	GT	a b	a > b	a > b



3C	EXTCODECOPY	addr destOffset offset length	-	memory[destOffset:destOffset+length] = address(addr).code[offset:offset+length]
3D	RETURNDATASIZE	-	size	size = RETURNDATASIZE()
3E	RETURNDATACOPY	destOffset offset length	-	memory[destOffset:destOffset+length] = RETURNDATA[offset:offset+length]
3F	EXTCODEHASH	addr	hash	hash = address(addr).exists ? keccak256(address(addr).code) : 0
40	BLOCKHASH	blockNumber	hash	hash = block.blockHash(blockNumber)
41	COINBASE	-	block.coinbase	block.coinbase
42	TIMESTAMP	-	block.timestamp	block.timestamp
43	NUMBER	-	block.number	block.number
44	DIFFICULTY	-	block.difficulty	block.difficulty
45	GASLIMIT	-	block.gaslimit	block.gaslimit

Quite similar to the assembler coding in 1980’s!

Ethereum Upgrade



Ethereum 1.0

2015.7.30 (1) Frontier

2016.3.15 (2) Homestead

2017.10.16 (3) Metropolis

2021.4.15 Berlin

2021.7? London

Layer 2

merge

Ethereum 2.0

(4) Serenity

2020.12.1 Beacon chain

2021.? *Shard Chain*

Proof of Stake casper

full-operation in 2021-2022?

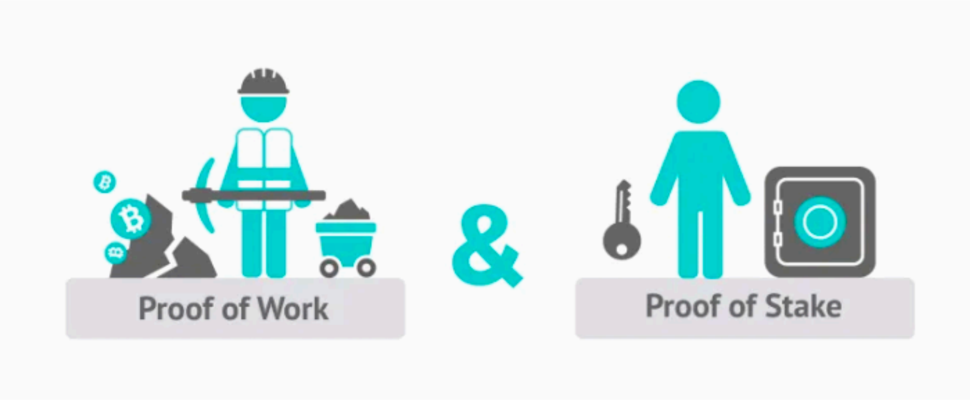
EIP1559

Gas tip and burning in *London*

Proof of Stake

The validator of a new block is selected randomly according to the weight of the **amount** and **age** of **token possessions**.

The concept avoids the problematic resource consumption observed in the operation of the Proof of Work, e.g. in the miners of the Bitcoin blockchain.



