



Blockchain #5

Bitcoin - 2

Prof. Byung Il Kwak



- ❑ Bitcoin's nodes
 - ▣ Full nodes
 - ▣ Lightweight nodes
- ❑ Merkle tree
- ❑ PoW (Proof-of-Work)
 - ▣ Hash-based PoW
 - ▣ Mining pool

CONTENTS

- ❑ Bitcoin's block

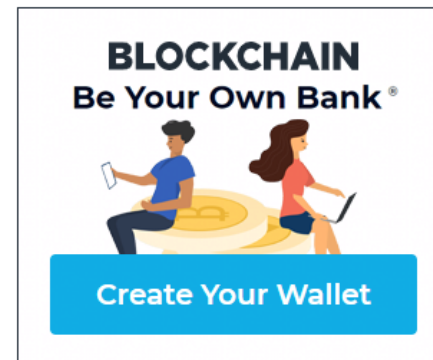
Genesis block (Block #0)

Summary

Number Of Transactions	1
Output Total	50 BTC
Estimated Transaction Volume	0 BTC
Transaction Fees	0 BTC
Height	0 (Main Chain)
Timestamp	2009-01-03 18:15:05
Received Time	2009-01-03 18:15:05
Relayed By	Unknown
Difficulty	1
Bits	486604799
Size	0.285 kB
Weight	0.896 kWU
Version	1
Nonce	2083236893
Block Reward	50 BTC

Hashes

Hash	00000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f
Previous Block	00
Next Block(s)	00000000839a8e6886ab5951d76f411475428afc90947ee320161bbf18eb6048
Merkle Root	4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b



```
GetHash() = 0x00000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f
hashMerkleRoot = 0x4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b
txNew.vin[0].scriptSig = 486604799 4 0x736b6e616220726f662074756f6069616220646e6f63657320666f206886e997262206e6f20726f606e636e61684320393030322f6e614a2f333020736560695420656854
txNew.vout[0].nValue = 5000000000
txNew.vout[0].scriptPubKey = 0x5f1df1682b704c8a578d0b8af74d385cde12c11ee50455f3c436ef4c3fbcf649b60e611feae06279a60939e028a8065c10b73071a6f16719274855feb0f08a6704 0P_CHECKSIG
block.nVersion = 1
block.nTime = 1231006505
block.nBits = 0x1d00ffff
block.nNonce = 2083236893

CBlock(hash=00000000019d6, ver=1, hashPrevBlock=0000000000000, hashMerkleRoot=4a5e1e, nTime=1231006505, nBits=1d00ffff, nNonce=2083236893, vtx=1)
  CTransaction(hash=4a5e1e, ver=1, vin.size=1, vout.size=1, nLockTime=0)
    CTxin(COutPoint(000000, -1), coinbase 04ffff001d01044554689652054696d657320303332f4a616e2f32303039204368616e6365636563f72206f6e206272696e6b206f66207365636f6e64206261696c6f757420666f722062616e6b73)
    CTxOut(nValue=50.00000000, scriptPubKey=0x5f1df1682b704c8a578d0b8af74d385cde12c11ee50455f3c436ef4c3fbcf649b60e611feae06279a60939e028a8065c10b73071a6f16719274855feb0f08a6704 0P_CHECKSIG)
  vMerkleTree: 4a5e1e
```

Genesis block (Block #0)

Block #0

BLOCKCHAIN
Be Your Own Bank®




Create Your Wallet

Summary	
Number Of Transactions	1
Output Total	50 BTC
Estimated Transaction Volume	0 BTC
Transaction Fees	0 BTC
Height	0 (Main Chain)
Timestamp	2009-01-03 18:15:05
Received Time	2009-01-03 18:15:05
Relayed By	Unknown
Difficulty	1
Bits	486604799
Size	0.285 kB
Weight	0.896 kWU
Version	1
Nonce	2083236893
Block Reward	50 BTC

Hashes	
Hash	00000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f
Previous Block	00
Next Block(s)	00000000839a8e6886ab5951d76f411475428afc90947ee320161bbf18eb6048
Merkle Root	4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b

BLOCKCHAIN
Be Your Own Bank®



Create Your Wallet

Block #1

Summary

Number Of Transactions	1
Output Total	50 BTC
Estimated Transaction Volume	0 BTC
Transaction Fees	0 BTC
Height	1 (Main Chain)
Timestamp	2009-01-09 02:54:25
Received Time	2009-01-09 02:54:25
Relayed By	Unknown
Difficulty	1
Bits	486604799
Size	0.215 kB
Weight	0.616 kWU
Version	1
Nonce	2573394689
Block Reward	50 BTC

Hashes

Hash	00000000839a8e6886ab5951d76f411475428afc90947ee320161bbf18eb6048
Previous Block	00000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f
Next Block(s)	000000006a625f06636b8bb6ac7b960a8d03705d1ace08b1a19da3fdcc99ddb
Merkle Root	0e3e2357e806b6cdb1f70b54c3a3a17b6714ee1f0e68bebb44a74b1efd512098

Ad closed by Google

Report this ad

Why this ad? ⓘ

Transactions

0e3e2357e806b6cdb1f70b54c3a3a17b6714ee1f0e68bebb44a74b1efd512098

(Size: 134 bytes) 2009-01-09 02:54:25

No Inputs (Newly Generated Coins)



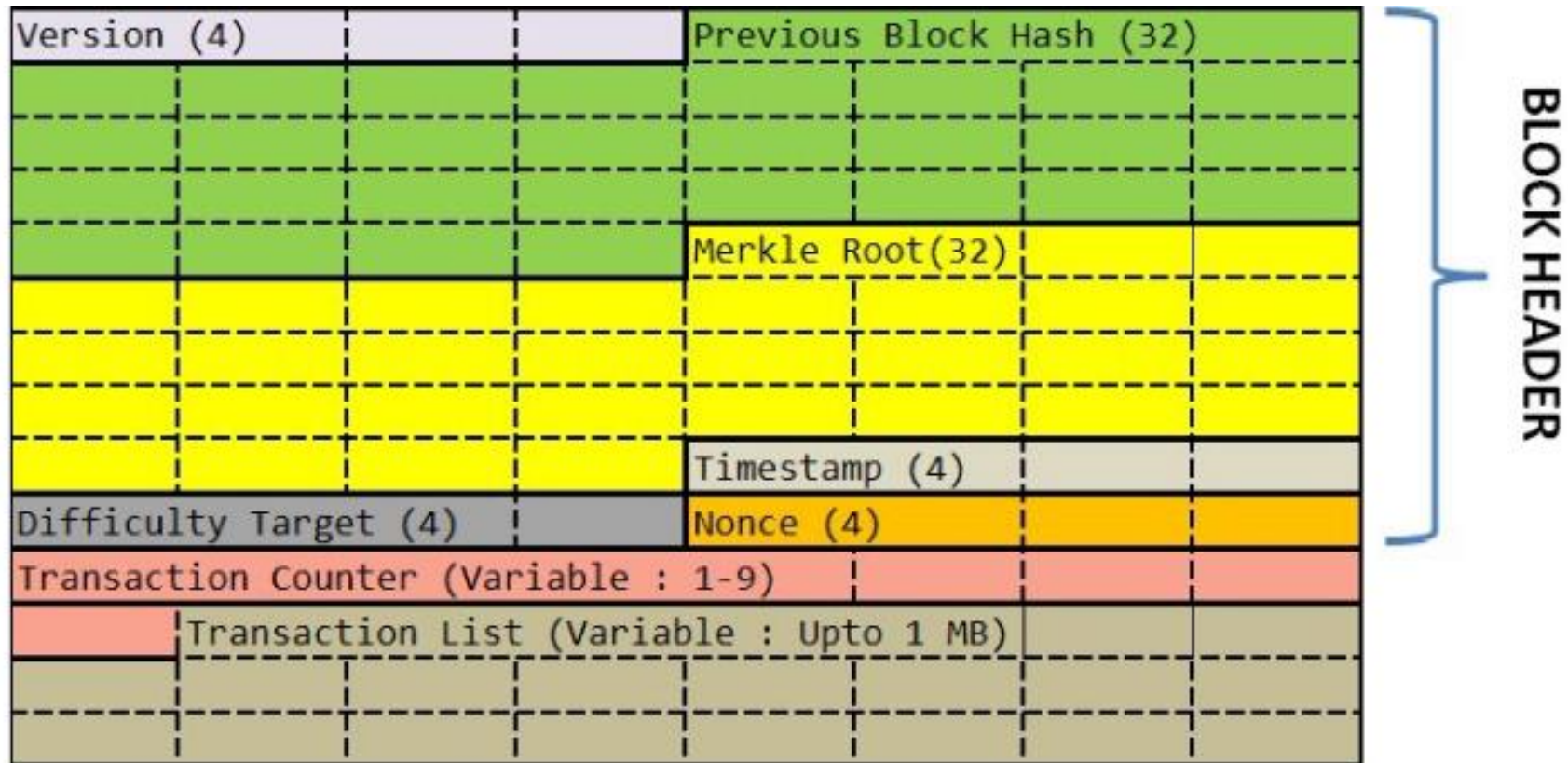
12c6DSiU4Rq3P4ZxziKxZrL5LmMBRzrJX - (Unspent)

50 BTC

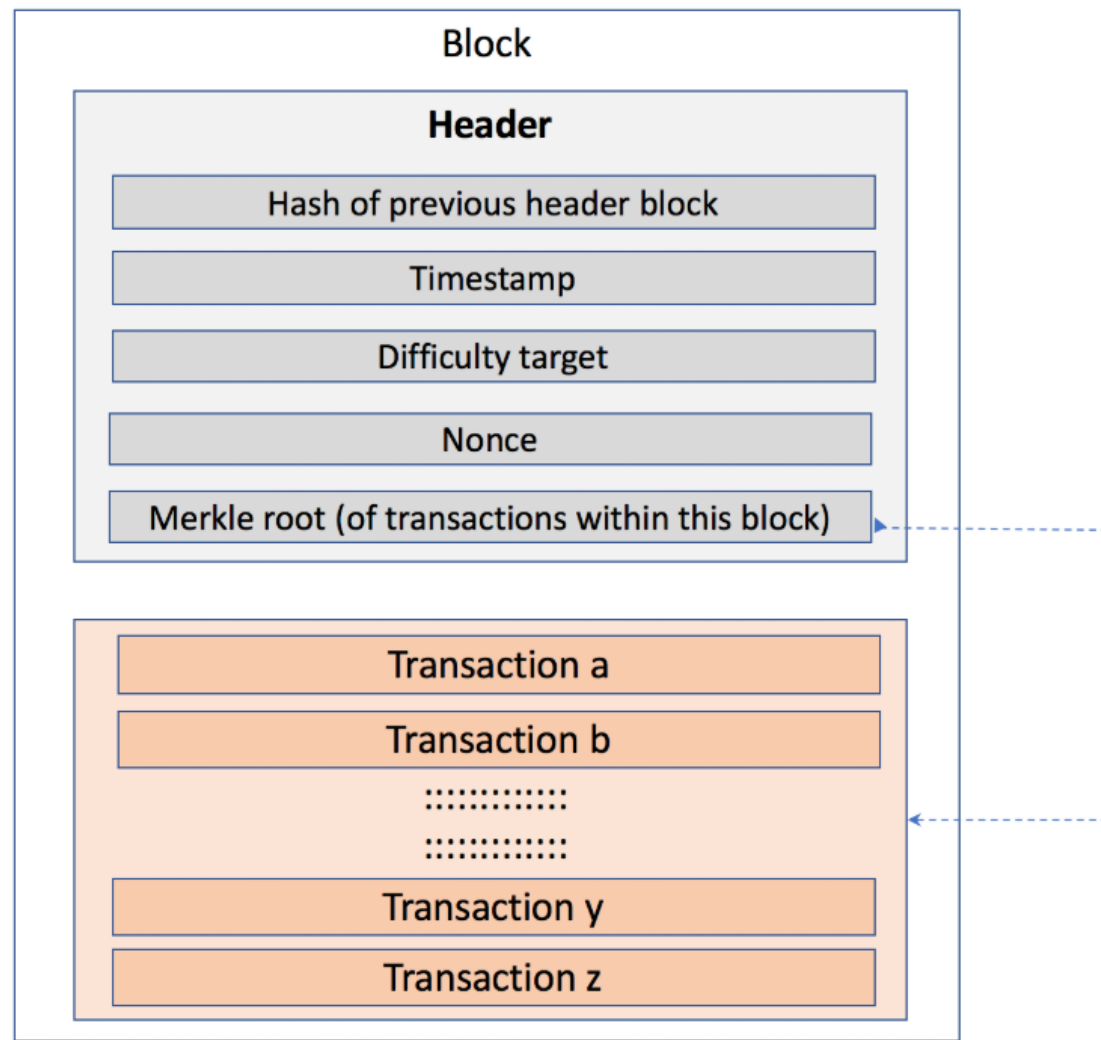
50 BTC

<https://www.blockchain.com>

Block Structure



Block Structure



<https://luxsci.com/blog/understanding-blockchains-and-bitcoin-technology.html>

Block Structure

❑ Magic number (4 bytes)

