 1

②ビットコインシステムにおける資産移転の仕組み

2021年6月23日
才所敏明
（株）IT企画・代表取締役社長
中央大学研究開発機構・研究員
（株）ZenmuTech顧問
toshiaki.saisho@advanced-it.co.jp
http://www.advanced-it.co.jp
https://www.facebook.com/toshiaki.saisho

 2

Personal Profile

- **Mar. 1970 Graduated from the Department of Engineering, University of Tokyo**
- **Apr. 1970～Dec. 1994 Performed various activities at Information Systems Division of Toshiba Corporation**
- **Jan. 1995～Sep. 2007 moved to Security R&D Divisions of Toshiba Corporation**
- **Sep. 2007 Retired from Toshiba Corporation**
- **Oct. 2007～ Established Advanced IT Corporation**
  My current positions are as follows.
  * President of Advanced IT Corporation
  * Executive Advisor of System7 (Los Angeles)
  * Adviser of ZenmuTech (Tokyo)
  * Researcher of Research Institute, Chuo University

Agenda

1. What is Bitcoin
2. Basic features of Blockchain
3. Bitcoin system overview
4. Bitcoin Transaction and Blockchain
5. Creating Bitcoin Transaction
6. Validating Bitcoin Transaction
7. Problems of Bitcoin

In the lecture, I will ask some questions.
I am planning to ask some of you to answer.
So please listen carefully.

Bitcoin（first CryptoAsset system）
The first system that adopted Blockchain

History of Bitcoin

Oct. 2008 Satoshi Nakamoto submitted a paper (Internet).

Jan. 2009 Software to realize the theory of Bitcoin developed.
(Immediately after that, the first transaction was done)

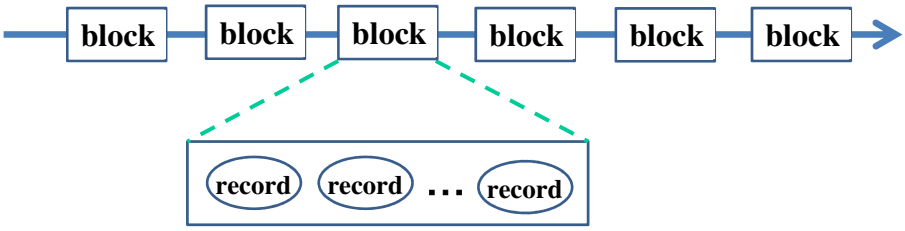
Feb. 2010 First Bitcoin Exchange was opened.

May 2010 First settlement by Bitcoin was done.
2 pizzas (≒$ 25) ＝ 10,000 BTC

Jun 2021 1BTC ≒ $38,244 ≒ ￥4,238,271
2 pizzas ＝ 10,000 BTC ≒ $382,440,000 ≒ ￥42,382,710,000

Blockchain

A chain of blocks storing several records (transactions)



（1）Recording technology without central management organization

（2）Recording technology with extremely low risk of record loss

（3）Recording technology that makes it difficult to falsify past records

（1）Recording technology without central management organization

Necessity of consensus algorithm

How to select a person / organization that composes a block that collects multiple unregistered records and adds it to the blockchain (approves the block)

Examples of consensus algorisms

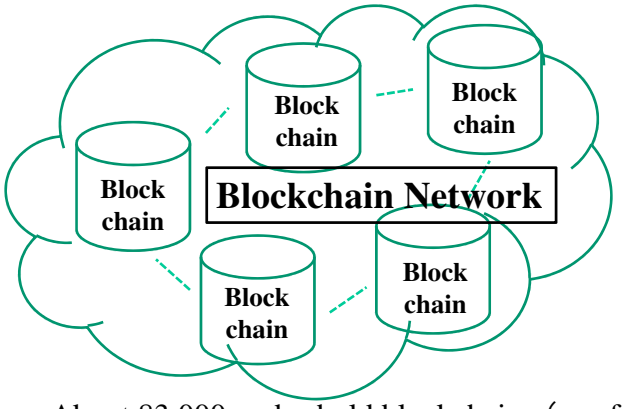
PoW（Proof of Work）: Provide approval rights and rewards to the person who first found the requested information **（Used in Bitcoin）**

PoS（Proof of Stake）: Provide approval rights and rewards based on asset holdings

PoI（Proof of Importance）: Provide approval rights and rewards according to asset holdings and usage

