Introduction to Blockchain and its Structure

Contents

- ➢ **What is blockchain?**
  - . History of blockchain
  - . Definition of blockchain
- ➢ **Structure of blockchain**

What is blockchain?

1. History of blockchain

- 1983, Development of ‘Blind Signature’ technology
  - “Hidden signature for non-trackable payments”, David Chaum, 1982
  - Handles technology to verify payment without exposing the identity of the trading partner
  - The proposed digital signature technology and cryptography related concepts are developed as the basis of cryptography

David Chaum

1. History of blockchain

- 1989, Established DigiCash (David Chaum)
  - A digital currency company based on your own ideas
  - Application of encryption, private key and public key, blind signature technology
  - ECash, the world's first cryptographic currency, with a unique hash value attached to a digitized dollar
  - Unlike credit cards where banks know all transactions, ECash guarantees anonymity that the third party can not know about transactions
  - In 1994, DigiCash succeeded in the first electronic apprival using ECash, and in 1995 it partnered with a small US bank to operate ECash digital money
  - It is bankrupt to the consumers who prefer convenience than privacy protection and a universal credit card

1. History of blockchain

- Developed HashCash technology in 1997
  - Adam Back proposed Hashcash as a Proof of Work (PoW) system to prevent email spam and DoS attacks in 1997

- Hashcash
  - Hashcash is a PoW system developed to prevent mass spam
  - To send an e-mail, a hash cache stamp must be received in advance. To receive this stamp, a computer proof operation (PoW) is performed to find a certain hash.
  - Work proof method introduced by Hachcash is applied to bitcoin developed by Satoshi Nakamoto later

Adam Back

source : http://wiki.hash.kr/

1. History of blockchain

- Bit Gold Technology ,1998
  - Nick Szabo devised the principle and structure of a virtual currency called "bit gold" in 1998 called the origin of bit coin
  - Decentralization Digital money allows participants to solve cryptographic puzzles through computing resources
  - Many people on the same network need to acknowledge the answer as valid so they can move on to the next puzzle
  - Once the puzzle is unlocked and passed the network certification, the puzzle becomes part of the next puzzle
  - Contributing to solving the double payment problem of digital money by blocking fraud through copy / paste

Nick Szabo

1. History of blockchain

- Proposal of B-Money in 1998
  - "B-Money, Anonymous, Distributed Electronic Cash System, Wei Dai, 1998 (www.weidai.com/bmoney.txt)
  - Designed B-Money, which greatly influenced the birth of Bitcoin
  - Each participant encrypts information about how much each participant has in B-Money, as a hash function in a separate database, and stores them as linked blocks
  - When a new block is added due to transaction occurrence, the PoW that gives the B-Money incentive to the successful participants first by decrypting the password, and the PoS which gives the incentive preference to some participants according to the amount of the crypto-money, Suggested method

Wei Dai

* PoW : Proof of Work, PoS : Proof of Stake

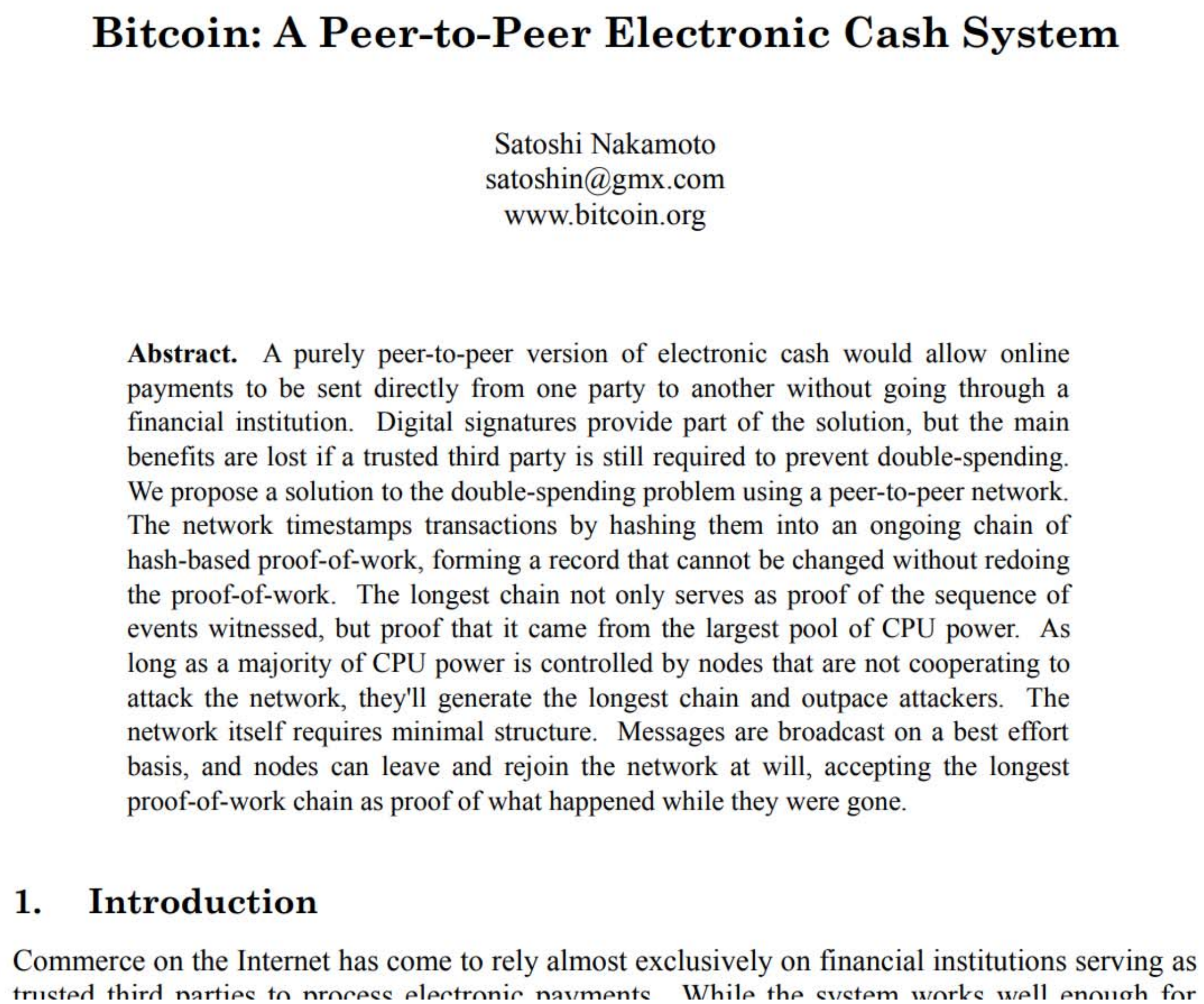
1. History of blockchain

- In 1998, B-Money presented five preconditions for establishing an electronic cash system
  1. Significant amounts of computational power and verification
  2. Compensation system for computer work
  3. Collective group ledgers that are recognized and updated by all members
  4. Transfer of funds is listed on the collected group ledger and verified through cryptographic hash
  5. Collective group ledgers that are recognized and updated by all members

1. History of blockchain

- 2008, Bitcoin (Satoshi Nakamoto)
  - Bitcoin is the first cipher made based on blockchain technology
  - Bitcoin's Currency unit: BTC
  - "Bitcoin: A Peer-to-peer Electronic Cash System"
  - "Proof of Work"
  - Peer-to-peer Network
  - Secure/distributed Ledger Management
  - SHA-256 hash algorithm based Mining
  - Bitcoin's market capitalization is $ 100 billion as of July 2018, or about 100 trillion won, which is the cigar currency of market cap

1. History of blockchain



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.