- ▣ 블록체인 네트워크에서의 식별자를 의미
- ▣ 상수 값은 `0xD9B4BeF9` (\Rightarrow Block의 시작부분을 의미함)

❑ Block size (4 bytes)

- ▣ 블록의 크기를 나타내며, 초반에는 36MB였으며, 2010년 DDoS 공격 및 중앙화 방지를 위해 1M로 축소시킴
- ▣ 현재는 최대 4MB까지 허용함

Block Structure

□ Version (4 bytes)

▣ 블록의 버전을 나타냄

- 블록체인 네트워크에서의 각 노드들은 동일한 버전으로 구현되어야함 (프로토콜 수행과 동일한 의사결정을 위함)

□ Previous block hash (32 bytes)

▣ 블록체인의 이전(마지막 추가) 블록의 헤더에 대한 Hash값을 의미

□ Merkle Root (32 bytes)

▣ 머클 트리의 루트 노드 값

- 머클 트리는 블록 바디에 있는 모든 트랜잭션과 위트니스 데이터로 만든 이진 트리를 의미

□ Timestamp

- 1970년 1월 1일 자정 (UTC/GMT)로부터 경과된 시간을 second 단위 기반으로 하는 Unix 'Epoch' 타임 스탬프로 인코딩된 4바이트의 데이터
 - Timestamp는 이전 11개 블록의 중간값보다 크고 Network-adjusted time + 2 시간보다 적은 값으로 구성
 - 여기에서, 'Network-adjusted time (네트워크 조정 시간)'이란 블록체인에 연결된 모든 노드가 반환한 타임 스탬프의 중앙값
 - 결과적으로, 블록의 Timestamp는 정확하지 않게 구성되며, 그 순서가 정확할 필요도 없음.

□ Difficulty Bits

- ▣ 예상 결과를 얻는 데 있어 현재의 난이도를 나타냄

□ Nonce

- ▣ 10분마다 개별적으로 생성되는 블록에 대한 카운터 값을 나타냄
 - 0과 같은 초기화된 숫자에서 시작하여 퍼즐이 풀리거나 다른 노드가 풀 때까지 1씩 추가하며 점진적으로 숫자가 증가함

Block Structure

- ❑ Transaction Counter (Variable: 1–9 bytes)
 - ▣ 블록에 포함된 거래(Transaction)의 수
- ❑ Transaction List (Variable: Total block size is 1 MB)
 - ▣ 해당 블록의 모든 거래에 대한 디지털 지문을 저장함

Block #442424

Block #442424

BLOCKCHAIN
Be Your Own Bank®



Create Your Wallet

Summary

Number Of Transactions	2601
Output Total	15,581.59608101 BTC
Estimated Transaction Volume	1,917.22805469 BTC
Transaction Fees	1.05181737 BTC

Height [442424 \(Main Chain\)](#)

Timestamp 2016-12-07 23:57:10

Received Time 2016-12-07 23:57:10

Relayed By [F2Pool](#)

Difficulty 286,765,766,820.55

Bits 402904457

Size 999.865 kB

Weight 3999.208 kWU

Version 0x20000000

Nonce 794862560

Block Reward 12.5 BTC

Hashes

Hash	000000000000000000004a8b7ad77058d1e17a843f69f305a647db7dbd198c31da
Previous Block	00000000000000000002335239496f9461a83554e4e2766d358083d2baa64f31e6
Next Block(s)	000000000000000000013bb15b8f7b8c58b87e7a89e88abea9378b1d6fe708cd7
Merkle Root	080bd756956661866121c1c2234fb48bce7036adcf2eb6cb48f160e0e90461e7

BLOCKCHAIN
Be Your Own Bank®



Create Your Wallet



- ## Transactions

15

Block #566750

BLOCKS

TRANSACTIONS

Height	Age	Transactions	Miner	Size (bytes)
566752	16 minutes	2703	BTC.com	1,178,167
566751	20 minutes	2516	ViaBTC	1,225,665
566750	38 minutes	2928	SlushPool	1,275,863
566749	54 minutes	180	SlushPool	73,794
566748	55 minutes	1049	BTC.com	502,614

<https://www.blockchain.com/en/explorer>

Block #566750

Block #566750

Summary	
Number Of Transactions	2928
Output Total	12,053.96485081 BTC
Estimated Transaction Volume	836.86208702 BTC
Transaction Fees	0.29046889 BTC
Height	566750 (Main Chain)
Timestamp	2019-03-12 12:29:51
Received Time	2019-03-12 12:29:51
Relayed By	SlushPool
Difficulty	6,068,891,541,676.55
Bits	388915479
Size	1275.863 kB
Weight	3993.035 kWU
Version	0x20000000
Nonce	1512968242
Block Reward	12.5 BTC

Hashes		18 digits
Hash	00000000000000000000000027d2d35b18d13e86217a8dfa4bdf10111917291cd5a675	
Previous Block	0000000000000000000000001cc636802c59782795014e2ee9df1d564740f94b3c537f	
Next Block(s)	000000000000000000000000132492532f3a2a8081ac764e149d842879a2c46eb78b0e	
Merkle Root	c7025ae27f88564f6a4d7a470fbcf67157313e6e9b0b685e6980d37b41c923d1	



- [illegible]



Raw-data of blocks

```
{ "hash": "000000000000000027d235b18d13e86217a8dfa4bdf10111917291cd5a675", "ver": 536870912, "prev_block": "00000000000000001cc636802c59782795014e2ee9df1d56470f94b3c537f", "next_block":  
["00000000000000000000132492532f3a2a8081ac764e149d842879a2c46eb78b0e"], "mrkl_root": "c7025ae27188564f6a4d7a470fbcf67157313e6e9b0b685e6980d37b41c923d1", "time": 1552393791, "bits": 388915479, "fee": 29046889, "nonce": 1512966  
242, "n_tx": 2928, "size": 1275863, "block_index": 1754169, "main_chain": true, "height": 566750, "tx":  
[{"hash": "393f4a82722db297a6059f3bfdafeb829c950be07db2477022665b1063b68836f", "ver": 1, "vin_sz": 1, "vout_sz": 3, "size": 290, "weight": 1052, "fee": 3720953111, "relayed_by": "0.0.0.0", "lock_time": 0, "tx_index": 424404611, "double_spend": false, "time": 1552393791, "block_index": 1754169, "block_height": 566750, "inputs":  
[{"sequence": 0, "witness": "012000000000000000000000000000000000000000000000000000000000000000", "script": "03dea508fabed6d96d35260c35357e782a1b55478d5538f3c5a9d73621a1db441ab1f151d0c671c01000000000000021650c00014c9a001122d671920d2f736c7573682f"}], "out":  
[{"type": 0, "spent": false, "value": 1279046889, "script": "76a9147c154ed1dc59609e3d26abb2df2ea3d587cd8c4188ac", "tx_index": 424404611, "n": 0, "addr": "1CK6KH6MHgYvmRQ4PAafKYDrg1ejbH1cE"},  
{"type": 0, "spent": false, "value": 0, "script": "6a4c2952534b424c4f434b3a84cce2eb0235817baa51866114827cc92d894d06c2ab0ab5711cf61ab4c28289", "tx_index": 424404611, "n": 1},  
{"type": 0, "spent": false, "value": 0, "script": "6a24aa21a9ed645ad67d7165ac57de0485160997d4cb72b95e8d09e90a9aa7809ec96809bb8", "tx_index": 424404611, "n": 2}], "rbf": true},  
{"hash": "2b233fc95f85a515cc330151d87611566e55b3786eace5c5ab1a6905fb36b640", "ver": 2, "vin_sz": 1, "vout_sz": 2, "size": 404, "weight": 854, "fee": 96300, "relayed_by": "0.0.0.0", "lock_time": 0, "tx_index": 424401998, "double_spend": false, "time": 1552393147, "block_index": 1754169, "block_height": 566750, "inputs":  
[{"sequence": 4294967294, "witness": "040047304402203744da5905d2e247f05db12e23285f2ad565bc038fbba093ef71f8be64a676402207cf01c269586f5147fde6f9d11270719616bef341b8373bbebeeeaa5e69b407120147304402207ebe490058346ef4e004a27f7f97dce3416d7a02cdf9ae396f87622a93d886ce0220633739f067d2302aa9a5e4f0c728afb8fd4207877047fe98b322e4c7efc7a46801695221027111c0d6cbc3a40c6e6197ed234bd6e59f277c88094fd33297b1e0a3787a5b7d102e71711c9840d68e6401d4bc5df78f1850e25ae41f082f4b38ceec37d60cab5442103eeae18900c0d12046f644b960a1ef84589f7f4f71d07914006d550bf85c576e153ae", "script": "220020fa28dc1e5eb222055e90f8cade9bcd13ca9ddab7a5ed029e27d41a736f7455ce", "prev_out":  
{"type": 0, "spent": true, "value": 220018151, "spending_outpoints":  
[{"tx_index": 424401998, "n": 0}], "script": "a91402a751dc8c10e35fed2c6eddc2575c9af2c71d2387", "tx_index": 424400094, "n": 0, "addr": "31w3iWUN5EMJMW2YRCc5m4RFqm3zN61xK2"}], "out":  
[{"type": 0, "spent": true, "value": 96424695, "spending_outpoints":  
[{"tx_index": 424407447, "n": 0}], "script": "a9143fc3c36c2642de20342c21913cf7f9f2df9927b987", "tx_index": 424401998, "n": 0, "addr": "37WB1Wko8fkCH7T2yswNzYn5Gcb9hGssf4"},  
{"type": 0, "spent": true, "value": 123497156, "spending_outpoints":  
[{"tx_index": 424404491, "n": 6}], "script": "a91402a751dc8c10e35fed2c6eddc2575c9af2c71d2387", "tx_index": 424401998, "n": 1, "addr": "31w3iWUN5EMJMW2YRCc5m4RFqm3zN61xK2"}],  
{"hash": "a456ceab764087255e579f4663af485df5c204b43ab525299884b5b008e24186", "ver": 2, "vin_sz": 1, "vout_sz": 3, "size": 258, "weight": 1032, "fee": 100000, "relayed_by": "0.0.0.0", "lock_time": 0, "tx_index": 424402420, "double_spend": false, "time": 1552393245, "block_index": 1754169, "block_height": 566750, "inputs":  
[{"sequence": 4294967295, "witness": "", "script": "483045022100c9a4e5c74bde950fc34048c4bc739c930d924915cfd3b2c54f992aadbbc99202202e6027471f04521fd8b0ee7acd328da1f5bcf9ebcd3446882f60131a4fb641b9012102cfd0c98eb906bfdc6ea92c0269875097a0c0a4d4bf582735c2daeb3eb501227", "prev_out": {"type": 0, "spent": true, "value": 3075001044, "spending_outpoints":
```

CONTENTS

- ❑ Bitcoin's transaction

Bitcoin's transaction

- 유효한 거래를 위한 요구 조건
 - ▣ 소유권 증명 (서명)
 - ▣ 사용 가능한 자금
 - ▣ 동일 자금을 사용하는 또 다른 거래가 없음
- 비트코인은 UTXO (Unspent Transaction Output) 모델을 사용하여 자금이 한번만 사용 되도록 수행

Unspent Transaction Output (UTXO)