c.f. Proof of Consensus

Ethereum 1.0: Scaling by ZK Rollup in Layer 2

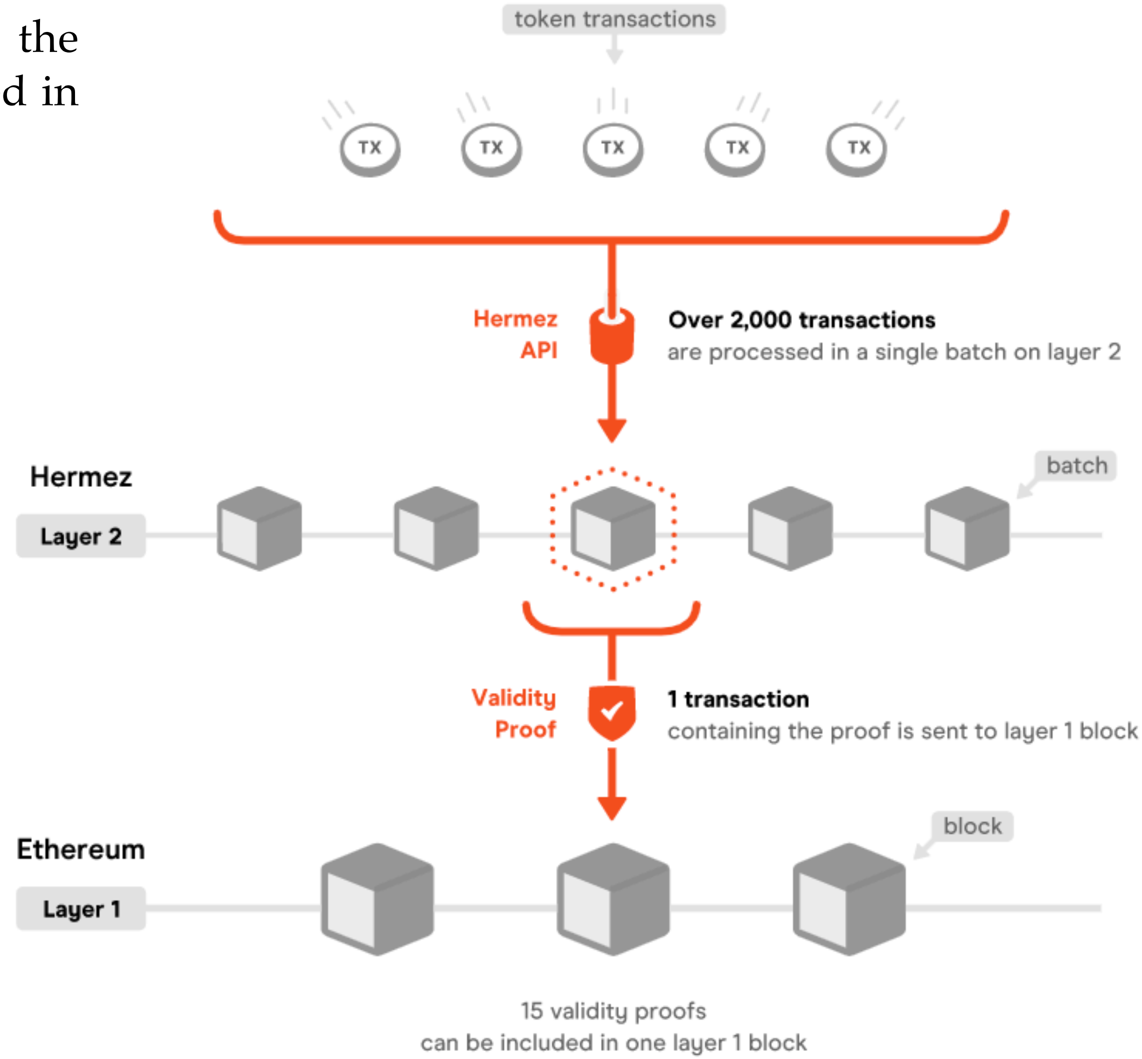
Transactions are rolled up in the layer-2. The validity proof is stored in the layer-1, the main-chain.