1. Introduction

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for

1. History of blockchain

- Bitcoin deployment in 2009
  - In January 2009, a person who writes a nickname of Satoshi Nakamoto was developed in C ++ language.
  - January 3, 2009 Satoshi Nakamoto developed bitcoin to create the first block, genesis block
  - January 10, Satoshi Nakamoto distributes bitcoin source code written in C ++ programming language as free open source by e-mail

1. History of blockchain

- First bitcoin mining in 2009
  - In January 2009, Satoshi Nakamoto mined 50 BTCs on his PC and then remitted 10-bit coins to Hal Finney (PGP developer, second to Phil Zimmermann)
  - Hal Finney mined bitcoin from his PC, at that time the block number was in the 70s, and he was the first bitcoin miner except the founder

Hal Finney

1. History of blockchain

- Bitcoin first paymen in 2009
  - Bitcoin trading has begun, but has not gained much attention in a few years, spreading a little around the enthusiast layer
  - At the time of the first FX announcement in October 2009, $ 1 = 0.00076 BTC, and the spread is accelerated.
  - On May 22, 2010, a programmer named Laszlo Hanyecz, based in Florida, USA, bought two pizzas for the first time using Bitcoin
  - At the time, the price of the second edition of Pizza was $ 40, which paid 10,000-bit coins. As of May 7, 2019, 10,000 BTC is a huge amount of about 69.1 billion won

Laszlo Hanyecz is the Pizza ordered
with bitcoin (2010)

1. History of blockchain

- Established Blockstream in 2014 (Adam Back)

- Adam Back founded Blockstream, and on August 15, 2017, almost everyone on the globe launched a blockchain satellite service to launch satellites to access bitcoin block-chain data without the Internet

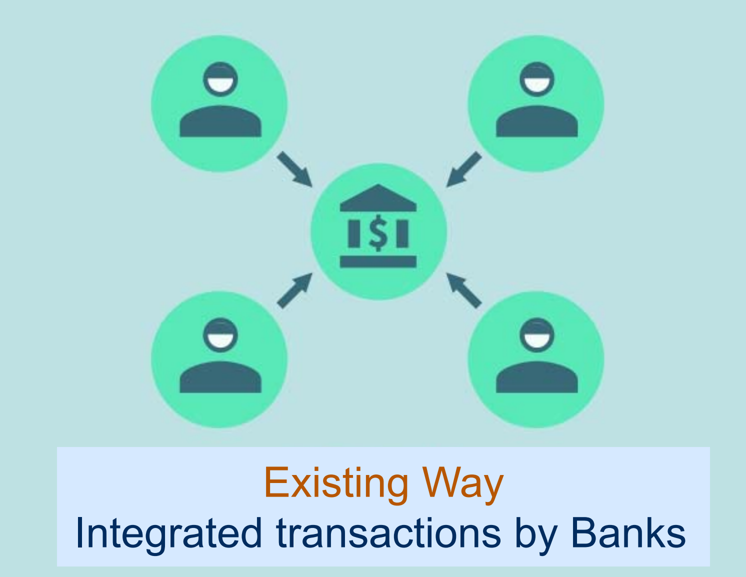
- Block Chain Satellite is the world's first public satellite service that allows anyone to operate and maintain a bitcoin node that can store the entire transaction history without restrictions on the network.

2. Definition of Blockchain

- What is the BlockChain?
  - o A kind of data distribution storage technolog
  - o Connect block data as chain
  - o Stored data is distributed to all users and stored
  - o Because of this distributed storage characteristic, it is also called Distributed Ledger Technology
  - o Bitcoin is the basic technology for the Bitcoin
  - o Bitcoin is the result of applying the block chain to ‘Currency'

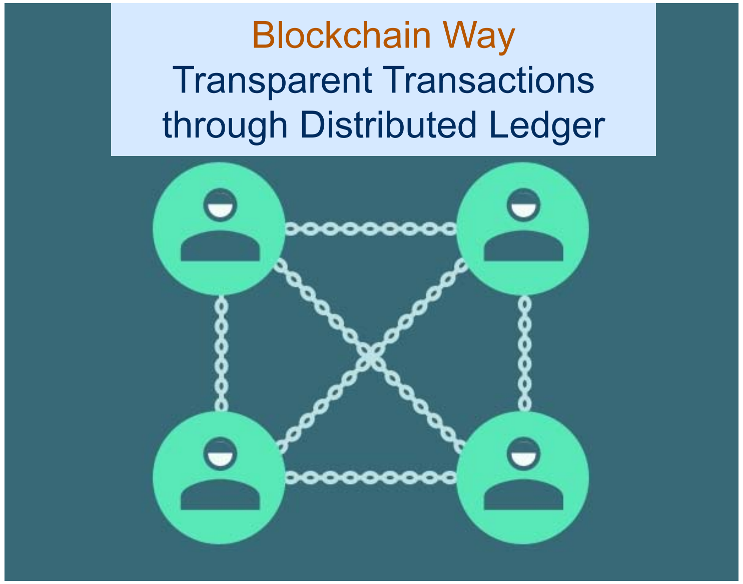
2. Definition of Blockchain

- Distributed Open Ledger
  - o Block-chain technology enables transparent history management without central management by sharing the same ledgers (data) between all users



Existing Way

Integrated transactions by Banks



Blockchain Way

Transparent Transactions through Distributed Ledger

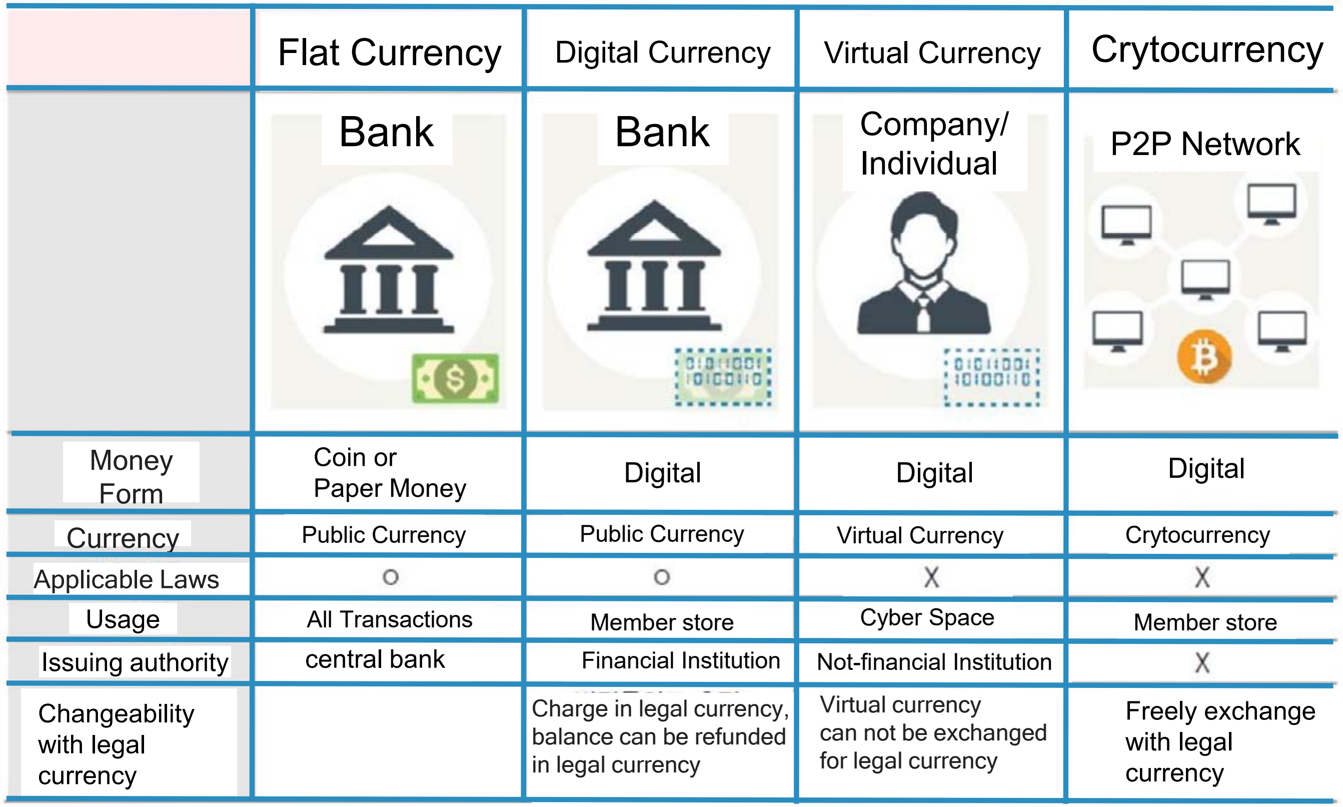
2. Definition of Blockchain

- Existing Transaction Method
  - The existing transaction method was that the bank had all the transaction details
  - The central bank has proven that A has sent $ 10,000 to B
  - The parties to the transaction must trust the central bank and leave all proof of transaction