□ UTXO model

- ▣ 비트코인은 해시 트리를 구성한 후 해시 루트를 블록의 해시값 계산에 사용함
 - 블록의 해시값을 블록에 저장해 이전 블록의 거래와 현재 블록의 거래 내역이 있음을 보장함
 - 단, 블록에 저장한 거래 데이터는 누구나 자유롭게 볼 수 있기 때문에, 자신이 소유한 암호화폐를 다른 사람이 사용할 수 없는 구조가 필요함
 - => UTXO (Unspent Transaction Output)

Unspent Transaction Output (UTXO)

□ UTXO model

계정 기반 잔액 저장 방식

Account	BTC
Alice	100
Bob	200



Alice -> Bob
50 BTC

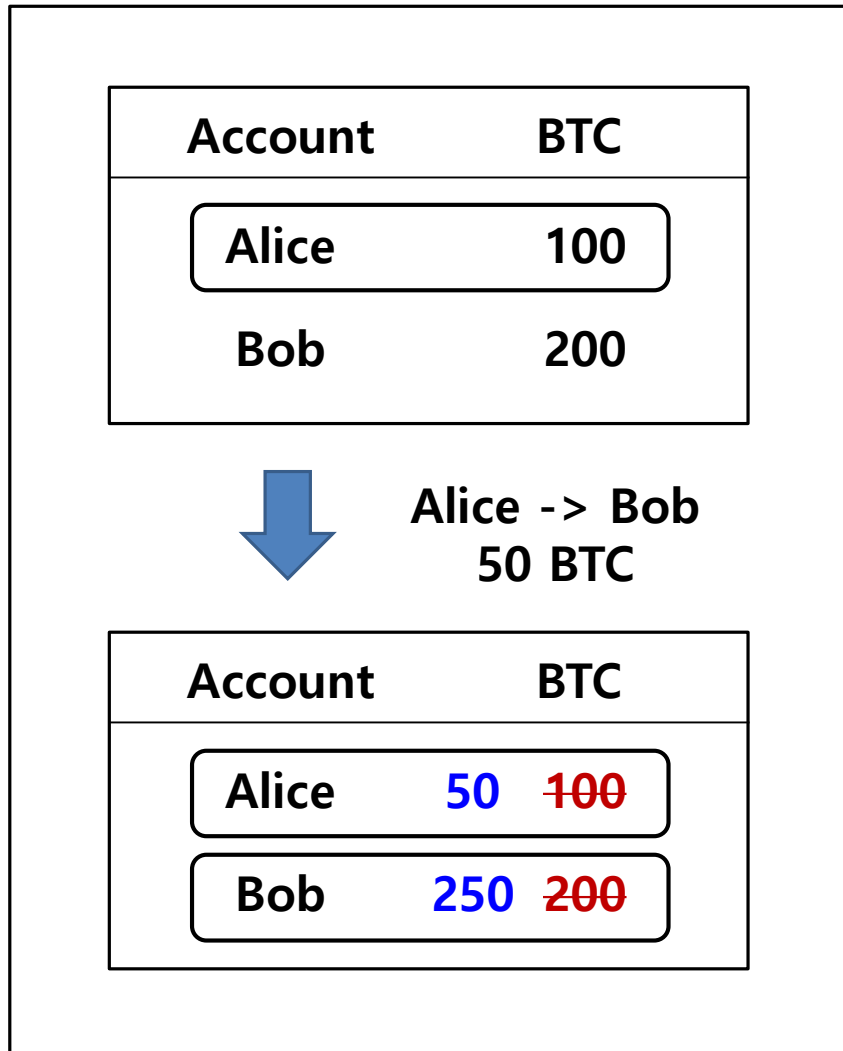
Account	BTC	
Alice	50	100
Bob	250	200

※ 정상적인 송금을 하기 위해
필요한 기능은??

Unspent Transaction Output (UTXO)

□ UTXO model

계정 기반 잔액 저장 방식

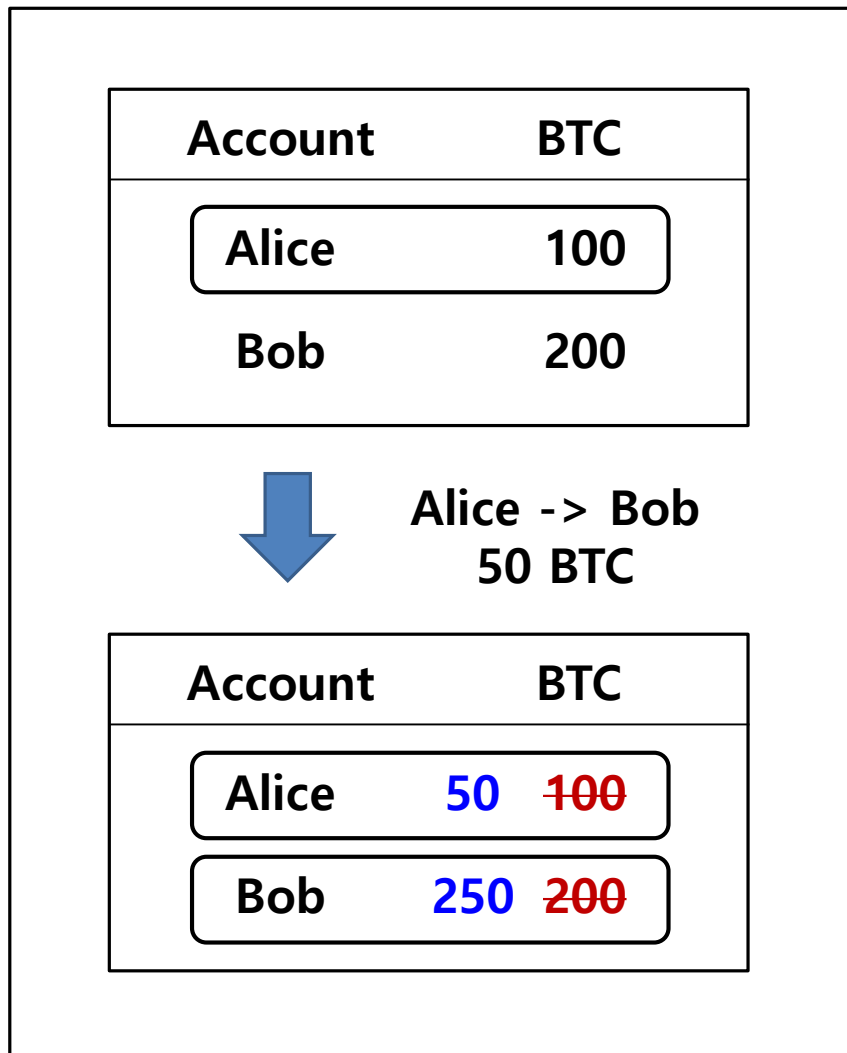


※ 정상적인 송금을 하기 위해
필요한 기능은??

Unspent Transaction Output (UTXO)

□ UTXO model

계정 기반 잔액 저장 방식

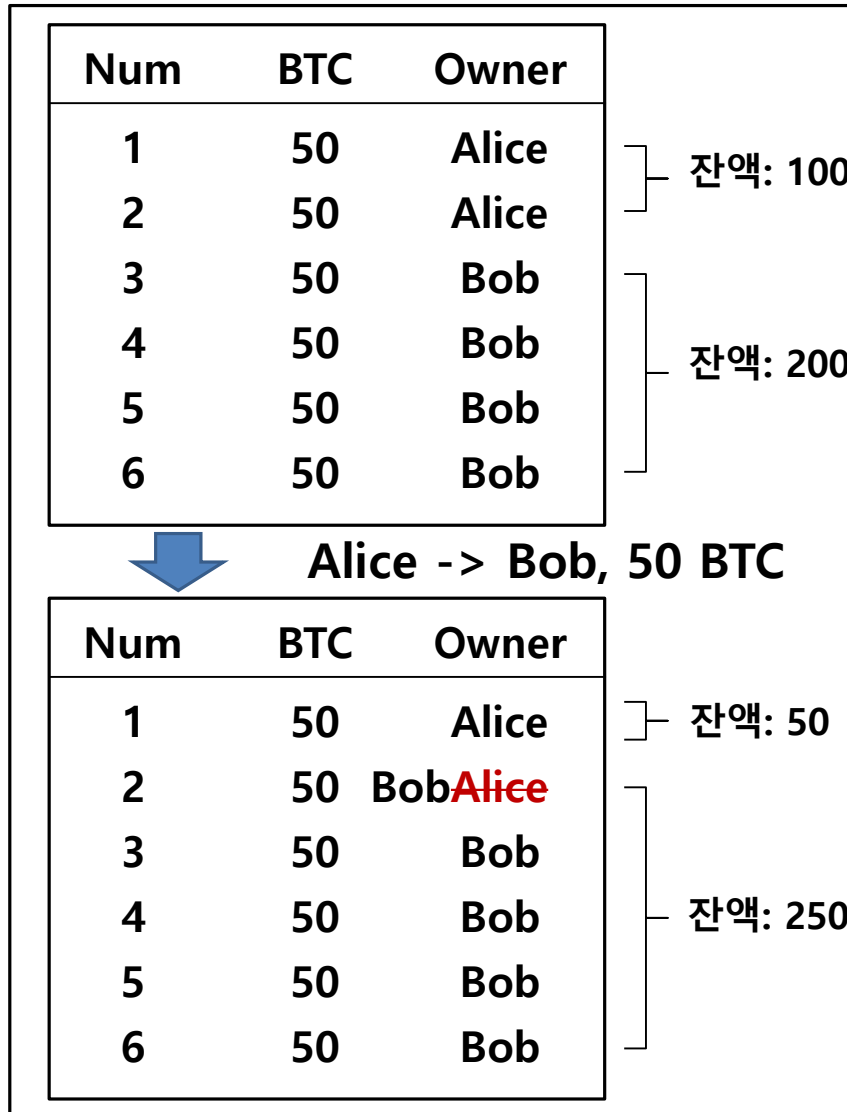


- ※ 만약 송금 시스템에 장애가 발생
 - 계좌의 잔액을 업데이트 하지 못했을 경우
 - 모든 거래를 원래 상태로 복원해야함

Unspent Transaction Output (UTXO)

□ UTXO model

거래 기반 방식



※ 만약 송금 시스템에 장애가 발생
- 송금 과정에서 장애가 발생해도
화폐 번호 2의 소유권이
Alice에게 있다면 50BTC가 사라질
일은 없음