- optimistic roll-up

or

- zero-knowledge (ZK) roll-up

to be implemented in Ethereum 1.0

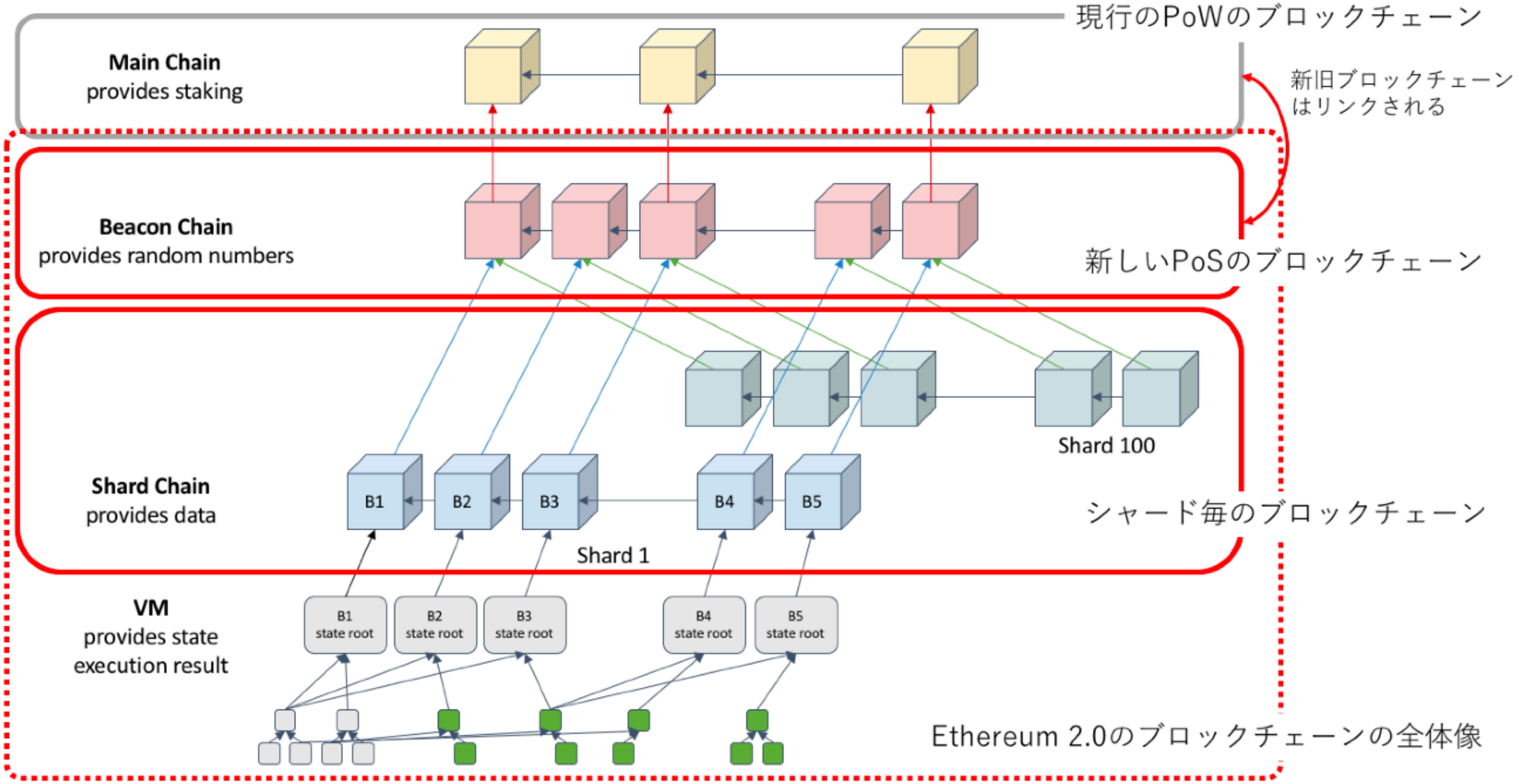


https://ethereum.org/en/developers/docs/scaling/layer-2-rollups/#zk-rollups

Ethereum 2.0: Scaling by Sharding

Sharding is a process of splitting into several (64) chains (shard-chains).

The concept is popularly used for database servers.



https://ethereum.org/en/eth2/shard-chains/#relationship-between-upgrades

IV. Applications

Web 3.0

Realization of a genuine decentralized network.

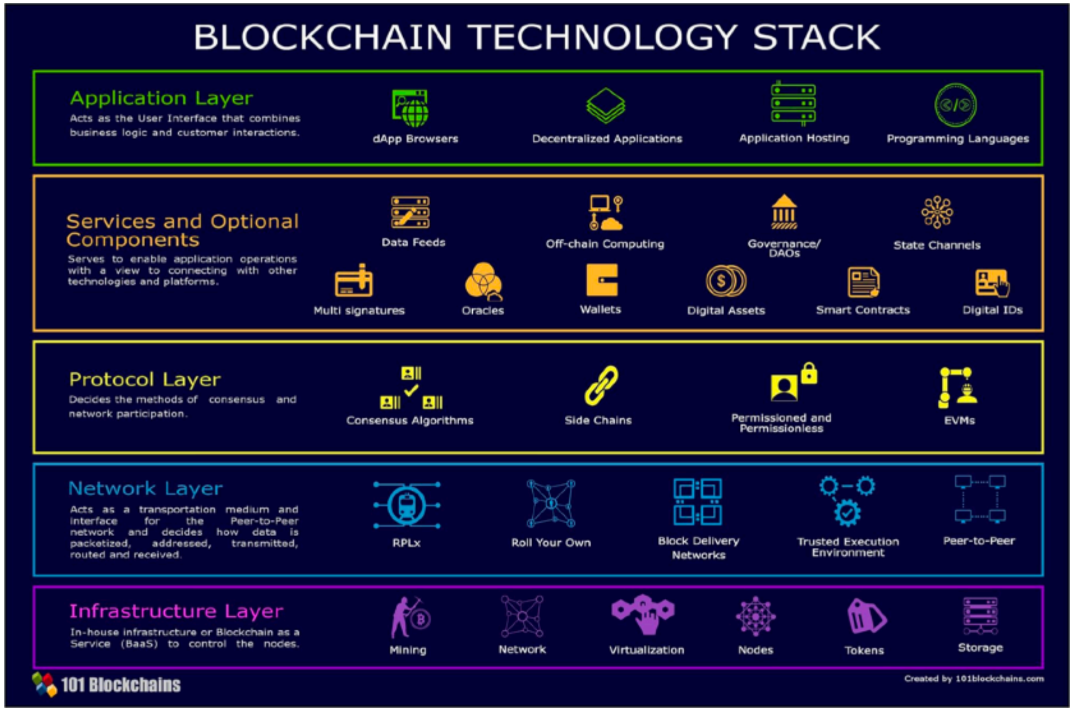
1969 ARPANET
1982 TCPIP
1995- Web 1.0: WWW
2005- Web 2.0: Interactive Web Applications.
202? Web 3.0: genuine decentralized network

controlled by big platformers (GAFA)