(2) Recording technology with extremely low risk of record loss

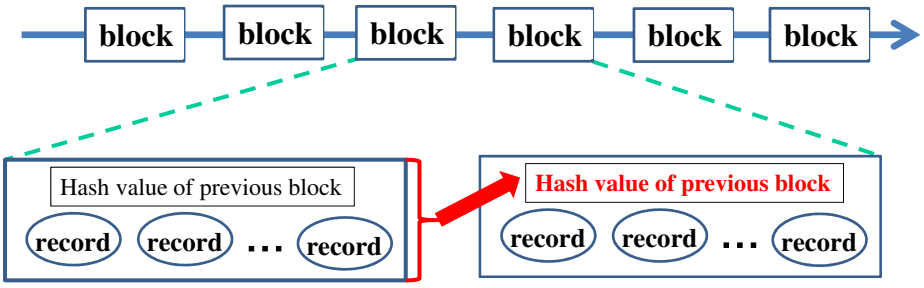
As records are stored and managed by many nodes



Bitcoin: About 83,000 nodes hold blockchains (as of Mar 2021)
The size of Blockchain is 328.57G (as of Mar 2021)

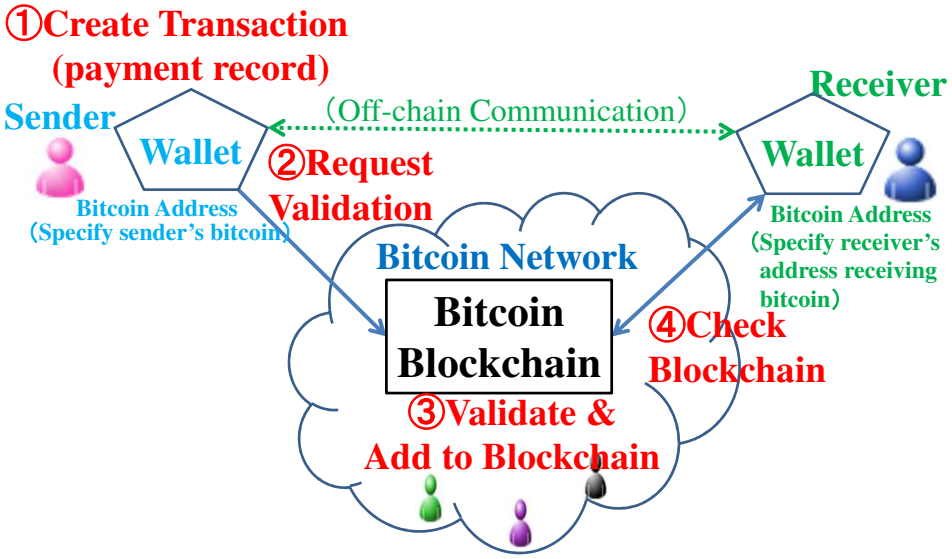
(3) Recording technology that makes it difficult to tampering past records

Because the information (hash value) of the past record is reflected in the subsequent record



In Bitcoin, record is called transaction.

Bitcoin System



Transaction Example
Transfer 10BTC from A to B

Transaction1 (from X to A)

Input	Output
	8BTC for A

Transaction2 (from Y to A)

Input	Output
	7BTC for A

Transaction3 (from A to B)

Input	Output
2nd output of transaction1	10BTC for B
1st output of transaction2	5BTC for A

Chain of Transaction

Output of Transaction1（from X to A）

8BTC	Bitcoin Address of A
（Payment Amount）	（Destination of payment）

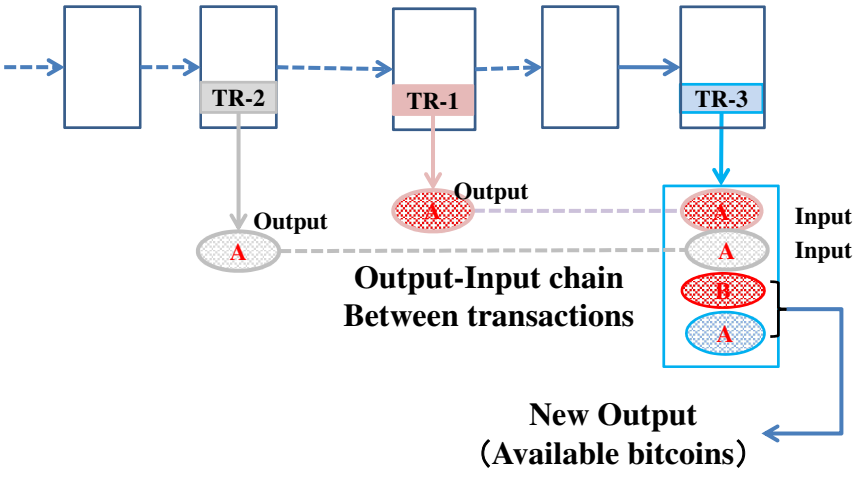
Transaction ID（to transaction）	**Output Index**	**Proof of right to use this bitcoin（Public key, Signature）**

Input of Transaction3（from A to B）

Bitcoin Address：Encoded string of SHARIP value of the Public key
SHARIP：SHA256 hash and then RIPEMD160 hash
Transaction ID：SHASHA value of the transaction
SHASHA：SHA256 hash and then SHA256 hash