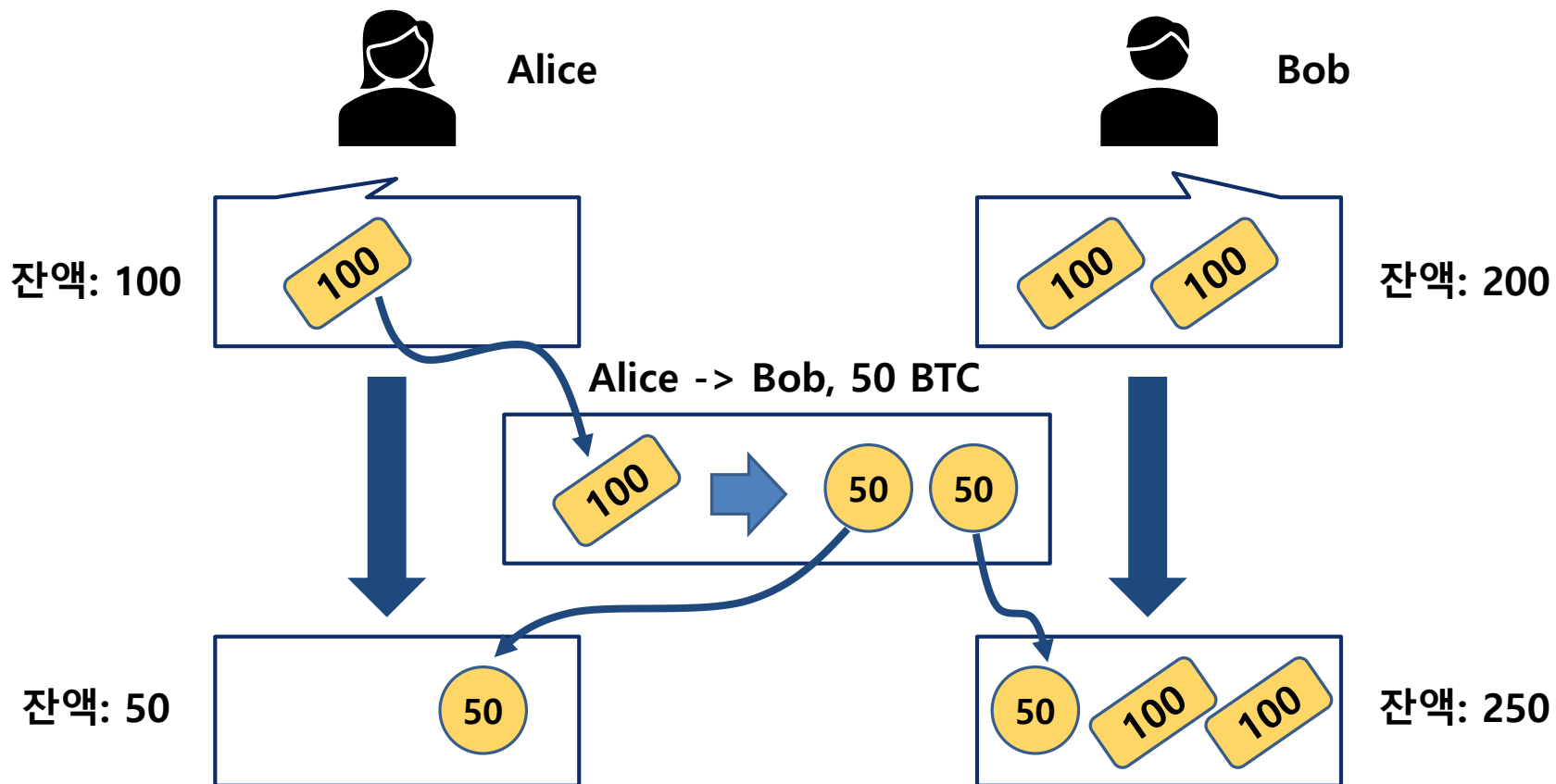
- 하지만, 화폐의 총 잔액을 계산해
일정한 단위로 나눠야 함

Unspent Transaction Output (UTXO)

□ UTXO model

▣ 거래 기반 방식

- 더 큰 돈을 주고 거스름돈을 받는 송금 구조

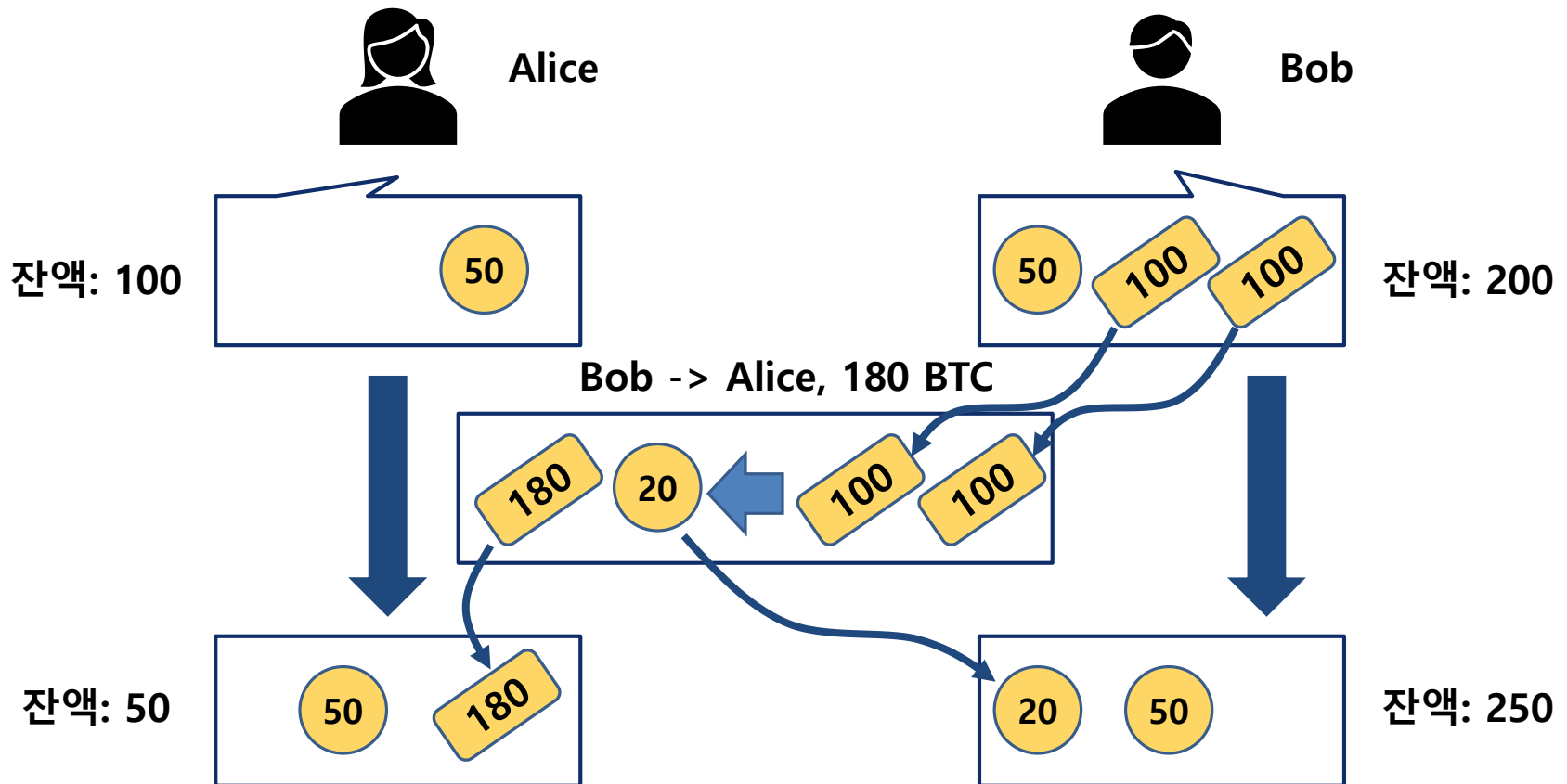


→ Unspent Transaction Output (UTXO)

□ UTXO model

▣ 거래 기반 방식

- 특정 금액을 바꾸고 거스름돈을 받는 송금 구조



Unspent Transaction Output (UTXO)

□ An example

Summary	
Address	31w3iWUN5EMJMW2YRCc5m4RFqm3zN61xK2
Hash 160	02a751dc8c10e35fed2c6eddc2575c9af2c71d23
Transactions	
No. Transactions	86231
Total Received	135,718.44808101 BTC
Final Balance	3,424.64301851 BTC



d3987a8c45ad017bcec697f70847ba61a455c9de37b7337cd54e2395adee5a45

(Fee: 0.001284 BTC - 150.35 sat/WU - 317.82 sat/B - Size: 404 bytes) 2018-12-18 18:33:09

31w3iWUN5EMJMW2YRCc5m4RFqm3zN61xK2 (0.54822336 BTC - Output)

→ 33tDmEs4QRV53RWTuxsWQKbdLVK816p7VB - (Spent) 0.1236083 BTC
31w3iWUN5EMJMW2YRCc5m4RFqm3zN61xK2 - (Spent) 0.42333106 BTC

-0.1248923 BTC

f63c0095fdabd4415ca3c1a72d9c60c72a9a66c3d37dab325617b9c9e037f01b

(Fee: 0.002433 BTC - 37.58 sat/WU - 81.4 sat/B - Size: 2989 bytes) 2018-12-18 18:30:14

3NM59NUtwHLgVmdWojCqHWCpXkTo4eyXtU (0.12090517 BTC - Output)
35aqCYDEJarhDpRuQAA5AbCweJtz9SGEo (0.00635014 BTC - Output)
3HWv7vhA4na4Anu2uEMMQvgeJCEcFkv1FN (0.85963011 BTC - Output)
3HcaRtYFNtbo9eVixn9n6fCcsFrVsxkev (0.11 BTC - Output)
3Lu1CH7TiA9Xkg4wiGgeuQipuCBAX2J8P (12.4 BTC - Output)
3BxF6Ef9bvRQsj4rsDkMeB7krV9kdqH3w1 (0.20538018 BTC - Output)
34XoEXEcwF4uTr18WqXfc75EeKKUfs3ymi (11.909 BTC - Output)
3DdDwAjymfreQ2DT929DDpz3UTIPGnKZnD (0.151 BTC - Output)
3EgWkdV9txwDQn2YkogzUQJhgTzeHyrpWK (0.0544 BTC - Output)
36toh9hKciGcEMKy1mf2PhprC9WemoRMUQ (0.31096418 BTC - Output)
36oFCzjp2x6bqibBj4PwKKkmnz3gqc6UFZ (10 BTC - Output)
3AyLabKSPM9ya1CHSnqUWCW3e5hAHii4B2 (3.16050068 BTC - Output)
39MFgm57QmeNcpjYcAALzhs8ASi1fyGkPJ (8.395115 BTC - Output)
3KXmWpvpbeobe3z6RmANrgps8KFvkdudsDF (1.013585 BTC - Output)
32d6GvpzmoxJYyJdG8wn1XEJAFWQMUSqtU (0.10686856 BTC - Output)
3DdDwAjymfreQ2DT929DDpz3UTIPGnKZnD (0.179 BTC - Output)
3ErjdsXNzEznGXKcpcB7JnRKYNFnixCUJ (0.0273145 BTC - Output)

→ 34oGHhrLct6fnhuBRbqRVemaeNY7Fzhsf - (Spent) 0.00758052 BTC
31w3iWUN5EMJMW2YRCc5m4RFqm3zN61xK2 - (Spent) 49 BTC

<https://www.blockchain.com/en/btc/address/31w3iWUN5EMJMW2YRCc5m4RFqm3zN61xK2?offset=85700&filter=6>

Unspent Transaction Output (UTXO)

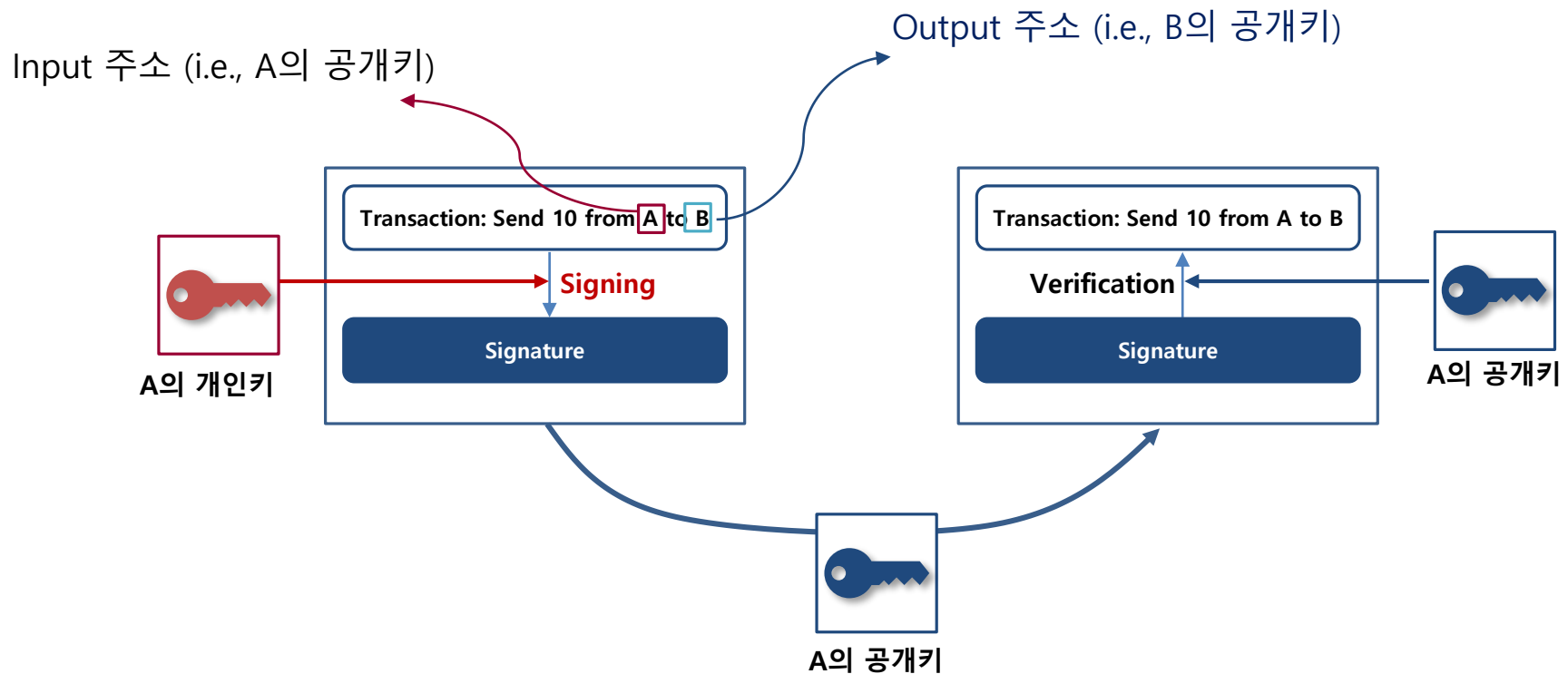
□ UTXO model

▣ UTXO의 특징

- 다른 사용자에게 일정량의 암호화폐를 받을 때 생성됨
- 받은 금액 그대로를 UTXO로 저장
 - 예를 들면, A, B, C에게 각각 1BTC, 2BTC, 3BTC를 받아 총 6BTC를 소유했다고 가정
 - 자신의 지갑에는 6BTC가 한꺼번에 묶인 것이 아니라, 1, 2, 3BTC를 각각 UTXO로 저장함
- UTXO에서 일부 금액을 송금할 경우, 새로운 UTXO를 생성하고 기존 UTXO는 파기함
 - 예를 들면, 3BTC가 있는 UTXO에서 2BTC를 다른 사람에게 송금하면, 2BTC가 있는 UTXO와 1BTC가 있는 UTXO를 생성함
 - 그 후, 3BTC가 있는 UTXO를 파기함