Blockchain as a platform of the network communication.

dAppsapplications on the blockchain platform

Decentralization
Privacy Control
System Down Tolerance


BLOCKCHAIN TECHNOLOGY STACK
Application Layer
Acts as the User Interface that combines business logic and customer interactions.
dApp Browsers
Decentralized Applications
Application Hosting
Programming Languages
Services and Optional Components
Serves to enable application operations with a view to connecting with other technologies and platforms.
Data Feeds
Off-chain Computing
Governance/DAOs
State Channels
Multi signatures
Oracles
Wallets
Digital Assets
Smart Contracts
Digital IDs
Protocol Layer
Decides the methods of consensus and network participation.
Consensus Algorithms
Side Chains
Permissioned and Permissionless
EVMs
Network Layer
Acts as a transportation medium and interface for the Peer-to-Peer network and decides how data is packetized, addressed, transmitted, routed and received.
RPLx
Roll Your Own
Block Delivery Networks
Trusted Execution Environment
Peer-to-Peer
Infrastructure Layer
In-house infrastructure or Blockchain as a Service (BaaS) to control the nodes.
Mining
Network
Virtualization
Nodes
Tokens
Storage
101 Blockchains
Created by 101blockchains.com

Fungible and Non-Fungible Tokens

Fungible Token 代替性 *governance or utility token* ERC20

Cryptocurrency Bitcoin, Ethereum, …

Token Economy like "points"

Local government, company, etc. 西粟倉村コイン

Estonia national cryptocurrency (*Estcoin*)

VALU / *Time Bank* support of each person

NFT (Non-Fungible Token) 非代替性 ERC721, ERC1155

Digital copyright

Art, musics, ..

Direct connection between creators and consumers

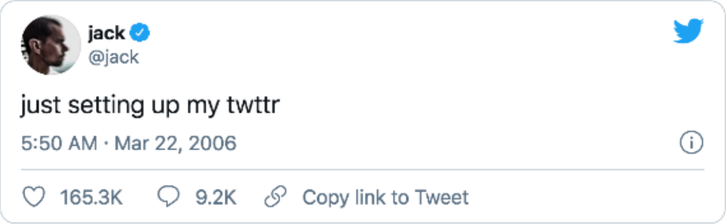
Traceable copyright

NFT

NFT (Non-Fungible Token)

ERC721, ERC1155

The first tweet by Jack Dorsey was bought with $2.9M. 2021.3.10



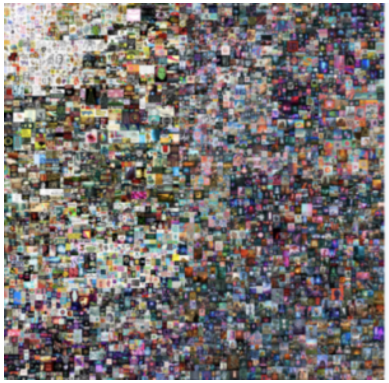
jack
@jack

just setting up my twttr

5:50 AM · Mar 22, 2006

A digital art by Beeple was bought with $69.3M. 2021.3.11

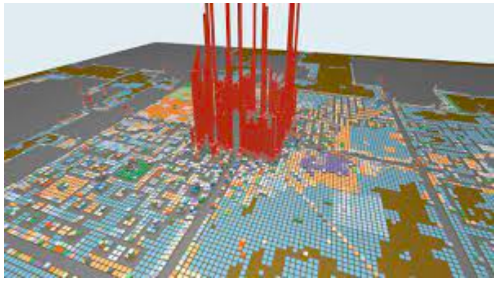
EVERYDAYS: THE FIRST 5000 DAYS



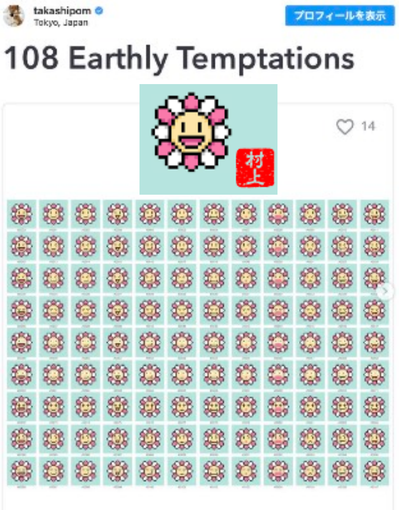
Game, Virtual Space

Cryptokities

Decentraland



The land in a virtual city is soled.



takashipom
Tokyo, Japan

108 Earthly Temptations

Art NFT
Takashi Murakami

Applications, Movements and Ideas

from

Blockchain Revolution by D. Taspcott and A. Tapscott (2016), etc.

