Overview of Blockchain and Bitcoin

2019-06-27
Toshiaki Saisho
Advanced IT Corporation
toshiaki.saisho@advanced-it.co.jp

 1

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**
  (My role) Promotion of practical use of IT in research and development in the Toshiba G companies
  Instruction and Support for engineers and researchers for advanced use of Computer, Network and various softwares
- **Jan. 1995～Sep. 2007 moved to Security R&D Divisions of Toshiba Corporation**
  (My role) Leading the research and development of security technology and business support activity
  Leading various research and development projects sponsored by the government
- **Sep. 2007 Retired from Toshiba Corporation**

 2

- **Oct. 2007～ Established Advanced IT Corporation**

  Current business of my company is
  consulting on R&D and the business activities
  based on the latest Information Technology
  and Information Security Technology.

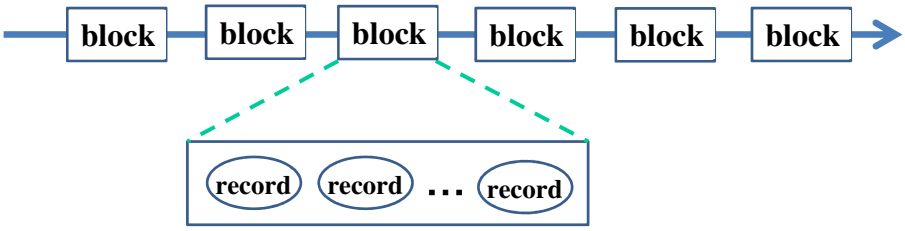
  My current positions are as follows.
  * President of Advanced IT Corporation
  * Executive Advisor of System7 (Los Angeles)
  * Adviser of ZenmuTech (Tokyo)
  * Researcher of Research Institute, Chuo University

Agenda

1. Basic features of Blockchain
2. Overview of Bitcoin and Bitcoin system
3. Overview of
   Bitcoin Transaction and Blockchain
4. Creating Bitcoin Transaction
5. Validating Bitcoin Transaction

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 block chain (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

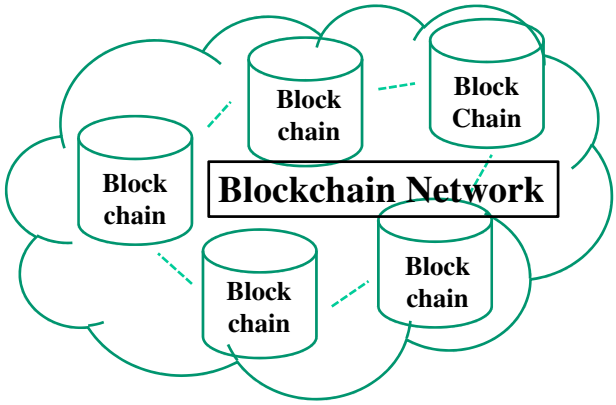
PoS（Proof of Stake）: Provide approval rights and rewards based on asset holdings

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

1. Basic features of Blockchain

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

As records are stored and managed by many nodes

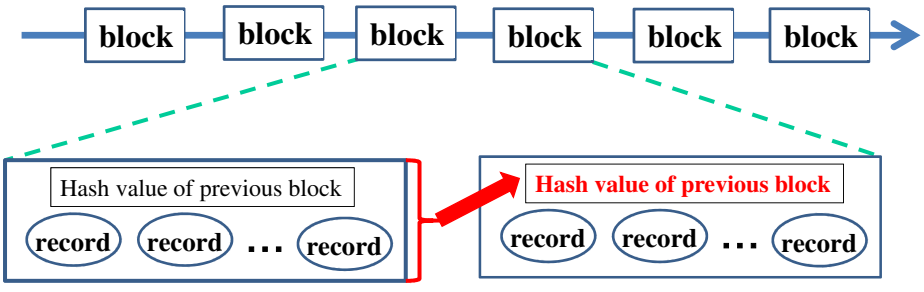


Reference: For Bitcoin, about 10,000 nodes hold block chains (as of February 2019)
(210GB＋5～10GB/month)

1. Basic features of Blockchain

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

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



  15 25

Bitcoin is the first realization system of Blockchain technology!

Bitcoin is the first CryptoAssets!