Unspent Transaction Output (UTXO)

□ Transaction 검증





Transaction 데이터 구조

Version	Input Count	Previous Output	Output Index	Script Length	Scriptsig	Sequence	Output Count	Value	Script Length	script PubKey	Lock Time
---------	-------------	-----------------	--------------	---------------	-----------	----------	--------------	-------	---------------	---------------	-----------

입력부 (vin)
출력부 (vout)

- Version: 현재 transaction 버전
- Input Count: 입력부 개수
- Previous Output: 이전 출력부의 Transaction ID
- Output Index: 이전 출력부들 중 잔액을 사용할 출력부 번호
- Script Length: 스크립트 길이
- Script sig: Signature 스크립트 (해제 스크립트), 전자서명
- Sequence: 시퀀스 번호
- Output Count: 출력부 개수
- Value: 송금 금액
- Script Length: 스크립트 길이
- ScriptPubKey: Locking 스크립트 (잠금 스크립트), 수신자의 공개키 해시값
- LockTime: 채굴자가 해당 트랜잭션을 언제 선택할 수 있는지 표시

Unspent Transaction Output (UTXO)

□ UTXO model

▣ 공개키 암호와 UTXO

- 공개 키 (Public key) -> 암호화폐의 접근 권한을 잠금
- 개인 키 or 비밀 키 (Private key) -> 암호화폐 이용 권한을 얻음
- 이때, **비트코인 스크립트**로 이용 권한의 잠금과 해제 등을 구현함 (P2PKH)



잠금 스크립트 (scriptPubKey)

출력 값을 소비하기 위해
충족되어야 하는 요건을
스크립트로 작성한 것
(수신자의 공개키,
비트코인 주소를 포함함)



해제 스크립트 (Scriptsig)

잠금 스크립트가 출력 값에 걸어 둔
조건을 해결해 출력 값이 소비될 수
있도록 하는 스크립트
(송신자의 전자서명과
공개키가 들어있음)

Unspent Transaction Output (UTXO)

□ UTXO model

▣ Pay-to-PubKey-Hash (P2PKH)

- 비트코인 내에서 가장 일반적인 스크립트 (script) 형식으로 비트코인 프로토콜에 대한 지불 거래 유형
 - 발신인이 (개인키에서) 유효한 서명 및 공개키 제공을 요구하는 경우, 트랜잭션 출력 스크립트는 서명 및 공개키를 사용하여 일부 암호 기능을 통해 공개키 해시와 일치하는지 여부를 확인

Unspent Transaction Output (UTXO)

□ UTXO model

▣ 비트코인에서의 거래

– Pay-to-PubKey-Hash (P2PKH)

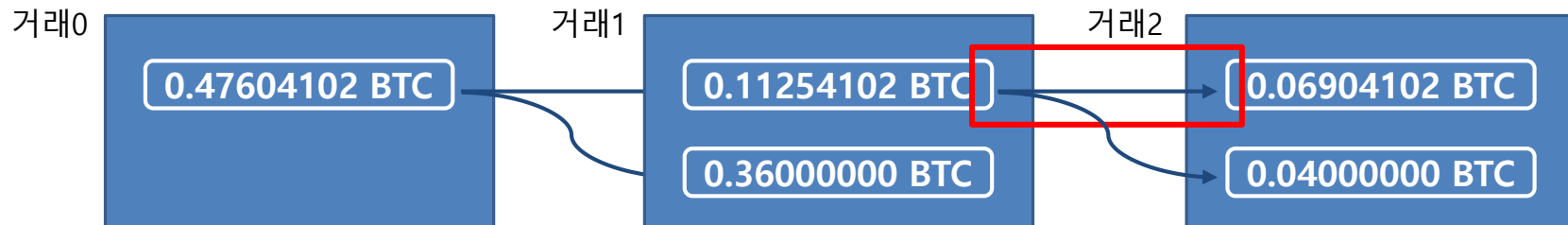
- 거래 1에서 전송 받은 비트코인을 거래 2에서 사용함
- 이런 경우, P2PKH의 사용 방식

거래1

txid: 4c96d74c3087788c7f1f759d5e2c1b44455546ef17acee5a2b05595e36c068e1

거래2

txid: 7dd123bbdad0af3612cb4440929f491a54716f0f400740c52b7b6226bd1fbecb



Unspent Transaction Output (UTXO)

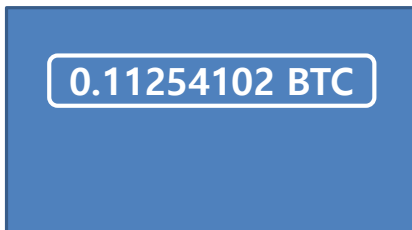
□ UTXO model

▣ 비트코인에서의 거래

– Pay-to-PubKey-Hash (P2PKH)

- 거래 1에서 전송받은 비트코인을 거래 2에서 사용함
- 이럴 때, P2PKH의 사용 방식

거래1

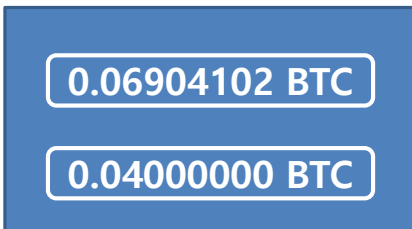


Outputs ⓘ

Index	0	Details	Spent
Address	1CmwT6awtLgspGeNCqBD3VgCa4joZebuke	Value	0.11254102 BTC
Pkscript	OP_DUP OP_HASH160 81297f8e75537c95dec04471d4c7327e335d03c1 <u>OP_EQUALVERIFY</u> OP_CHECKSIG		

RIPEMD160 (SHA256 (PubKey))

거래2



Inputs ⓘ

Index	0	Details	Output
Address	1CmwT6awtLgspGeNCqBD3VgCa4joZebuke	Value	0.11254102 BTC
Pkscript	OP_DUP OP_HASH160 81297f8e75537c95dec04471d4c7327e335d03c1 OP_EQUALVERIFY OP_CHECKSIG		
Sigscript	<div>3044022004a86a37cc25d58e6cf26b4e955e87f61ddd85916a638a7ecea4d100f7d394a0220748a5ca0b0656643254c226da0a9193ccaa106e72fff27a719a764ea2a35db5701</div> <div>034a7345544bc0e79d65a53494a563054455b510b856b6585265ec5a529dfa51b2</div>		
Witness	Sig		

PubKey

➔ Unspent Transaction Output (UTXO)

□ UTXO model

▣ 비트코인에서의 거래

– Pay-to-PubKey-Hash (P2PKH)

■ 거래 1에서 전송받은 비트코인을 거래 2에서 사용함

■ 이럴 때, P2PKH의 사용 방식

■ 해제 스크립트는 거래 2의 input, 잠금 스크립트는 거래 1의 output

복합 스크립트

<sig>	<PubKey>	DUP	<HASH160>	<PubKeyHash>	<EQUAL VERIFY>	<CHECKSIG>
-------	----------	-----	-----------	--------------	----------------	------------

해제 스크립트 (Scriptsig)

잠금 스크립트 (scriptPubKey)

거래1



거래2



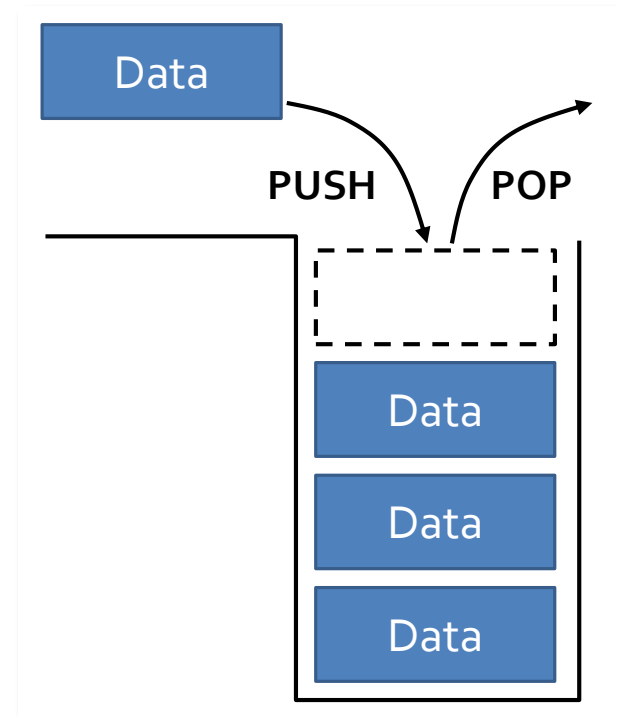
Unspent Transaction Output (UTXO)

□ UTXO model

▣ 비트코인에서의 거래

- P2PKH에서 복합스크립트 작동 방식

- 스택 (Stack) 데이터 구조를 적용
- Push와 Pop을 연산과정으로 사용
 - Push는 데이터 최상단에 데이터를 추가하는 연산
 - Pop은 최상단에서 데이터를 제거하는 연산
 - Pop 연산에서 "+, -, ×, ÷" 연산을 수행

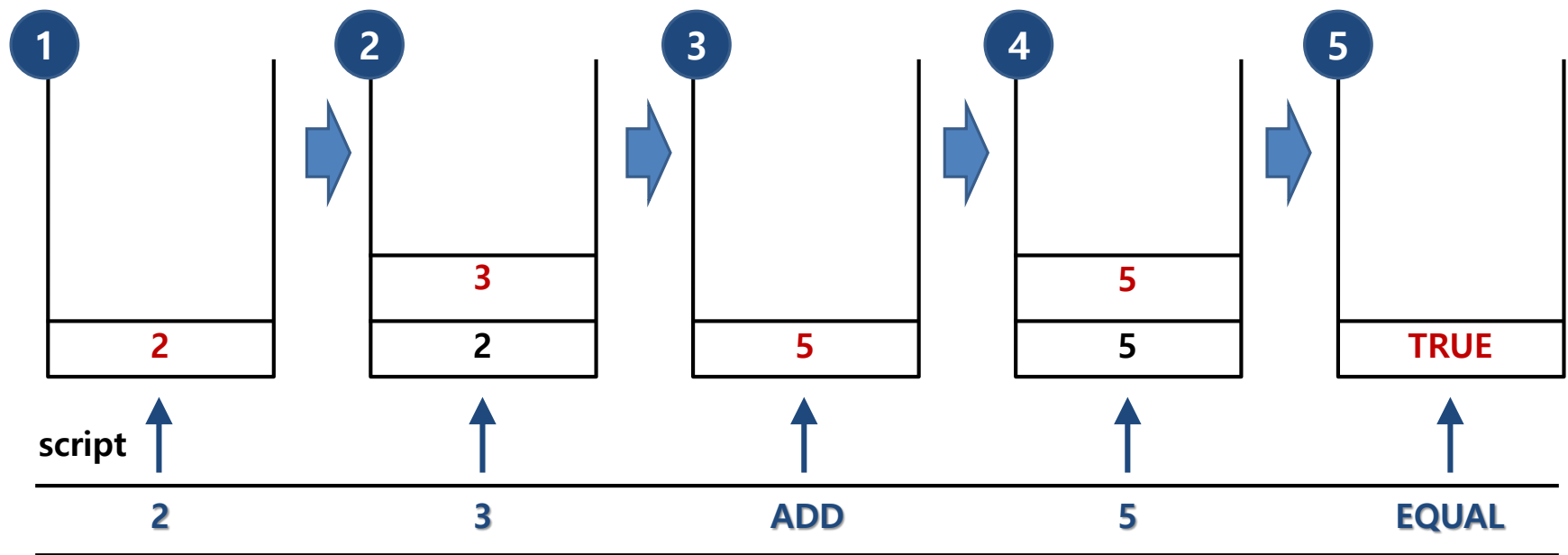


Unspent Transaction Output (UTXO)