Financial Systems

Bank, Credit, Stock companies

- complicated historical system
- many intermediate companies
- still working with paper documents
- infrastructures: branches, ATM systems, safe storage, …
- identity check

Card payment at a Starbucks

- at least 5 intermediate companies
- takes several days for payment to the shop

地債
Issue of bonds from local government

- more than 10 companies: advisers, lawyer, insurance, ban, …

Large part of the above issues can be solved by using a blockchain.

No use of accountant, lawyer, insurance manager, …
会計士/税理士 弁護士 保険管理者

DeFi: Decentralized Finance

DeFi Decentralized Finance 非中央集権金融

Replacement of banks, stock companies, ETF, etc.

Money Creation (信用創造)

DEX 非中央集権通貨取引 0x

Market Capitalization
2021.5.16

DeFi	$100 B
Bitcoin	$918 B
ETH	$448 B

Gold	$10,700 B
Apple	$2,120 B
Amason	$1,590 B
FB	$867 B

2021.5.20

Bitcoin	$705 B
ETH	$292 B

On Ethereum

Aave	lending platform
Compound	lending platform
Yearn.finance	distributed aggregator
Uniswap	automated market maker

v3 (2021.5.6)

liquidity mining pool NFT

流動性

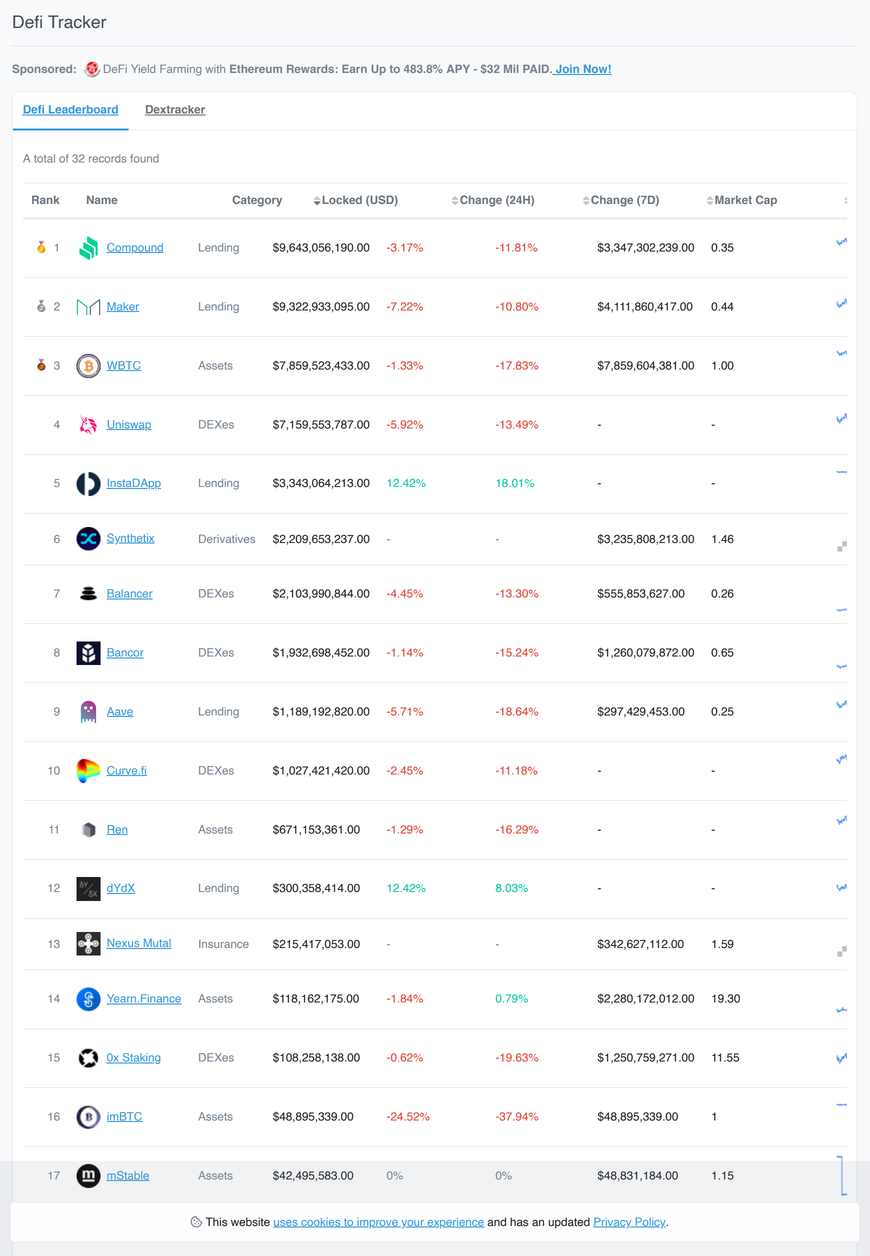
Polcadot platform of blockchains, cross-chain, wrapped coin