- Blockchain Transaction Method
  - Stores transaction details rather than central bank
  - The fact that A sent money to B is saved to all participating nodes.
  - All the participating nodes have proven that they sent money

Type of Curreny

Comparison of Flat Currency, Digital Currency, Virtual Currency and Cryptocurrency



	Flat Currency	Digital Currency	Virtual Currency	Crytocurrency
	Bank	Bank	Company/ Individual	P2P Network
Money Form	Coin or Paper Money	Digital	Digital	Digital
Currency	Public Currency	Public Currency	Virtual Currency	Crytocurrency
Applicable Laws	○	○	X	X
Usage	All Transactions	Member store	Cyber Space	Member store
Issuing authority	central bank	Financial Institution	Not-financial Institution	X
Changeability with legal currency		Charge in legal currency, balance can be refunded in legal currency	Virtual currency can not be exchanged for legal currency	Freely exchange with legal currency

https://brunch.co.kr/@bzconomics/19

Blockchain Structure

https://coinmarketcap.com

3. Structure of Blockchain

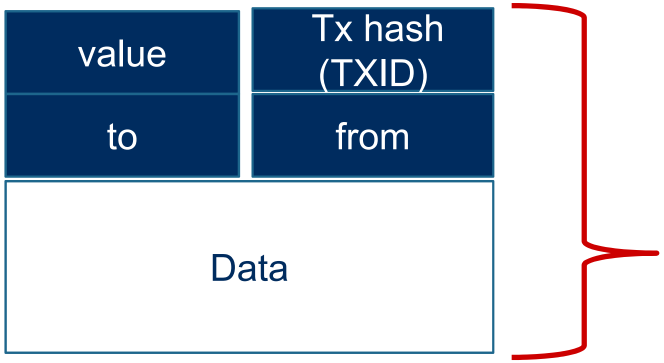
- Transaction

- Generate data to be stored in transaction units

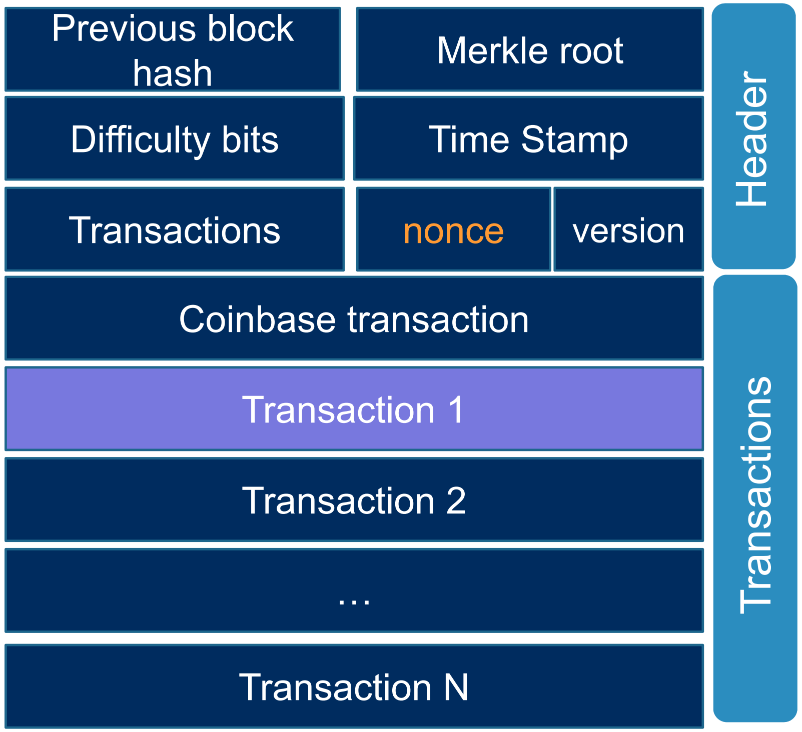
- Block

- Record a set of transactions in block

Example of the transaction



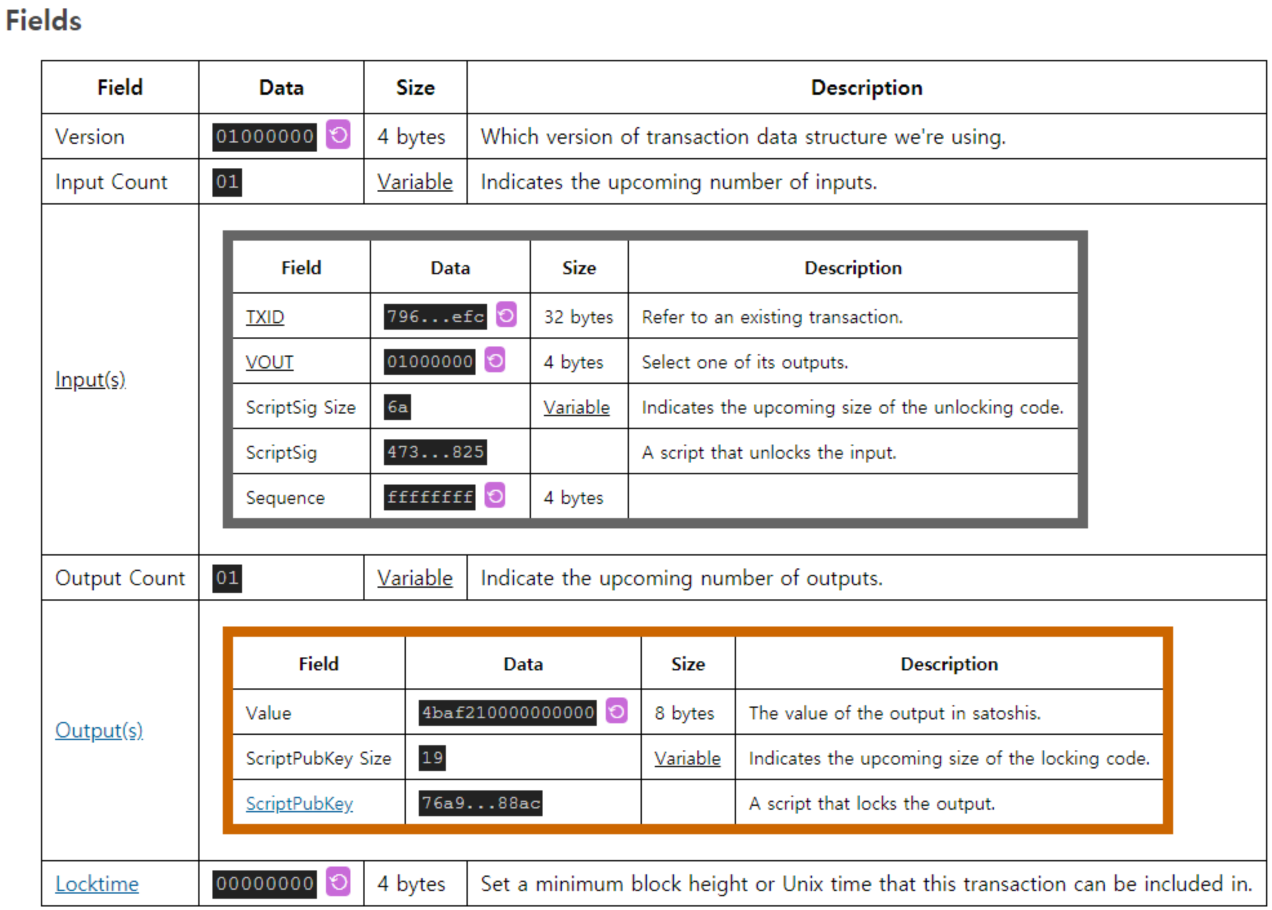
Example of the Block Structure



* A *TXID* (Transaction ID) is basically an *identification number* for a bitcoin transaction.
* You get a TXID by hashing transaction data through SHA256 twice.