□ UTXO model

▣ 공개키 암호와 UTXO

- 비트코인 스크립트 언어 작동 방식



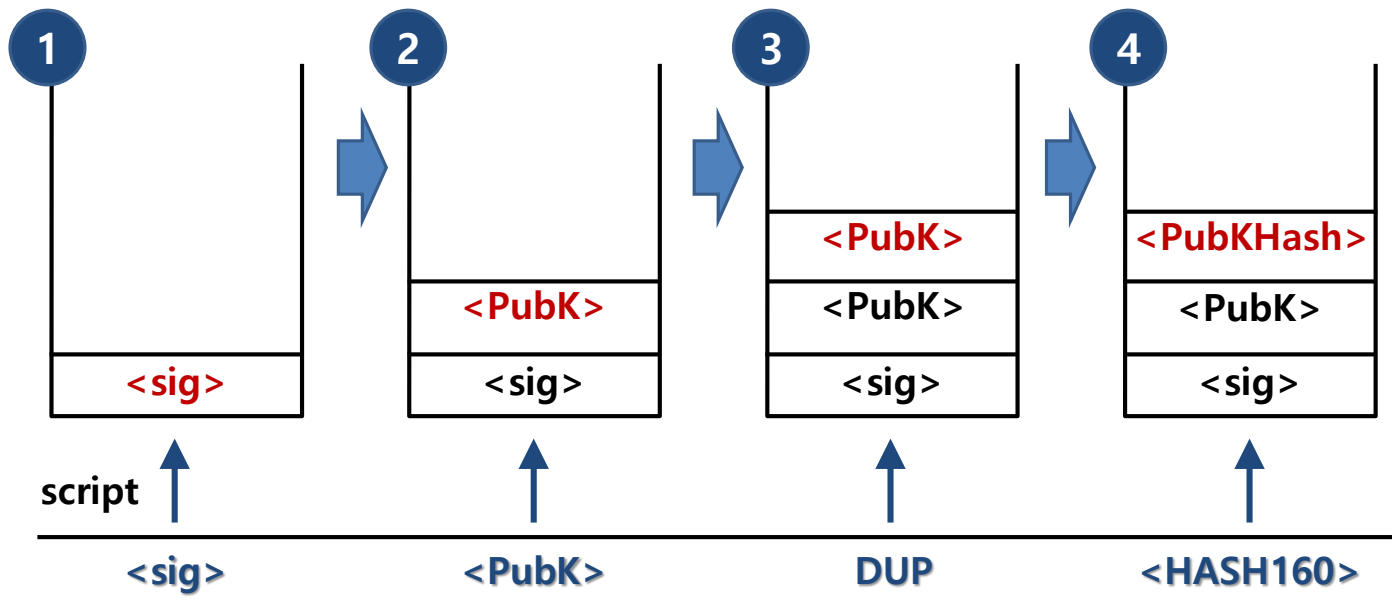
Unspent Transaction Output (UTXO)

□ UTXO model

▣ 공개키 암호와 UTXO

- 비트코인 스크립트 언어 작동 방식

■ P2PKH (Pay-to-Public-Key-Hash): '공개키 해시'에 지불하는 방식



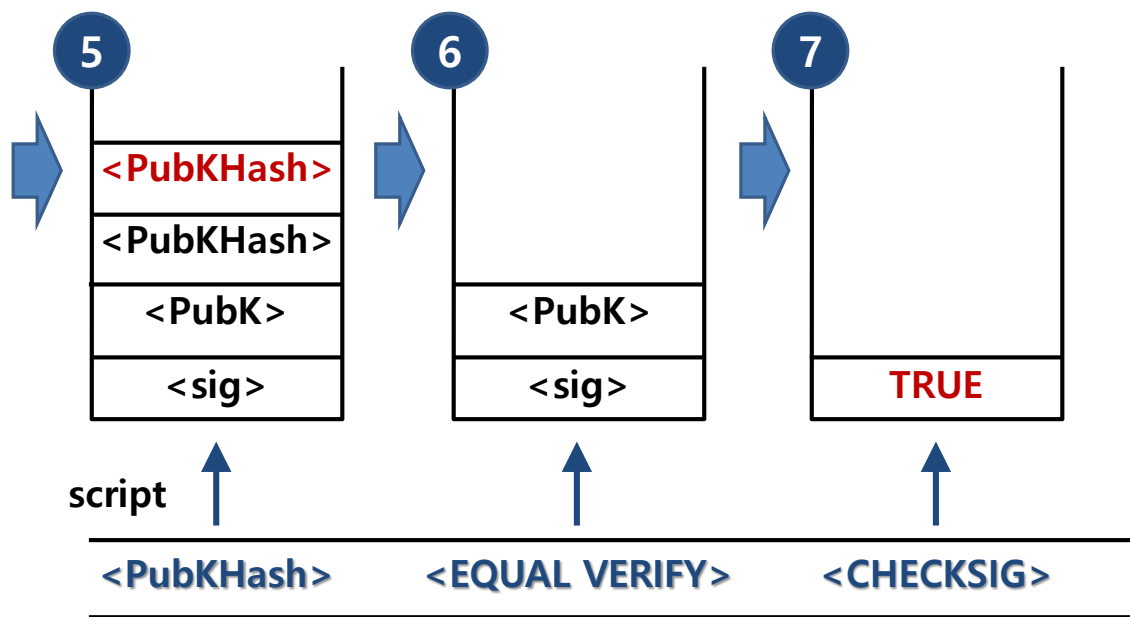
Unspent Transaction Output (UTXO)

□ UTXO model

▣ 공개키 암호와 UTXO

- 비트코인 스크립트 언어 작동 방식

■ P2PKH (Pay-to-Public-Key-Hash): '공개키 해시'에 지불하는 방식

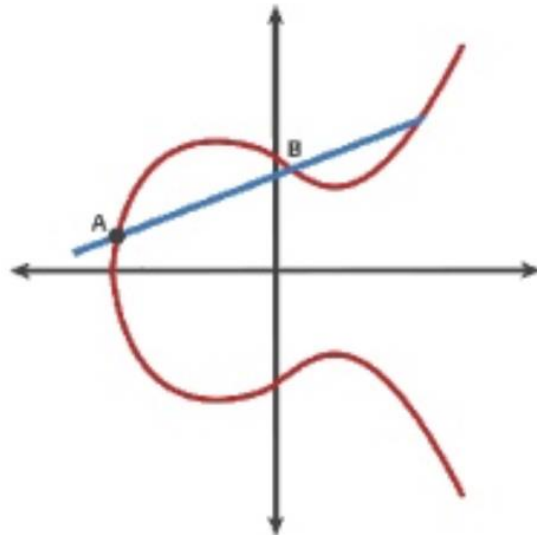


CONTENTS

☐ Public address

ECDSA

Elliptic Curve Digital Signature Algorithm



Public address

18E14A7B6A307F426A94F8
114701E7C8E774E7F9A47E
2C2035DB29A206321725



256 bits

개인키 생성

0450863AD64A87AE8A2FE83C1AF1A8403C
B53F53E486D8511DAD8A04887E5B23522C
D470243453A299FA9E77237716103ABC11
A1DF38855ED6F2EE187E9C582BA6



520 bits

공개키 생성

16UwLL9Risc3QfPqBUvKof
HmBQ7wMtjvM

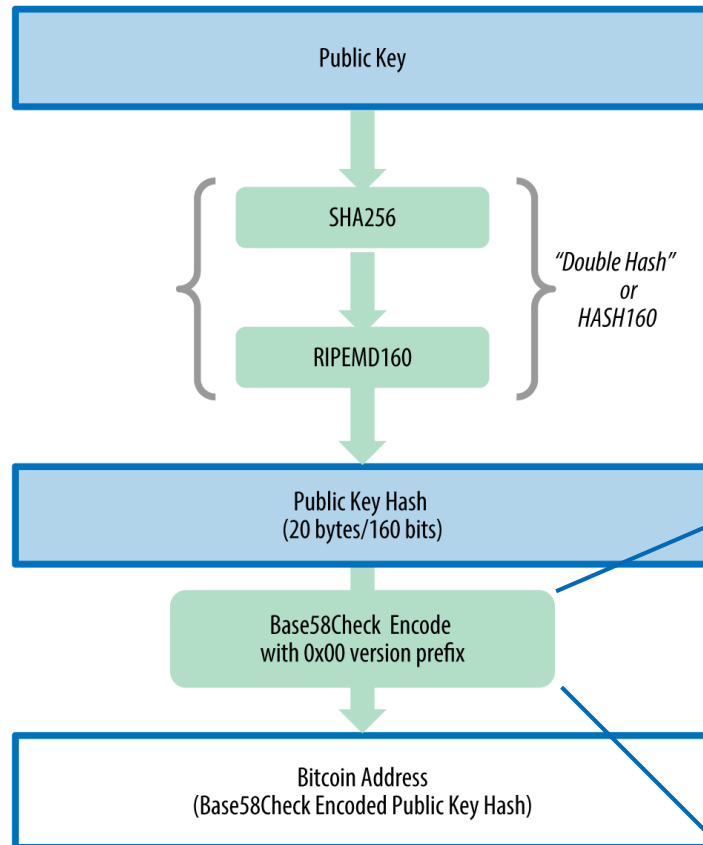


160 bits

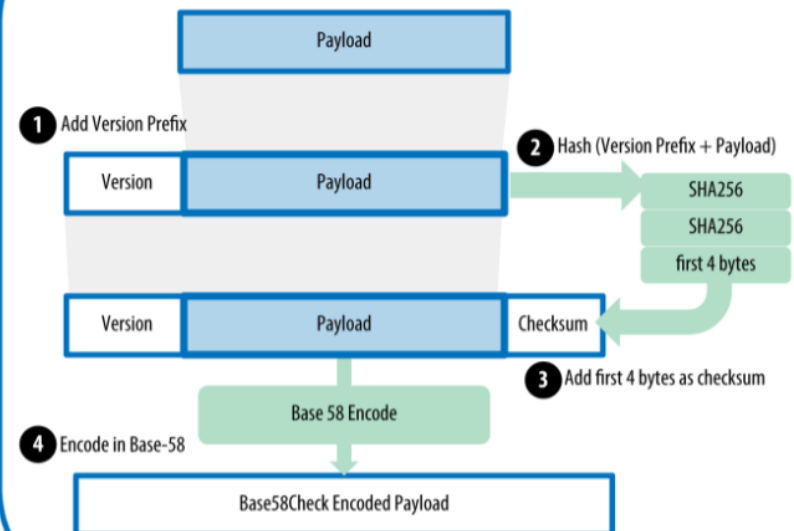
비트코인 주소 생성

Public address

Public Key to Bitcoin Address



Base58Check Encoding



Transaction View information about a bitcoin transaction

13217f0b0c63d3d364a5be4f3e5bd61d885d35d7b02c839706f67878f7b589f9

1KKKK6N21XKo48zWKuQKXdvSsCf95ibHFa

Output)

0.0001 BTC -



1LLLfmFp8yQ3fsDn7zKVBHMmnMVvbYaAE6

(Spent)