Substrate

Binance Smart Chain

Ethereum DeFi Leader Board

https://etherscan.io/defi#defi-leaderboard



Defi Tracker

Sponsored: DeFi Yield Farming with **Ethereum Rewards: Earn Up to 483.8% APY - $32 Mil PAID.** Join Now!

A total of 32 records found

Rank	Name	Category	Locked (USD)	Change (24H)	Change (7D)	Market Cap	
1	Compound	Lending	$9,643,056,190.00	-3.17%	-11.81%	$3,347,302,239.00	0.35
2	Maker	Lending	$9,322,933,095.00	-7.22%	-10.80%	$4,111,860,417.00	0.44
3	WBTC	Assets	$7,859,523,433.00	-1.33%	-17.83%	$7,859,604,381.00	1.00
4	Uniswap	DEXes	$7,159,553,787.00	-5.92%	-13.49%	-	-
5	InstaDApp	Lending	$3,343,064,213.00	12.42%	18.01%	-	-
6	Synthetix	Derivatives	$2,209,653,237.00	-	-	$3,235,808,213.00	1.46
7	Balancer	DEXes	$2,103,990,844.00	-4.45%	-13.30%	$555,853,627.00	0.26
8	Bancor	DEXes	$1,932,698,452.00	-1.14%	-15.24%	$1,260,079,872.00	0.65
9	Aave	Lending	$1,189,192,820.00	-5.71%	-18.64%	$297,429,453.00	0.25
10	Curve.fi	DEXes	$1,027,421,420.00	-2.45%	-11.18%	-	-
11	Ren	Assets	$671,153,361.00	-1.29%	-16.29%	-	-
12	dYdX	Lending	$300,358,414.00	12.42%	8.03%	-	-
13	Nexus Mutal	Insurance	$215,417,053.00	-	-	$342,627,112.00	1.59
14	Yearn.Finance	Assets	$118,162,175.00	-1.84%	0.79%	$2,280,172,012.00	19.30
15	0x Staking	DEXes	$108,258,138.00	-0.62%	-19.63%	$1,250,759,271.00	11.55
16	imBTC	Assets	$48,895,339.00	-24.52%	-37.94%	$48,895,339.00	1
17	mStable	Assets	$42,495,583.00	0%	0%	$48,831,184.00	1.15

This website uses cookies to improve your experience and has an updated Privacy Policy.

Art, Music, Copyright

Creator economy: bringing back the rights to the creators!

Direct control of contents by the creators.

Music creators have only 15-20% royalty of the products without any control.

The rests are taken by the complicated supply chains.

Digital Copyright Control by blockchains

Flexible right control by the creators.

Automatic payments.

Traceable usage: market data collection

Token by the creators

Support by core fans.

Art IPO

Share, dividends, profits for multiple owners

mycelia
sustainable and
vibrant music
industry ecosystem

Imogen Heap

Business Models

Possible blockchain operation of

Uber	taxi
Airbnb	hotel, accommodation

- rating (review) system
- Digital ID
- Privacy protection
- dApp insurance
- auto-driving cars