Bitcoin Blockchain (transaction history)

Chain of blocks containing multiple transactions



Data structure of transaction

Size	Field	Description
1～9bytes	Number of inputs	Number of transaction inputs
(variable length)	Input	Transaction input
1～9bytes	Number of outputs	Number of transaction outputs
(variable length)	Output	Transaction output

Data structure of transaction input

Size	Field	Description
32bytes	Hash of transaction (Transaction ID)	Pointer to transaction including UTXO to be used for depositing
4bytes	Output index	Index number of UTXO to be used for depositing
1～9bytes	Script size	Length of script in bytes
(variable length)	scriptSig	Script that meets the usage conditions of unused UTXO used for depositing

UTXO：unspent transaction output

Data structure of transaction output

Size	Field	Descryption
8bytes	amount	Value of Bitcoin in Satoshi unit
1～9bytes	Script size	Length of script in bytes
(variable length)	scriptPubKey (bitcoinaddress)	Script to specify necessary conditions to use the amount

Example：A receive 10 BTC from X and send 10 BTC to B

Transaction（TR-X） from X to A

Number of inputs			1
In①	Transaction ID		
	Output index		
	Script size		
	Script Sig	Signature	Signature with X's secret key
		Public key	Public key of X
Number of outputs			1
Out①	amount		10
	scriptPubKey (bitcoinaddress)		Hash of public key of A

Transaction（TR-A） from A to B

Number of inputs			1
In①	Transaction ID		TR-X
	Output index		1
	Script size		size
	script Sig	Signature	Signature with A's secret key
		Public key	Public key of A
Number of outputs			1
Out①	amount		10
	scriptPubKey (bitcoinaddress)		Hash of public key of B

5. Creating Bitcoin Transaction

 17

Transaction（TR-A）from A to B ①

Number of inputs		1
In①	Transaction ID	TR-X
	Output index	1
Number of outputs		1
Out①	amount	10
	scriptPubKey（bitcoinaddress）	Hash of public key of B

Transaction（TR-A）from A to B ②

Number of inputs		1
In①	Transaction ID	TR-X
	Output index	1
	Script size	size
	scriptPubkey	Hash of public key of A
Number of outputs		1
Out①	amount	10
	scriptPubKey（bitcoinaddress）	Hash of public key of B

5. Creating Bitcoin Transaction

 18

Transaction（TR-A）from A to B ②

Number of inputs		1
In①	Transaction ID	TR-X
	Output index	1
	Script size	size
	scriptPubkey	Hash of public key of A
Number of outputs		1
Out①	amount	10
	scriptPubKey（bitcoinaddress）	Hash of public key of B

Hash（SHASHA）

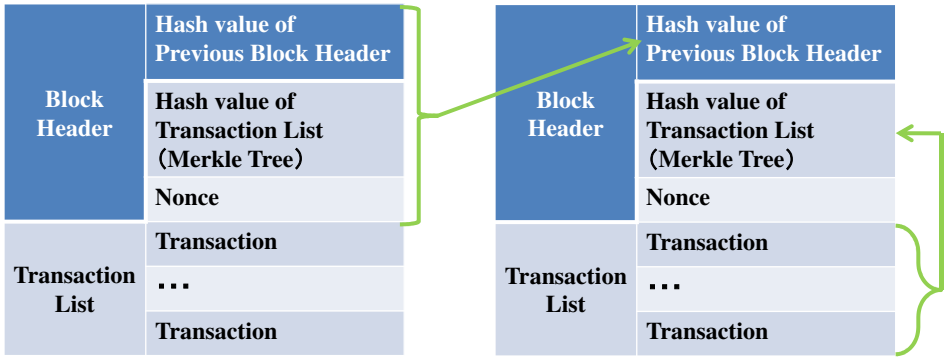
Sign（ECDSA）

Secret Key of A

Transaction（TR-A）from A to B ③

Number of inputs			1
In①	Transaction ID		TR-X
	Output index		1
	Script size		size
	script Sig	Signature	Signature with A's secret key
		Public key	Public key of A
Number of outputs			1
Out①	amount		10
	scriptPubKey（bitcoinaddress）		Hash of public key of B

Chain of Blocks



Selection of transactions to be included in the block
Collect transactions that are not in any blocks yet.
Mining by the miner for each block which it made by that miner
Discover 32bits Nonce such that 256bits hash value（SHA256） of the block becomes a value with 18 0‘s in hexadecimal digits leading at the head.
Construction of Blockchain
Hash Value of previous Block Header (SHASHA)

Mining
（Generating the correct block）

Condition of correct block：
The 256bits hash value（SHA256） of the block is a value with 18 0‘s in hexadecimal digits leading at the head.
Discover random number(Nonce) that satisfy the condition that becomes the correct block earlier than anyone!
A person who first discovered is given a reward. Currently, 12.5BTC.
A reward is paid by a special transaction called a coinbase at the head of the list of transactions.