0.0001 BTC

0.0001 BTC

Summary

Size 223 (bytes)

Weight 892

Received Time 2014-01-21 08:30:33

Included In Blocks [282135](#) (2014-01-24 01:14:19 + 3,884 minutes)

Confirmations 284646

Visualize [View Tree Chart](#)

Inputs and Outputs

Total Input 0.0001 BTC

Total Output 0.0001 BTC

Fees 0 BTC

Fee per byte 0 sat/B

Fee per weight unit 0 sat/WU

Estimated BTC Transacted 0.0001 BTC

Scripts [Hide scripts & coinbase](#)

CONTENTS

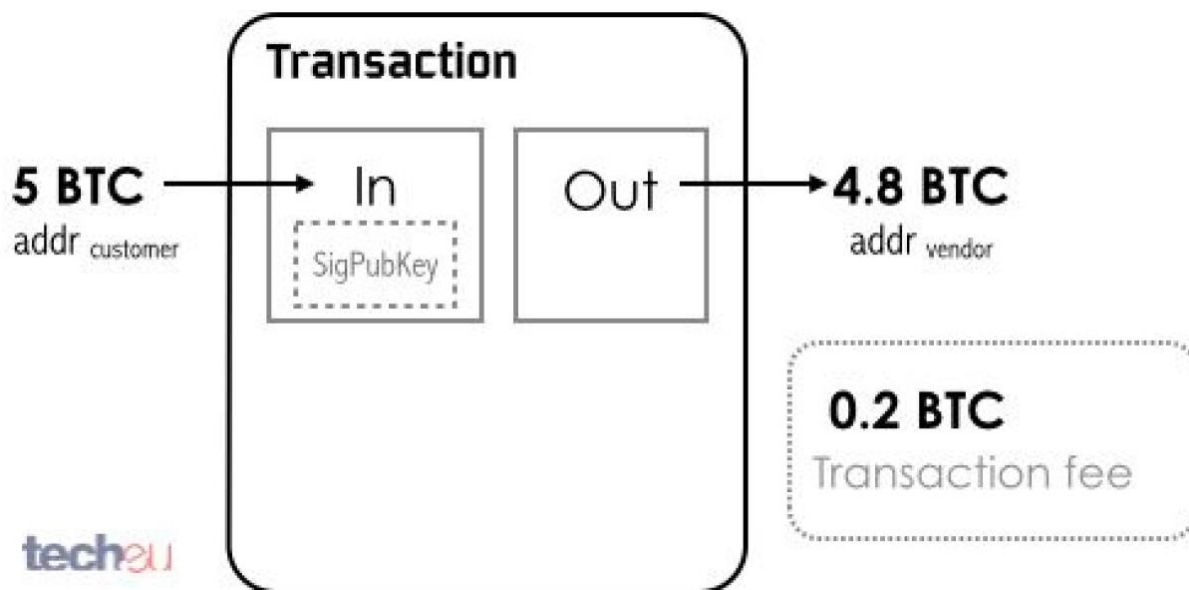
- ❑ Real-mining and confirmation of bitcoin

Mining incentive

- Bitcoin node가 Proof-of-Work (PoW)를 하는 이유
 - ▣ PoW 채굴 과정을 통한 incentive를 배분함
 - 블록 생성하게 될 경우, 이에 대한 보상으로 Bitcoin을 보상함
 - ▣ PoW 채굴 과정에서 주어지는 incentive?
 - 2020년 5월, 3번째 반감기
 - 채굴 보상 현재 6.25BTC
 - ▣ 또한, 거래에 대한 거래 수수료를 받게 됨
 - ▣ 즉, 채굴 수익 = 블록생성 보상 + 거래 수수료

Mining incentive

□ 거래 수수료



➔ Mining incentive

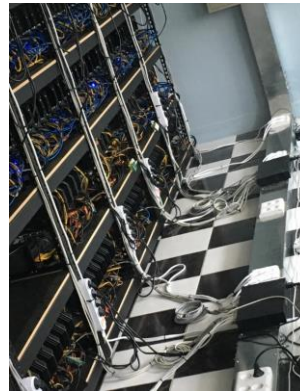
□ 채굴하는데 드는 비용

청구내역		고객 사항		사용량 사항		사용량 비교	
기본 요금	246,400	계약종별	일반용(갑)저압	당 월 심 야	39,832.00	당 월	5,979 kWh
전력량요금	551,861	정기검침일	매월 18 일	전 월 심 야	37,447.00	전 월	4,747 kWh
역률 요금	-2,464			당 월 기타	58,445.00	전 년 동 월	5,037 kWh
자동납부할인액	-1,000	계기배수	1	전 월 기타	54,851.00		
모바일청구할인	-200	역률	100				
전기요금계	794,597	계약전력	40 kW				
부가가치세	79,460	가구수	0				
전력기금	29,400	TV대수	0				
원단위결사	-7	최대수요전력	34 kW				
당월요금 계	903,450						
	903,450						
청구금액		903,450					

모델명	임대료	모델명	임대료
비트메인 L3	120,000	비트메인 Z9	70,000
비트메인 S9	170,000	이노실리콘 A8+	80,000
비트메인 A3	160,000	이노실리콘 S11	170,000
비트메인 D3	160,000	이노실리콘 D9	130,000
비트메인 B3	70,000	바이칼 N기종	50,000
비트메인 E3	120,000	바이칼 B	70,000
비트메인 X3	70,000	바이칼 X10	70,000

Mining incentive

▣ 채굴하는데 드는 비용



Mining incentive

▣ 채굴하는데 드는 비용

▣ Application Specific Integrated Circuit (ASIC)



<https://www.buybitcoinworldwide.com/wp-content/themes/kepler/img/miners/21.jpg>

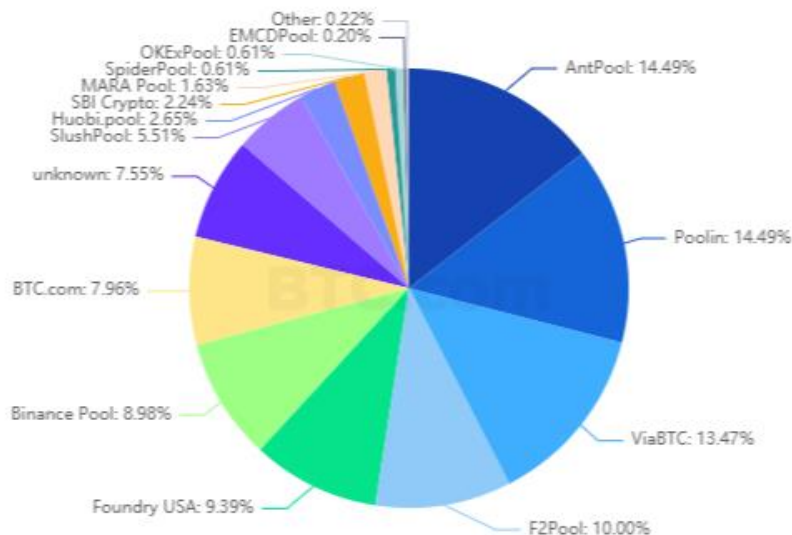


https://sc01.alicdn.com/kf/HTB18YN_JFXXXXcgXFXXq6xXFXXXw/221223714/HTB18YN_JFXXXXcgXFXXq6xXFXXXw.jpg

□ Mining pool











▣ 채굴을 위해 다수의 채굴기를 연결한 네트워크

- 전 세계 채굴 업체들이 채굴 성공률을 높이기 위해 자발적으로 결성한 채굴 조합
- 마이닝 풀에 가입하여 채굴에 성공한 경우, 참가자들은 각자의 해시 파워를 통해 비율에 따라 채굴 보상을 받을 수 있음



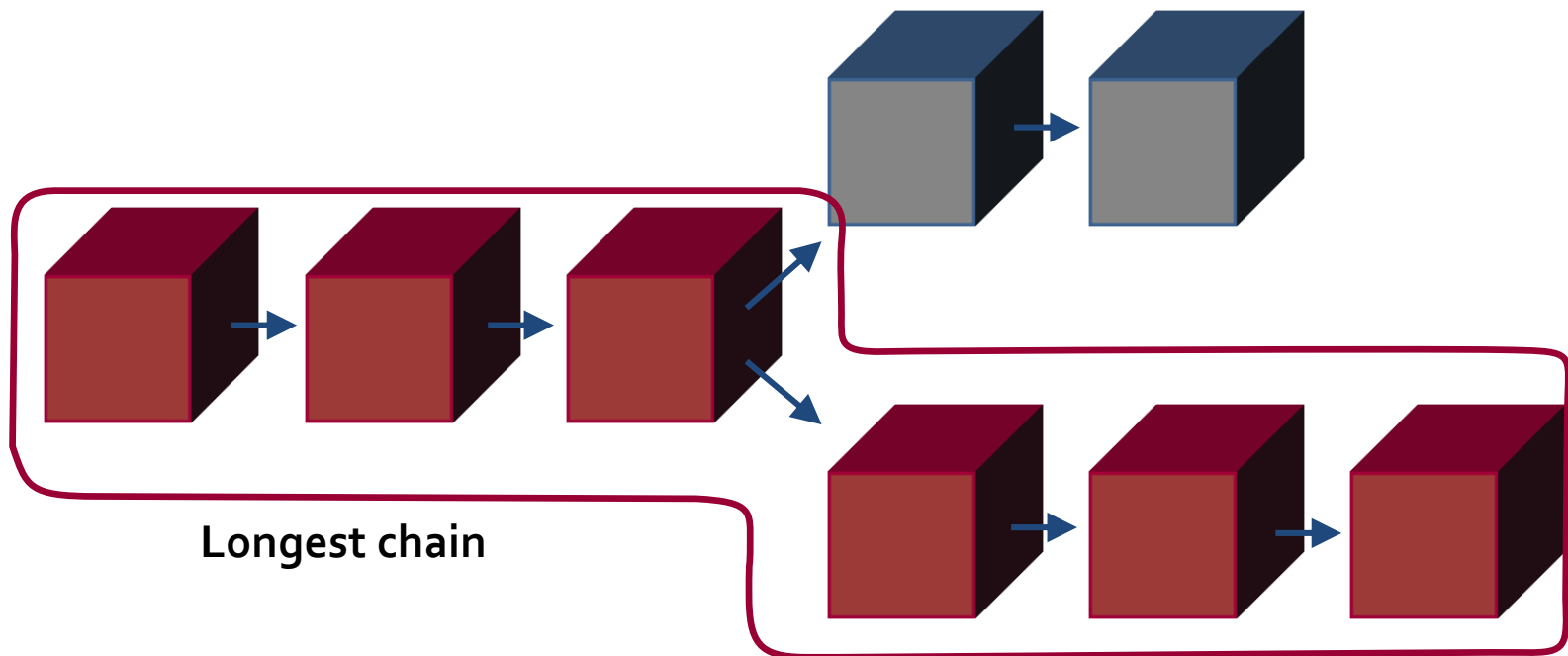
□ Mining pool

- ▣ 장점: 마이닝 풀에 개별적으로 참여할 수 있고, 소프트웨어가 바뀔 때 업그레이드에 용이성이 있음
- ▣ 단점: 풀 관리자를 신뢰해야만 하고, 마이닝이 중앙화 되어 있어 외부로부터 공격을 받을 수 있음

랭킹	마이닝풀	해시레이트	비율	블록 수량	빈 블록(비율)	평균 블록 수수료(BTC)
0	전체 네트워크	133906.41 PH/s	100.00%	490	1(0.20%)	0.08282937
1	 Poolin	19402.77 PH/s	14.49%	71	0(0%)	0.07120494
2	 AntPool	19402.77 PH/s	14.49%	71	0(0%)	0.08352761
3	 ViaBTC	18036.37 PH/s	13.47%	66	0(0%)	0.09004508
4	 F2Pool	13390.64 PH/s	10.00%	49	1(2.04%)	0.07920371
5	 Foundry USA	12570.81 PH/s	9.39%	46	0(0%)	0.08339513
6	 Binance Pool	12024.25 PH/s	8.98%	44	0(0%)	0.09154330
7	 BTC.com	10657.86 PH/s	7.96%	39	0(0%)	0.07579624
8	 unknown	10111.30 PH/s	7.55%	37	0(0%)	0.08195685
9	 SlushPool	7378.52 PH/s	5.51%	27	0(0%)	0.09280109
10	 Huobi.pool	3552.62 PH/s	2.65%	13	0(0%)	0.08771924

Confirmation

- Transaction 이 확정 되기 위해서는 6 번의 confirmation이 필요
 - 6번의 confirmation = 6개의 연결된 블록 생성
 - 6번의 confirmation = 약 10 min * 6 = 약 1 hour (그 이상이 될 수 있음 -> 거래수수료가 적을 경우)



□ Longest chain

- ▣ 6 번의 Confirmation을 기다리는 것은 결제 완전성 (Settlement Finality) 때문

- ▣ 이중 지불 (Double-spending) 문제

- 중복하여 지불하는 문제가 발생했을 때, 어느 한쪽에서 빠르게 길게 연결된 블록들을 만들 경우, 길게 연결된 블록들을 선택
 - 컴퓨팅 작업을 가장 많이 한 체인을 선택

CONTENTS

- ❑ Exchange markets

Exchange markets

□ Bitcoin 수집 방법

- ▣ 채굴

- ▣ Bitcoin ATM기 (현금 -> Bitcoin)

- ▣ 암호화폐 거래소 (현금/다른 암호화폐 -> Bitcoin)

Exchange markets

□ Mining



Graphic cards



ASIC

Exchange markets

□ Bitcoin ATM



올해 비트코인 ATM 시간당 1대씩 증가...전년 대...
tokenpost.kr



비트코인 ATM기, 전 세계 6,000대 돌파 - 코...
coinpress.co.kr



ATM 설치 현황



비트코인 합법화된 美 LA에 비트코인 ATM 2대 ...