Sharing economies: car, electricity, space, …

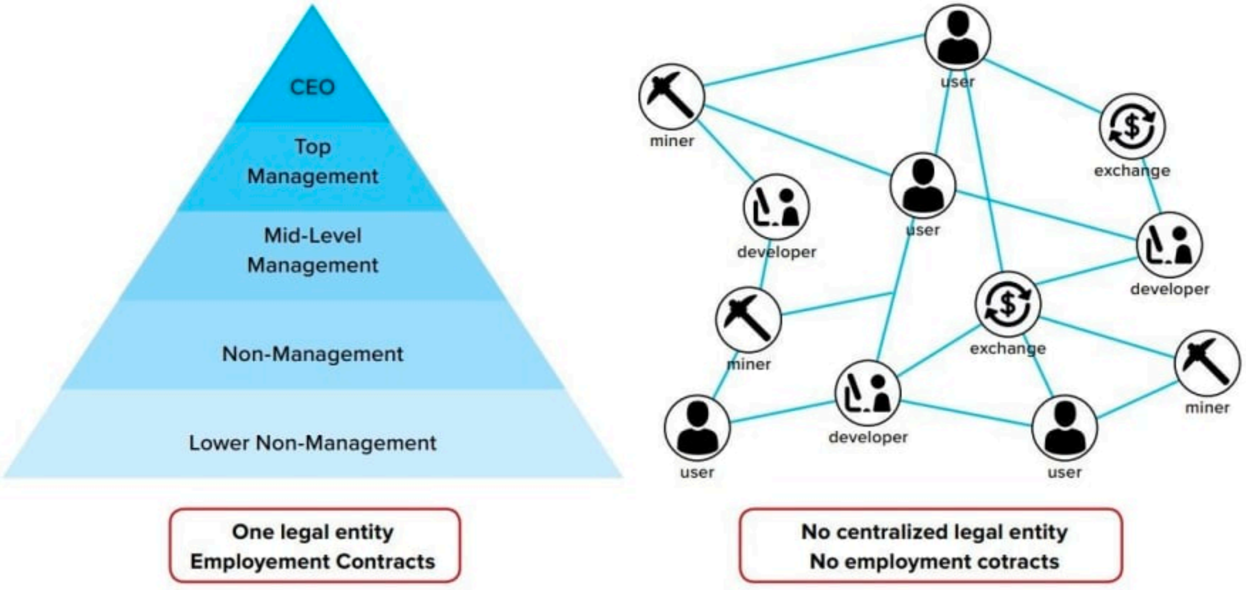
Producer to consumer business, traceability

Organizations

DAO Decentralized Automated Organization

DAC Decentralized Automated Company

operated under smart contract.



Consensys (Ethereum) company is operated under DAO.

Blockchain + IoT

Essentially all the application of IoT is enhanced by the trust communication and reliable record provided by blockchains.

Automatic communication/upgrade of IoT devices

Electricity grid control

Transportation, automatic driving,

Factories, maintenances,

Building management

Shopping

…

Inclusion

Financial inclusion of people in developing countries

- Smart phones are relatively available but bank accounts are not.
  - 2 billion of people does not have an access to financial systems
  - Financial institutions do not have incentive to support poor people.
- Immigrants remittance to the families in the home country.
  - large commission (5-10%), slow transfer (a week), complicated paper procedure, long queue, …
  - $38B/year is paid to the money transfer companies

Distribution of chance instead of redistribution capitals

Donation

- Reliable transfer to the person in need
- Direct support of people in other countries
- Cloud funding, micropayment

Government, Politics, Nation

e-Estonia: Digital Government

Digital IDs (90%)

election, tax payment, social security, hospital

transportation fee

passport, driving license, family / residence registration

official documents recorded in blockchains (open to public)

real estate registration

e-Estonia
The Epic Story of the e-State
Victor Guzun, Kiev, 01.06.2018, Ukrainian Institute of Future
www.guzun.ee

since 1991

digital residence service

open to the world!

launching a company in 20 minutes!

Realization of a Virtual Nation!

independently from the residence place

social contract theory   or Citizen of the World?

V. Future and Summary

Regulation by Governments on Cryptocurrencies

Japan

2016.5.25 Fund Settlement Law (改正資金決済法)成立 2017.4.1 施行

2018.1.26 Coincheck Incident

2019.3.15 資金決済法: 仮想通貨→暗号資産

2021.9- Japan Digital Agency, no explicit statement to blockchain? (デジタル庁)

Japan was a cryptocurrency heaven in 2017…

US

2014.3 IRS defines Bitcoin as capital instead of currency

2019- 8 Bitcoin (&1 Ethereum) ETF applications to SEC (no approval yet)

2021.4 Coinbase IPO

ETF: Exchange Traded Fund

IPO: Initial Public Offering of a stock

Canada

Explicitly promoting blockchain

2020.2.18 Bitcoin ETF launched

2021.4.20 Ethereum ETF launched

China

2017 China regulation of ICO and cryptocurrency exchange

2020.1 China law of cryptography, control by the government

2020.10 Digital Yuan (DECP:デジタル人民元) operation in Shenzhen

ICO: initial coin offering, a popular way to launch a new cryptocurrency or token.