Validating each Transactions

(1) Check the validity of specified Public Key

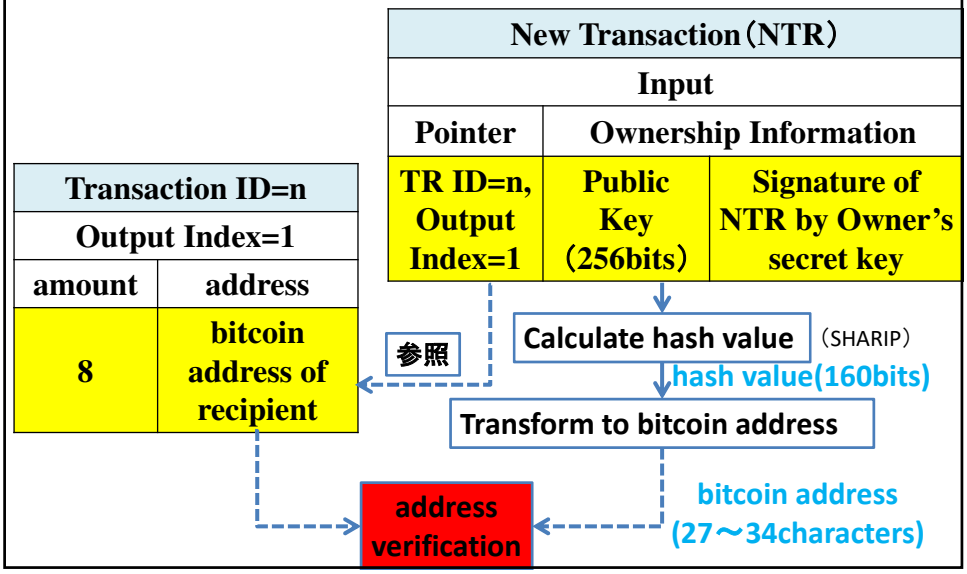
(2) Check the validity of
Transaction owner's private key
by signature verification

(3) Check that the specified output is still unspent

(4) Check that the total of input amount and
the total of output amount are the same

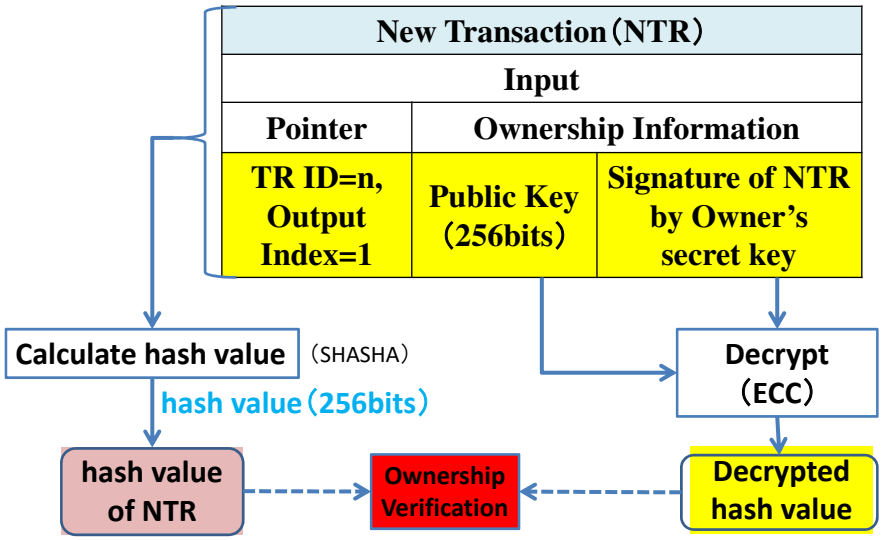
Validation of Transaction (1)

Check the validity of specified Public Key



Validation of Transaction（2）

Check the validity of TR owner's private key by signature verification



Future of Bitcoin and Blockchain

Blockchain technology has many new possibilities and is expected to be widely used in society.

However, there are many challenges with Bitcoin, its first application system.

(1) Problems that accelerate global warming
Huge power consumption in mining competition
➔To adopt a consensus algorithm other than PoW

(2) Problem of privacy leakage
Bitcoin blockchain is open to the public.
A certain degree of anonymity is ensured,
but it is also possible to identify users and assets.

(3) Problem of rapid increase Bitcoin abuse for money laundering, financing for terrorists, fraudulent and illegal transaction settlement, etc.
A certain level of anonymity guarantee encourages Bitcoin abuse.

It is expected that the application of blockchain will expand in the future while avoiding the issues pointed out by Bitcoin.

End