*If we suppose blocks are generated every 10 minutes, 80 bytes * 6 * 24 * 365 = 4.2MB per year : block header

3. Structure of Blockchain: Transaction Data of Bitcoin



Fields

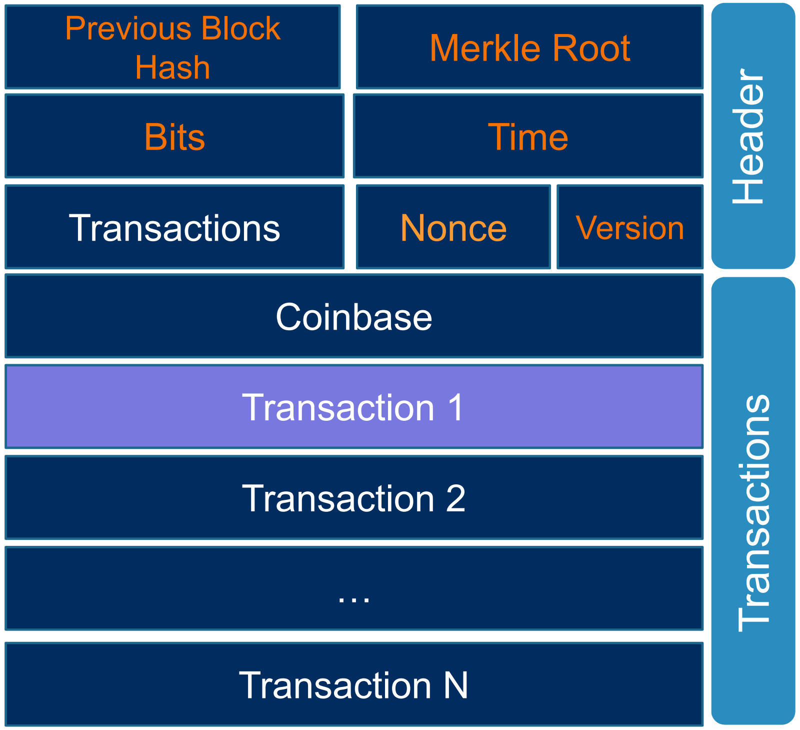
<table>
<tr><th>Field</th><th>Data</th><th>Size</th><th>Description</th></tr>
<tr><td>Version</td><td>01000000</td><td>4 bytes</td><td>Which version of transaction data structure we're using.</td></tr>
<tr><td>Input Count</td><td>01</td><td>Variable</td><td>Indicates the upcoming number of inputs.</td></tr>
<tr><td>Input(s)</td><td colspan="3">
<table>
<tr><th>Field</th><th>Data</th><th>Size</th><th>Description</th></tr>
<tr><td>TXID</td><td>796...efc</td><td>32 bytes</td><td>Refer to an existing transaction.</td></tr>
<tr><td>VOUT</td><td>01000000</td><td>4 bytes</td><td>Select one of its outputs.</td></tr>
<tr><td>ScriptSig Size</td><td>6a</td><td>Variable</td><td>Indicates the upcoming size of the unlocking code.</td></tr>
<tr><td>ScriptSig</td><td>473...825</td><td></td><td>A script that unlocks the input.</td></tr>
<tr><td>Sequence</td><td>ffffffff</td><td>4 bytes</td><td></td></tr>
</table>
</td></tr>
<tr><td>Output Count</td><td>01</td><td>Variable</td><td>Indicate the upcoming number of outputs.</td></tr>
<tr><td>Output(s)</td><td colspan="3">
<table>
<tr><th>Field</th><th>Data</th><th>Size</th><th>Description</th></tr>
<tr><td>Value</td><td>4baf210000000000</td><td>8 bytes</td><td>The value of the output in satoshis.</td></tr>
<tr><td>ScriptPubKey Size</td><td>19</td><td>Variable</td><td>Indicates the upcoming size of the locking code.</td></tr>
<tr><td>ScriptPubKey</td><td>76a9...88ac</td><td></td><td>A script that locks the output.</td></tr>
</table>
</td></tr>
<tr><td>Locktime</td><td>00000000</td><td>4 bytes</td><td>Set a minimum block height or Unix time that this transaction can be included in.</td></tr>
</table>

- f4184fc596403b9d638783cf57adfe4c75c605f6356fbc91338530e9831e9e16 - First ever Bitcoin transaction to Hal Finney in 2010.
- a1075db55d416d3ca199f55b6084e2115b9345e16c5cf302fc80e9d5fbf5d48d - Pizza transaction for 10,000 BTC in 2010.

3. Structure of Blockchain

- Block

✓Record a set of transactions in block



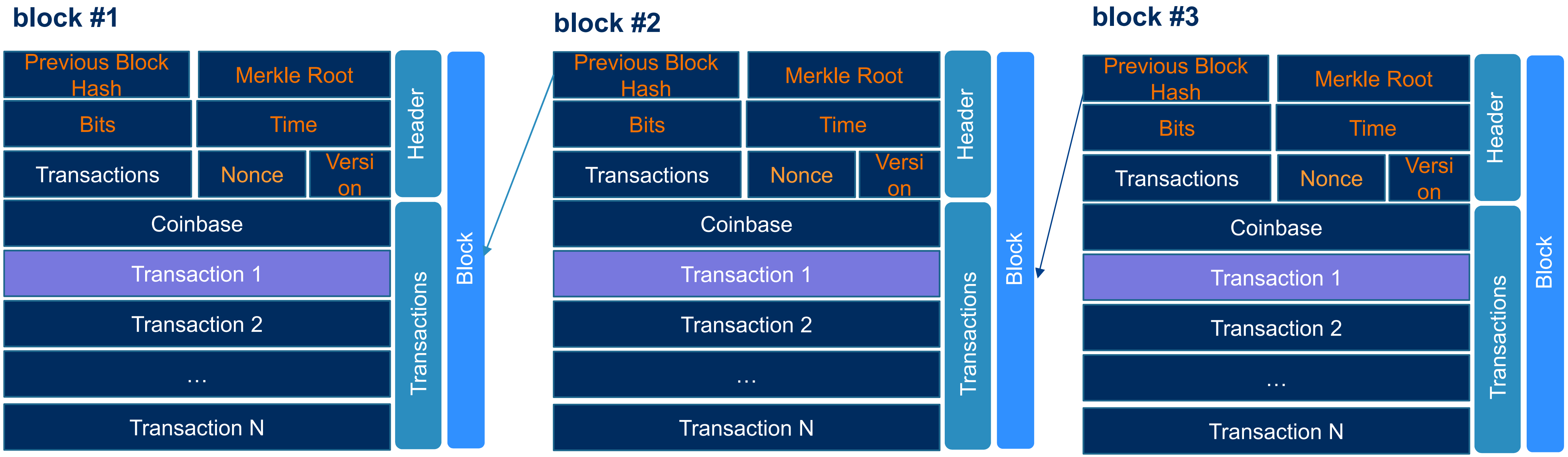
Block header (80bytes)

Field	Description
Version	The version of the block.
Previous Block Hash	The Block Hash of the block that this block is being built on top of. This is what "chains" the blocks together. (by SHA256)
Merkle Root	All of the transactions in this block, hashed together. Basically provides a single-line summary of all the transactions in this block.
Time	When a miner is trying to mine this block, the *Unix* time at which this block header is being hashed is noted within the block header itself.
Bits	A shortened version of the Target.
Nonce	The field that miners change in order to try and get a hash of the block header (a Block Hash) that is below the Target.