History of Bitcoin

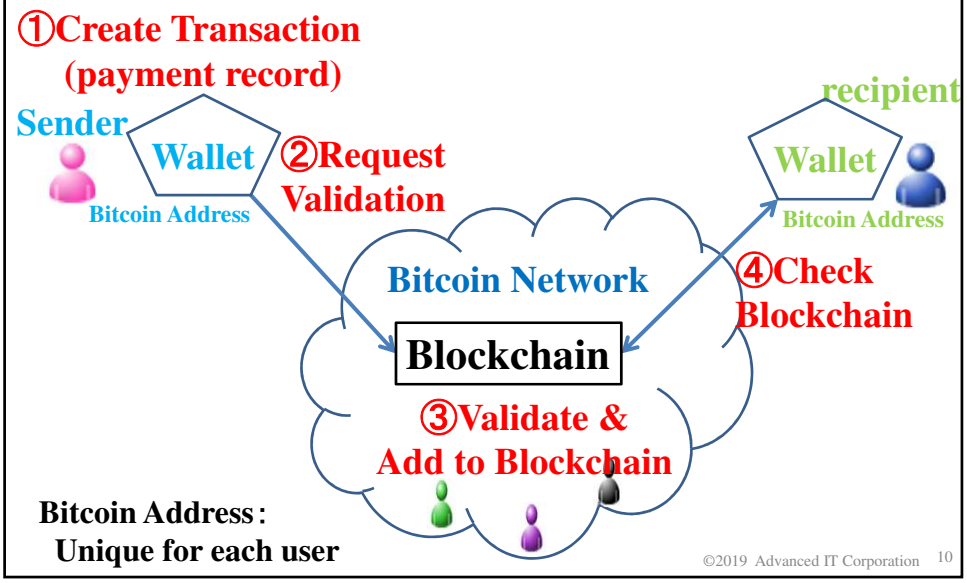
Oct. 2008 Satoshi Nakamoto submitted a paper (Internet).

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 (1 BTC ≒ 0.2 yen)

Bitcoin System



Bitcoin Address:
Unique for each user

Transaction Example
Transfer 10BTC from A to B

Transaction1（from X to A）

Input	Output
	8BTC for A

Transaction3（from A to B）

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

Transaction2（from Y to A）

Input	Output
	7BTC 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)**

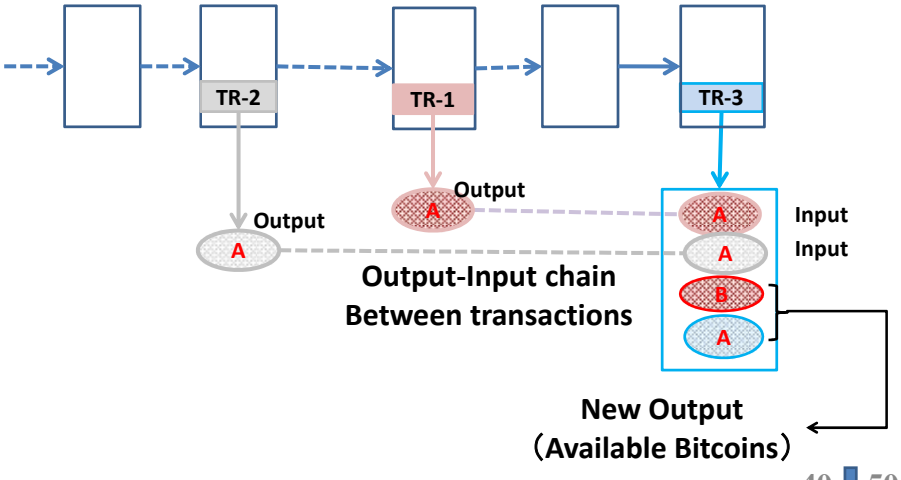
Input of Transaction3（from A to B）

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

3. Overview of Bitcoin Transaction and Blockchain

Blockchain (transaction history DB)

Chain of blocks containing multiple transactions



 13 40 ⬇ 50

4. Creating Bitcoin Transaction

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

 14

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

4. Creating Bitcoin Transaction

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

Transaction (TR-2) 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-1
	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

4. Creating Bitcoin Transaction

①

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

②

Number of inputs			1
In①	Transaction ID		TR-1
	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

4. Creating Bitcoin Transaction

②

Number of inputs		1
In①	Transaction ID	TR-1
	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

③

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

4. Creating Bitcoin Transaction

Chain of Blocks

Block Header	Hash value of Previous Block	
	Hash value of Transaction List (Merkle Tree)	
	Nonce	
Transaction List	Transaction	
	…	
	Transaction	

Block Header	Hash value of Previous Block	
	Hash value of Transaction List (Merkle Tree)	
	Nonce	
Transaction List	Transaction	
	…	
	Transaction	

Selection of transactions to be included in the block
Collect transactions that are not in any blocks yet.
Plus its own compensation transaction (called coin base).

Mining by the minor for each block which it made by that minor
To discover Nonce such that the hash value of the block becomes a hash value with 16 0's at the head.