India

2021.3 Planning to prohibit using cryptocurrencies

Estonia

Digital Government

Reactions in Societies

Reactions from established interests

- Bank companies wanted to rule-out cryptocurrencies. Now they are trying to employ blockchain and digital currency under their control

  R3-Consortium MUFG Coin (Mitsubishi-UFJ)

- Facebook is preparing to issue its own cryptocurrency: Diem (Libra)

  in the year 2021?

- Payment by cryptocurrency

- 2016-	in Japan: BIC Camera, Kojima, … more than 300 companies
- 2018	Square (Cash App)
- 2020.10	Paypal
- 2021.3	Tesla (cancelled in 2021.5)

Issues and Concerns to Overcome

Scaling and other technological developments

Long transaction time

Long term liquidity / sustainable incentive
流動性 持続性

Electricity consumption / global warming

Regulation by governments / resistance from establishments

Privacy control / crime and money laundering

Surveillance society 監視社会

Domination by automatic agents AIによる支配

Applications to Our Field?

Broad ideas from younger generations!

NFT

Owner of each nuclear excited states?

Owner of the experimental data, energy spectra?

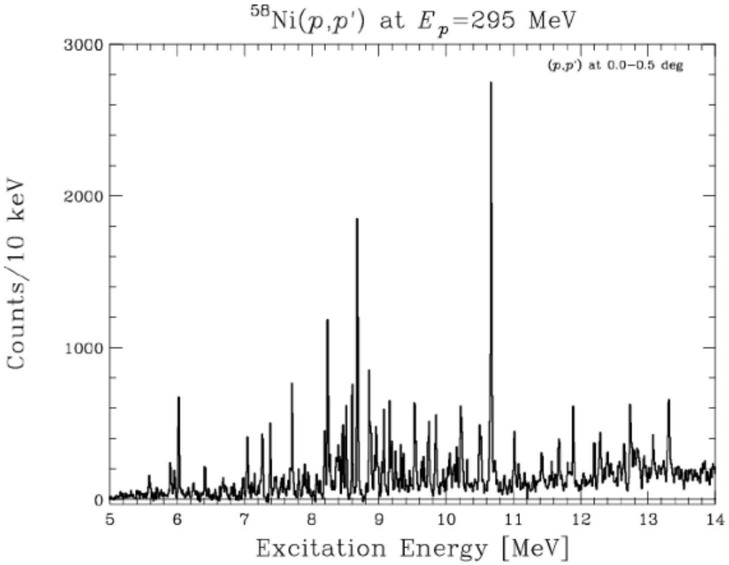
Registration of original ideas or theories?

Registration of a hash of papers?

Decentralized Science Journals

Funding management, application review,

…



Summary and My Messages

Blockchain Technology	Trust Protocol 信頼のプロトコル
- Cryptocurrency	… establishing as a currency
- Smart Contract	… growing quickly
- Other applications	… many applications under development

Satoshi Nakamoto’s dream

“Decentralized peer to peer currency”

has partly been realized but still have a way to be really useful.

Speculative capitalists are obstructing the realization.

High and unstable price!

But I believe Bitcoin or another cryptocurrency will finally realize the dream in near future.

Summary and My Messages

Blockchain technology is very use for many applications and will quickly change the world independently from whether people notice it or not.

Criticism to the electricity consumption:

I personally don't like to the present mining situation of Bitcoin.

However, it is not valid to say mining is just wasting electricity for nothing. Mining is contributing to keep the trust system.

From an opposite view, those workers like accountant, lawyers, bank clarks, or insurance agents are contributing to keep the economy system producing nothing.

Also less demanding consensus protocols are under development.

Summary and My Messages

Blockchain is a creature in the digital world.

Once it is born, it lives by itself with strong viability.

Blockchain+AI: A self-evolutionable blockchain?

I'm quite interested how the blockchain technology changes the world in coming years toward a genuine democratic society.

Develop your new ideas!

References

References

- Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System
- Ethereum White Paper, Yellow Paper
- B. Singhal G. Dhameja, P.S. Panda「ブロックチェーン実践入門」オーム社 (2020)
- ドン・タプスコット, アレックス・タプスコット「ブロックチェーン・レボリューション」ダイヤモンド社 (2016)
- A.M. Antonopoulos and G. Wood 「マスタリング・イーサリアム」 オライリー・ジャパン(2019)
- MIT OpenCourseWare, Gary Gensler, Blockchain Basics and Cryptography, 2018
- 中田敦彦 YouTube大学 「ブロックチェーン」
- 落合陽一「日本再興戦略」幻冬舎 (2018)