- Transactions: Number of transactions
- Coinbase : A *coinbase transaction* is the first transaction in a block. Miners use it to collect the block reward, and any additional transaction fees
- Transaction: Transaction record

3. Structure of Blockchain

- Chain
  - o Blocks are associated with each other using the 'previous block hash' value



block #1

Previous Block Hash | Merkle Root
Bits | Time
Transactions | Nonce | Version
Coinbase
Transaction 1
Transaction 2
…
Transaction N

Header
Transactions
Block

block #2

Previous Block Hash | Merkle Root
Bits | Time
Transactions | Nonce | Version
Coinbase
Transaction 1
Transaction 2
…
Transaction N

Header
Transactions
Block

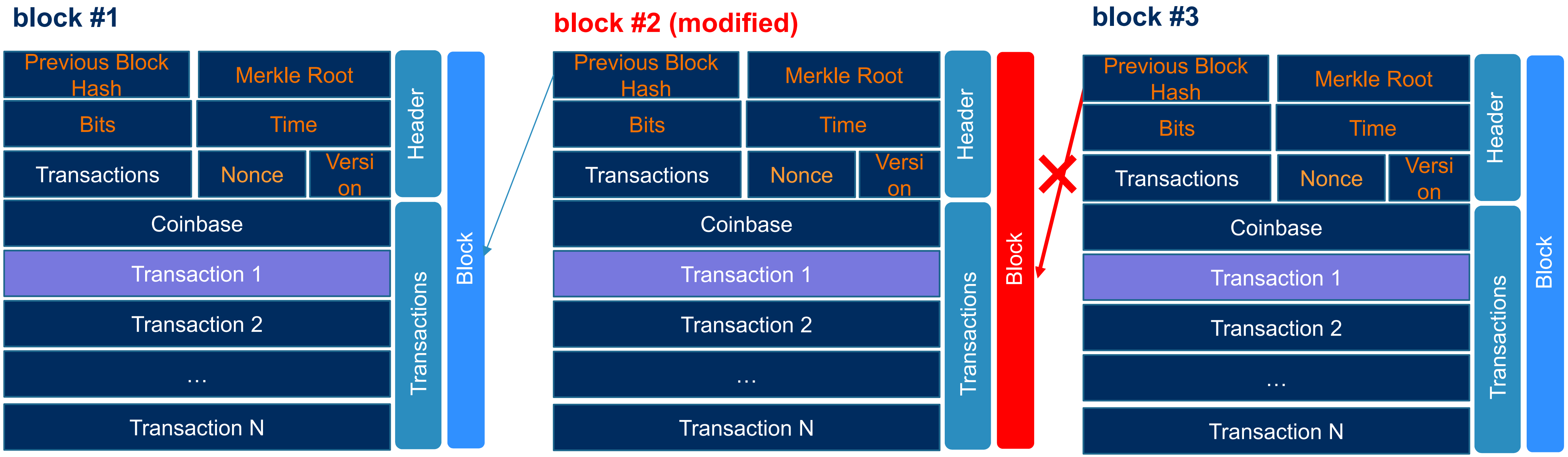
block #3

Previous Block Hash | Merkle Root
Bits | Time
Transactions | Nonce | Version
Coinbase
Transaction 1
Transaction 2
…
Transaction N

Header
Transactions
Block

3. Structure of Blockchain

- Prevent data tampering by chain
  - When modulating block # 2, the previous block hash stored in block # 3 does not point to modulated block # 2, so it can not be linked and stored in chain form



block #1

Previous Block Hash | Merkle Root
Bits | Time
Transactions | Nonce | Version
Coinbase
Transaction 1
Transaction 2
…
Transaction N

Header
Transactions
Block

block #2 (modified)

Previous Block Hash | Merkle Root
Bits | Time
Transactions | Nonce | Version
Coinbase
Transaction 1
Transaction 2
…
Transaction N

Header
Transactions
Block

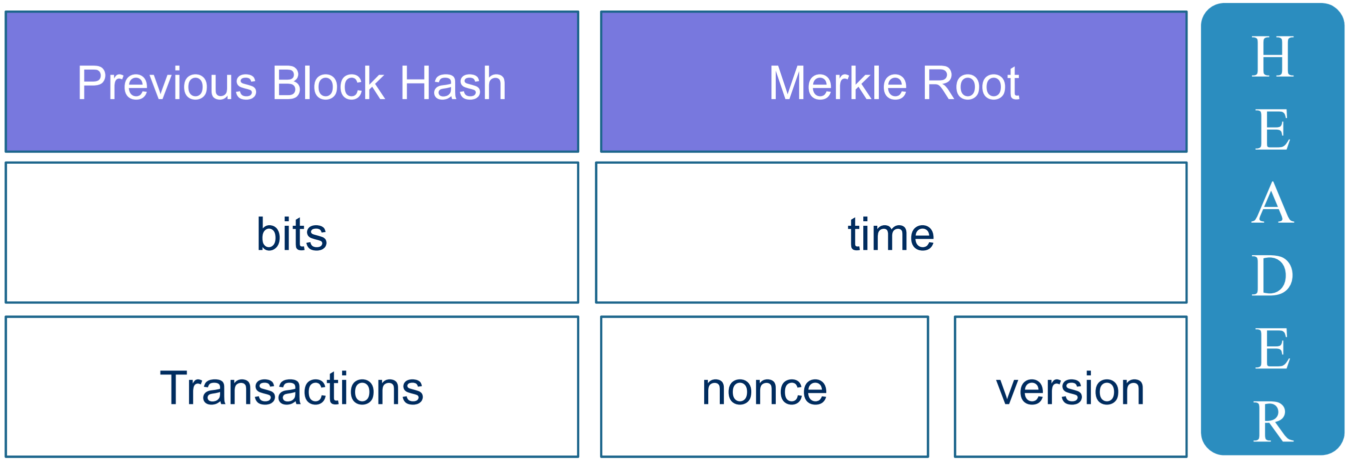
block #3

Previous Block Hash | Merkle Root
Bits | Time
Transactions | Nonce | Version
Coinbase
Transaction 1
Transaction 2
…
Transaction N

Header
Transactions
Block

3. Structure of Blockchain : Block Header

- Previousblockhash
  - o The hash of the block located immediately before the block
- Merklehash
  - o When constructing a hash of each transaction contained in a block as a binary tree, the hash value located in the tree root