Construaction of BlockChain
Hash Value of previous Block Header (SHASHA)

4. Creating Bitcoin Transaction

Mining
(Generating the correct block)

A block is a collection of transactions.
First, collect transactions that are not included in any block yet,
and then add its own compensation transaction to its collection,
and then compute the hash by adding an arbitrary numerical value (Nonce)
to discover Nonce whose hash value satisfies the condition of correct block.

Hash value of Previous Block Header	Hash value of Transaction List (Merkle Tree)	Nounce (randum number)	Transaction List

Condition of correct block:
The hash value(SHASHA) of the block is a hash value with 16 0's at the top!
Discover random number(Nounce) that satisfy the condition
that becomes the correct block earlier than anyone!
A person who first discovered is given a reward. Currently, 25 BTC.
(Rate:1BTC ≒79,550Yen June, 2016 , 1BTC ≒941,200Yen June, 2019)

A reward is paid by a special transaction called a coinbase
at the head of the list of transactions.

 21 65

5. Validating Bitcoin Transaction

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

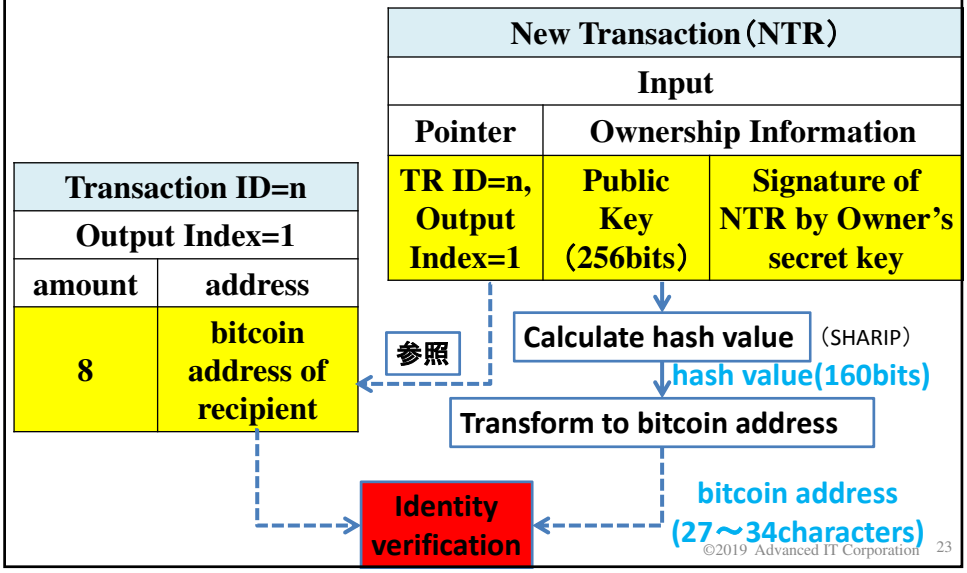
(4) Check that the total of input amount and
the total of output amount are the same

 22

5. Validating Bitcoin Transaction

Validation of Transaction（1）

Check the validity of specified Public Key

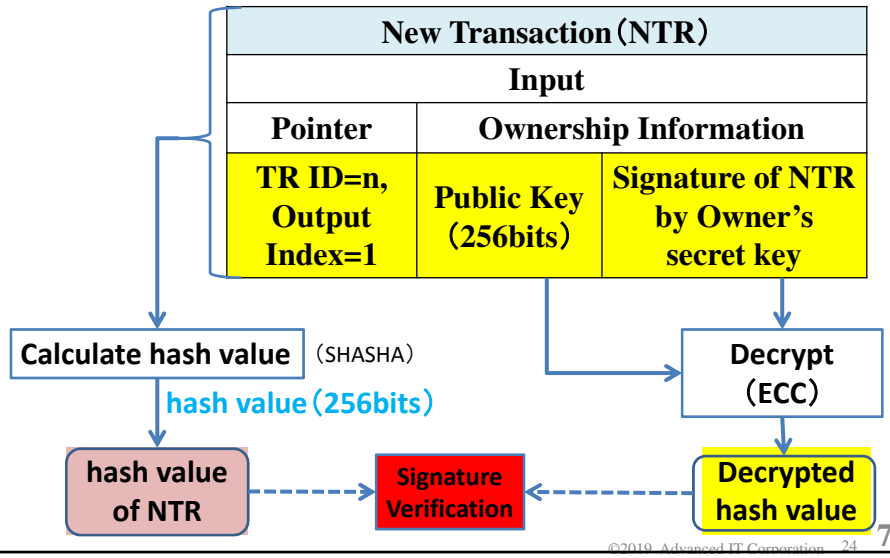


 23

5. Validating Bitcoin Transaction

Validation of Transaction（2）

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



 24 75

End