Previous Block Hash

Merkle Root

bits

time

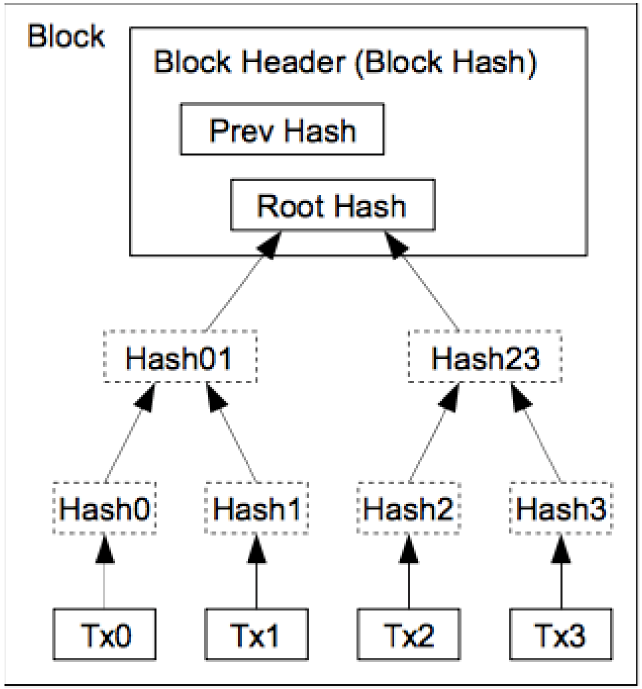
Transactions

nonce

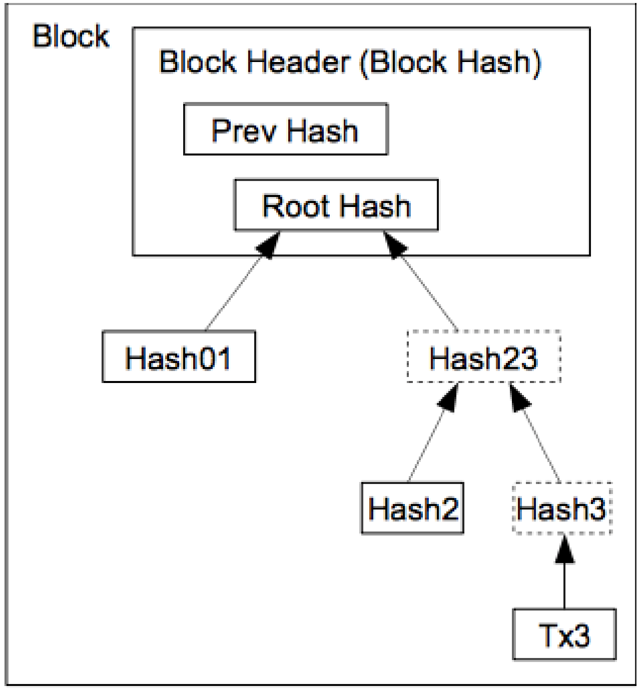
version

HEADER

3. Structure of Blockchain: Merkle Hash Tree



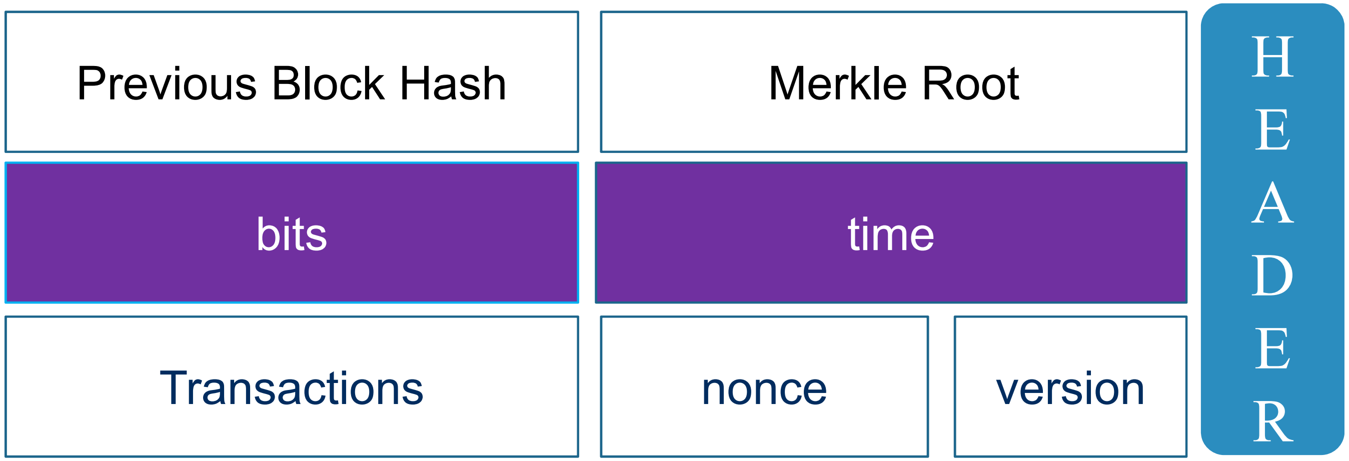
Transactions Hashed in a Merkle Tree



After Pruning Tx0-2 from the Block

3. Structure of Blockchain: block header

- Time stamp
  - o The time the block was created
- bits
  - o Value for difficulty control



Previous Block Hash

Merkle Root

bits

time

Transactions

nonce

version

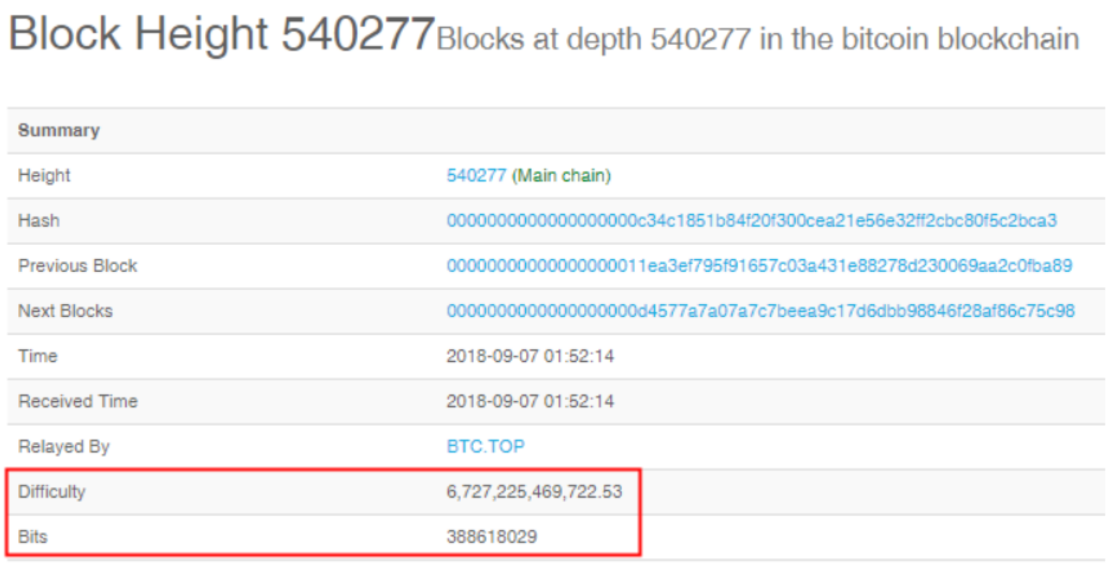
HEADER

3. Structure of Blockchain

See the difficulty information in bit coin block 540277

link: https://www.blockchain.com/en/btc/block-height/540277

- Difficulty : 6,727,225,469,722.53
- Bits : 388618029 = 0x1729D72D



Block Height 540277 Blocks at depth 540277 in the bitcoin blockchain

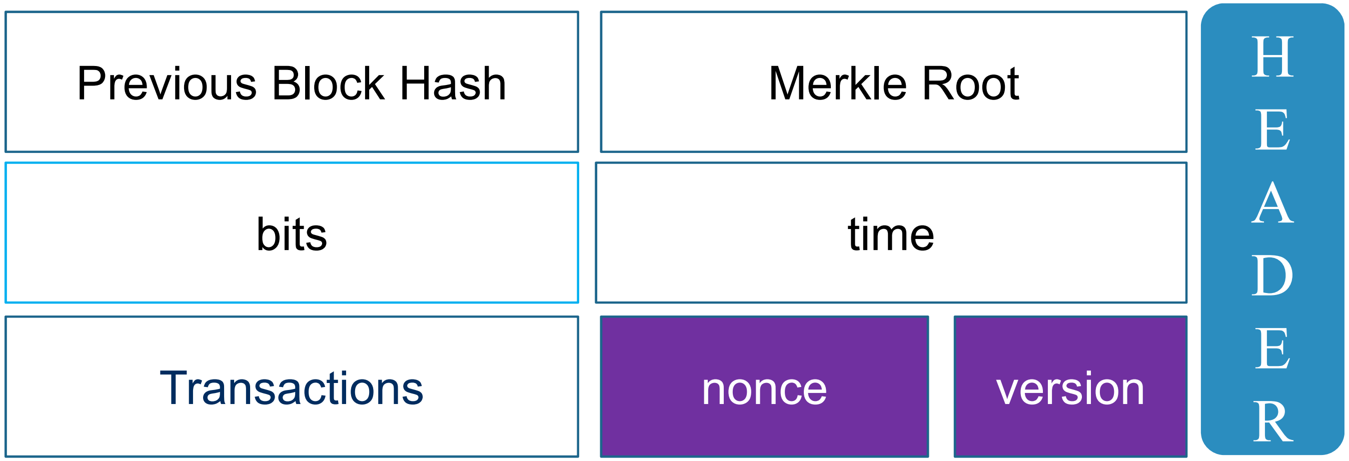
Summary	
Height	540277 (Main chain)
Hash	0000000000000000000c34c1851b84f20f300cea21e56e32ff2cbc80f5c2bca3
Previous Block	00000000000000000011ea3ef795f91657c03a431e88278d230069aa2c0fba89
Next Blocks	0000000000000000000d4577a7a07a7c7beea9c17d6dbb98846f28af86c75c98
Time	2018-09-07 01:52:14
Received Time	2018-09-07 01:52:14
Relayed By	BTC.TOP
Difficulty	6,727,225,469,722.53
Bits	388618029

Difficulty means what times as difficult as the easiest difficulty(=genesis). It is difficult to 6,727.... times.

3. Structure of Blockchain: block header

- Nonce
  - A value that increases by 1, starting at the first zero and finding a hash value satisfying the condition

- **Version**
  - Software or Protocol Version

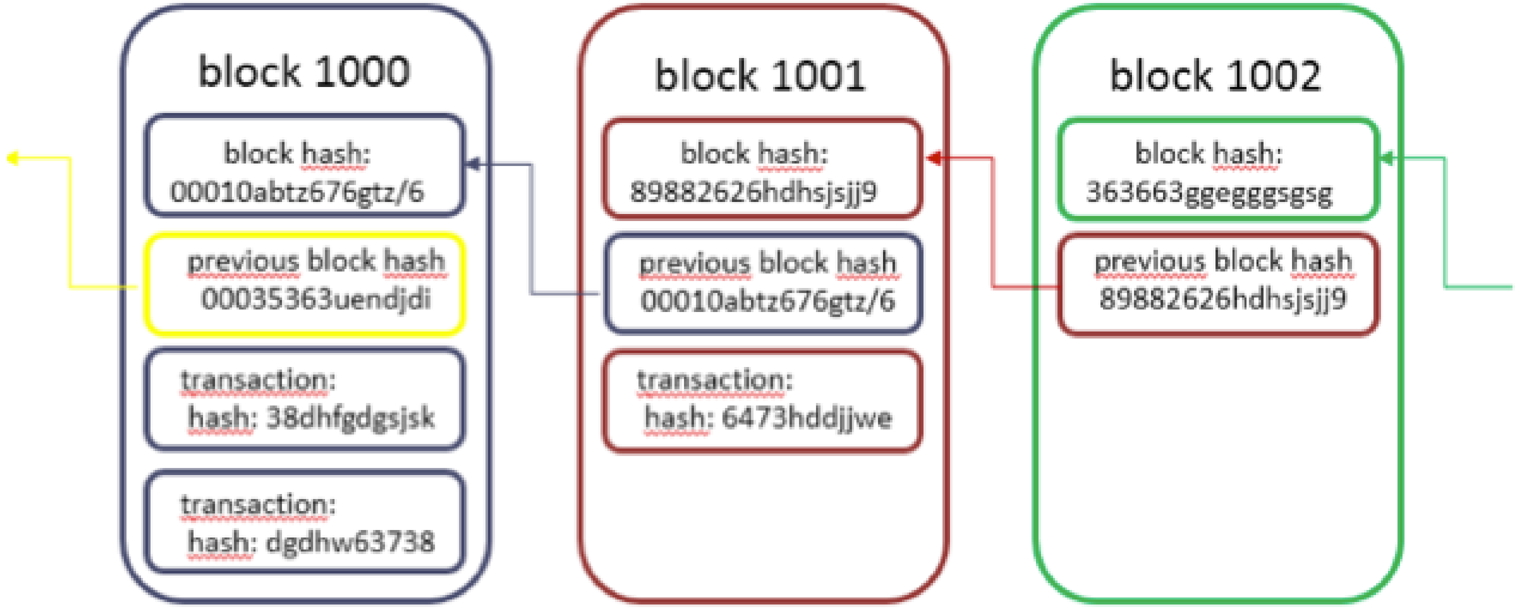


3. Structure of Blockchain : Block Hash

- Discriminator (id) of Block
- The value calculated by applying SHA256 hash function with 6 block header information as input value
- The name is a block hash, but the value is not a hash of the entire block, but a hash of the block header

3. Structure of Blockchain: block Hash

- Be conneted with previous block using previousblockhash value of block header



block 1000

block hash: 00010abtz676gtz/6

previous block hash 00035363uendjdi

transaction: hash: 38dhfgdgsjsk

transaction: hash: dgdhw63738

block 1001

block hash: 89882626hdhsjsjj9

previous block hash 00010abtz676gtz/6

transaction: hash: 6473hddjjwe

block 1002

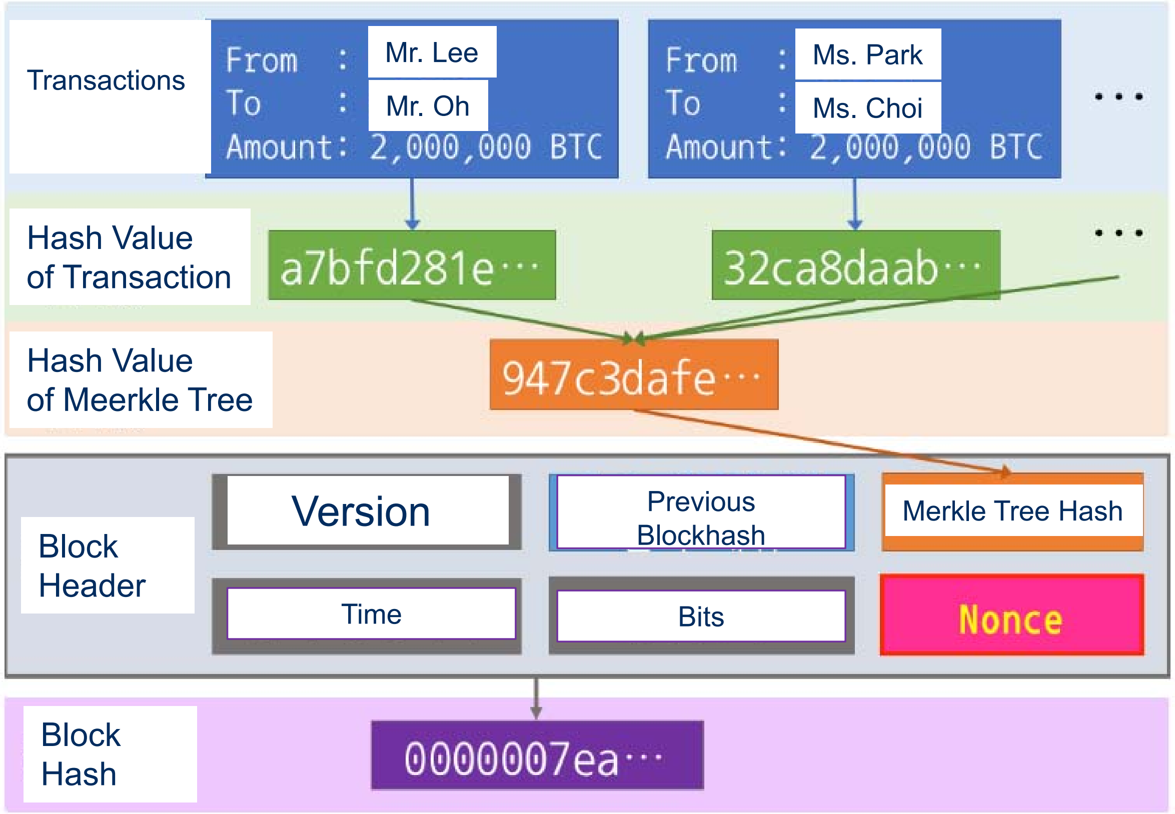
block hash: 363663ggegggsgsg

previous block hash 89882626hdhsjsjj9

3. Structure of Block : Block Generation

- Individual transaction information is aggregated with Merklehash
- Version, Previousblockhash, Merklehash, Time, Bits : Five header information is established at the time of creating the block hash.
- We need to obtain a nonce value to obtain a block hash value and create a valid block with this block hash value as an identifier

3. Structure of Block : Block Generation



Source : https://homoefficio.github.io

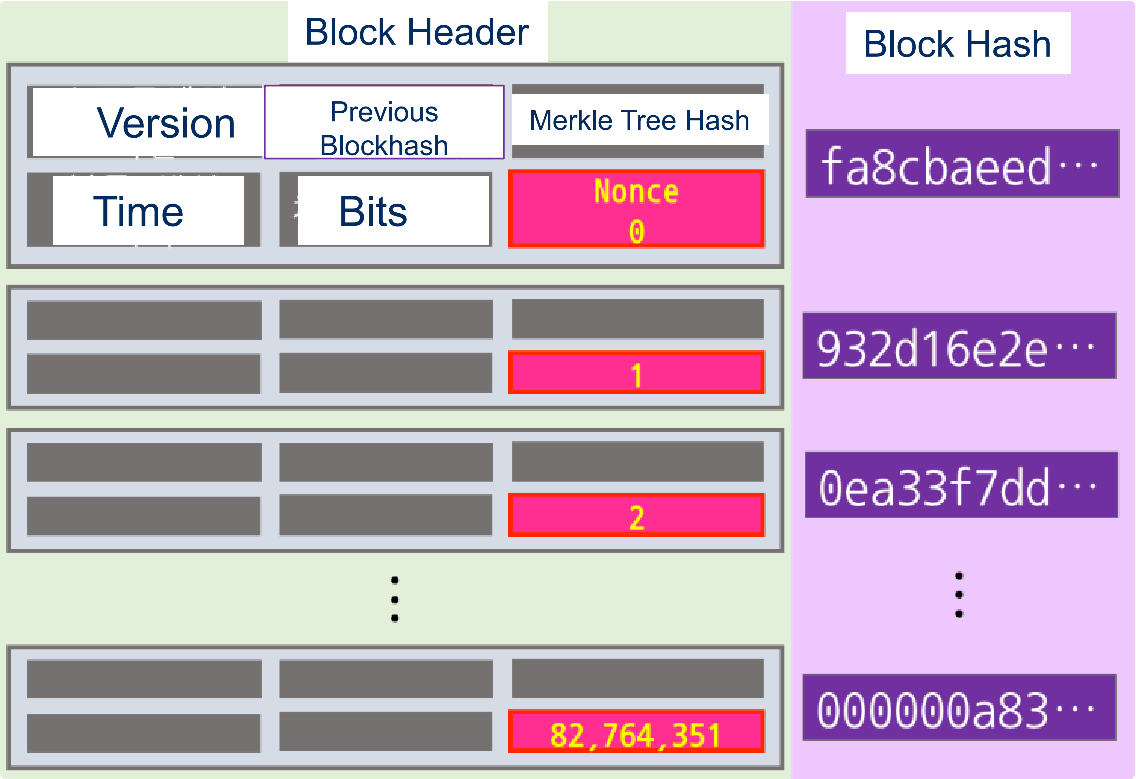
3. Structure of Block : PoW (Mining)

- We need to obtain a nonce value to obtain a block hash value and create a valid block with this block hash value as an identifier

- Nonce value refers to a value that makes the block hash value less than a certain number, calculated as one of the input values of this Nonce value.

3. Structure of Block : PoW (Mining)

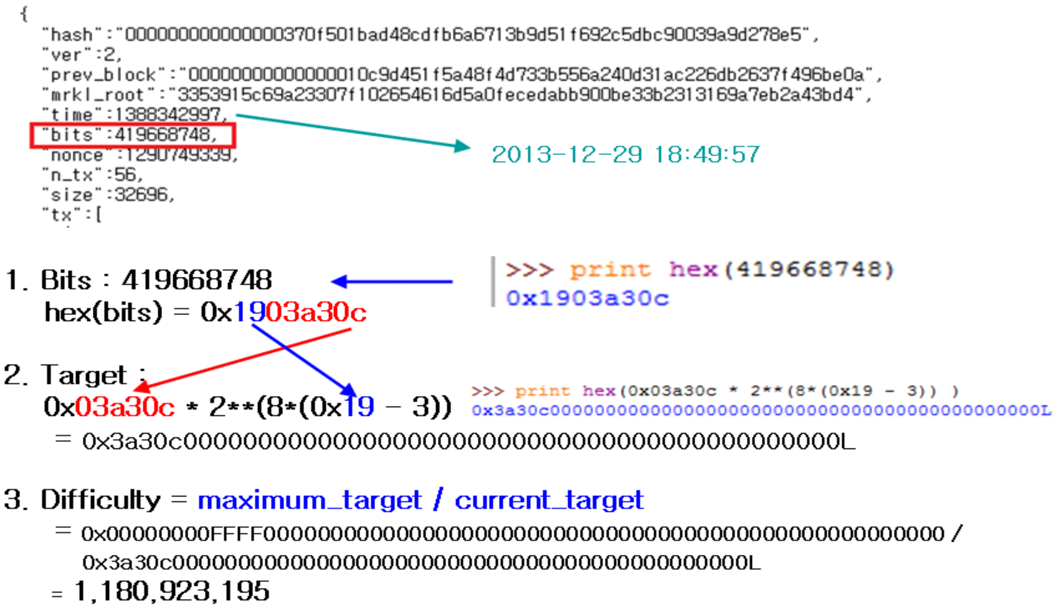
- The process of obtaining the Nonce value that causes the block hash to be smaller than a specific value of 000000a84 ...



Source : https://homoefficio.github.io

3. Structure of Block : PoW (Mining)

The method of obtaining the difficulty from bits



```
{
  "hash":"000000000000000370f501bad48cdfb6a6713b9d51f692c5dbc90039a9d278e5",
  "ver":2,
  "prev_block":"000000000000000010c9d451f5a48f4d733b556a240d31ac226db2637f496be0a",
  "mrkl_root":"3353915c69a23307f102654616d5a0fecedabb900be33b2313169a7eb2a43bd4",
  "time":1388342997,
  "bits":419668748,
  "nonce":1290749339,
  "n_tx":56,
  "size":32696,
  "tx":[
```

2013-12-29 18:49:57

1. Bits : 419668748
   hex(bits) = 0x1903a30c

```
>>> print hex(419668748)
0x1903a30c
```

2. Target :
   0x03a30c * 2**(8*(0x19 – 3))
   = 0x3a30c00000000000000000000000000000000000000000000L

```
>>> print hex(0x03a30c * 2**(8*(0x19 - 3)) )
0x3a30c00000000000000000000000000000000000000000000L
```

3. Difficulty = maximum_target / current_target
   = 0x00000000FFFF0000000000000000000000000000000000000000000000000000 /
   0x3a30c00000000000000000000000000000000000000000000L
   = 1,180,923,195

. difficulty = difficulty_1_target / current_target

. The highest possible target (difficulty 1) is defined as 0x1d00ffff

. difficulty_1_target can be different for various ways to measure difficulty. Traditionally, it represents a hash where the leading 32 bits are zero and the rest are one (this is known as "pool difficulty" or "pdiff"). The Bitcoin protocol represents targets as a custom floating point type with limited precision; as a result, Bitcoin clients often approximate difficulty based on this (this is known as "bdiff")

. The **target** is a 256-bit number (extremely large) that all Bitcoin clients share. The SHA-256 hash of a block's header must be lower than or equal to the current target for the block to be accepted by the network. The lower the target, the more difficult it is to generate a block

3. Structure of Blockchain : Reward

- Excessive CPU, electricity is consumed to obtain Nonce value
- Reward is the sum of the newly issued Block and the transaction fees of the transaction included in the block
- Makes the first deal to deposit a certain amount of bit coins in the block to be created to the mined successful miner
- Reward in case of Bitcoin,
  - o 1~210,000th blocks : 50BTC
  - o 210,000th ~ 420,000th blocks : 25BTC
  - o 420,000th ~ 630,000th blocks : 12.5BTC

Q & A