비트코인 법정통화

[Source [비트코인 atm - Google 검색](#)]

Exchange markets

❑ Exchanges:

❑ <https://bitcoin.org/en/exchanges>

❑ Trading between different types of currency

International

Peer-to-Peer (P2P)

Asia

Bahrain

Indonesia

Israel

Japan

Kuwait

Malaysia

Oman

Singapore

South Korea

Saudi Arabia



Oman

[Currency.com](#)

[Rain](#)



South Korea

[Bithumb](#)

[Coinone](#)

[Currency.com](#)

[Korbit](#)



Taiwan

[Currency.com](#)

[MaiCoin MAX](#)

[Bitopro](#)



Singapore

[Binance](#)

[Currency.com](#)

[Mine Digital](#)



Saudi Arabia

[Currency.com](#)

[Rain](#)



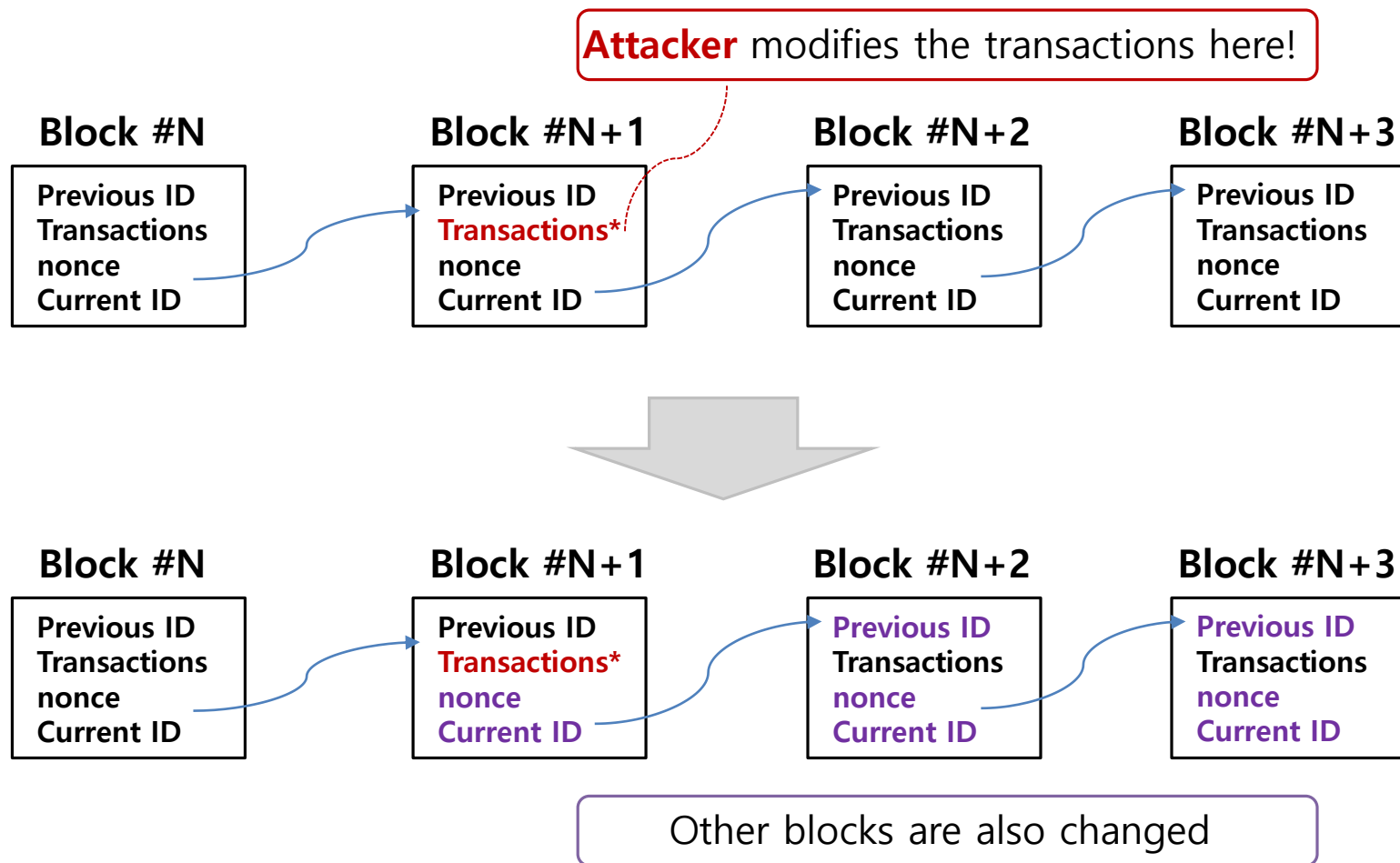
Turkey

[Koinim](#)

CONTENTS

- ❑ Attacks on bitcoin

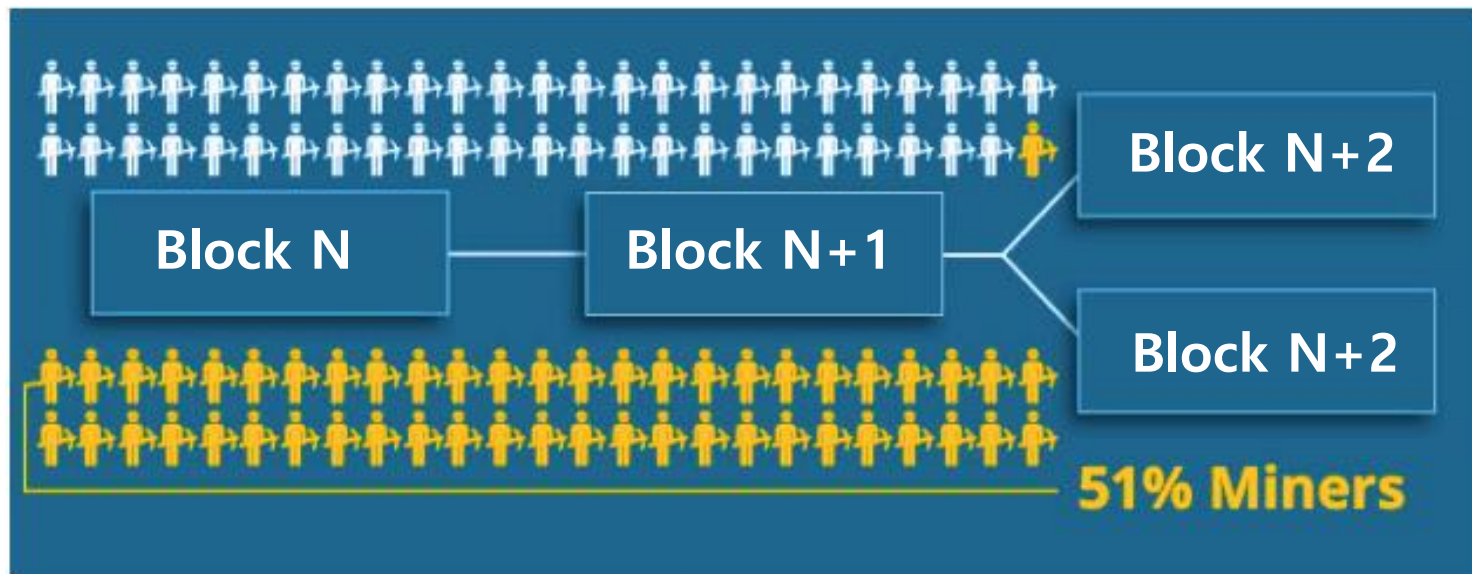
Attacks on bitcoin



Attacks on bitcoin

❑ Problem of PoW - 51% attacks

- ❑ 블록체인 노드의 사용자 또는 그룹(즉, 마이닝 풀)이 전체 채굴 능력 대부분을 제어하는 경우 51% 공격 가능



Attacks on bitcoin

□ Example of PoW - 51% attacks

▣ Alice는 51% 공격 사건에 연루되어 있으며, Bob은 정상 사용자

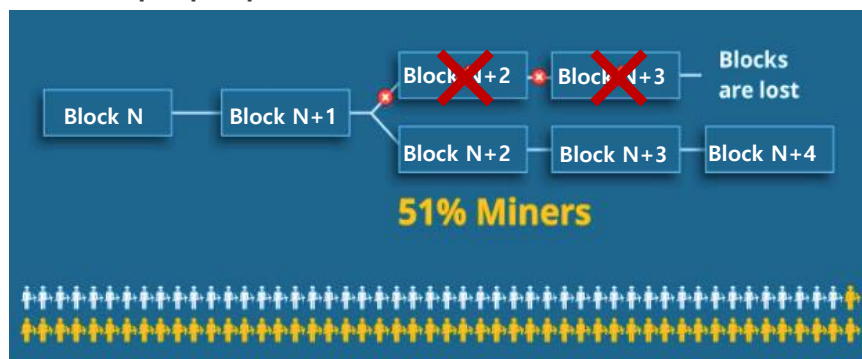
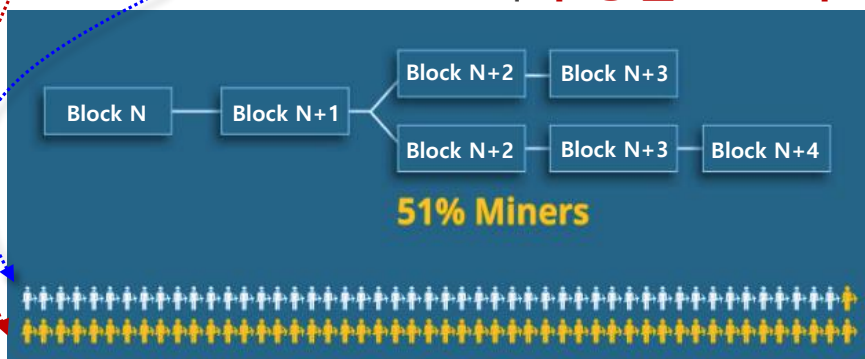
- Bob의 트랜잭션이 블록에 배치될 때 **공격자**가 트랜잭션을 수정 및 조작함 => 블록체인에서 포크가 발생 => **Alice의 그룹**은 해당 체인에는 더 많은 블록이 포함될 가능성이 높음

■ Alice의 그룹이 전체 채굴 능력의 대부분(51%)을 가지고 있음

- Longest-chain Rule에 의해 네트워크에서 더 오래 지속되는 분기가 남아 있게 되고, 짧은 분기는 거부됨

■ Bob의 **수정된 트랜잭션**은 블록에 저장됨

Alice Bob



- ❑ Bitcoin's block
- ❑ Bitcoin's transaction
 - ❑ UTXO
 - ❑ Transaction structure
- ❑ Public addresses
- ❑ Real-mining and confirmation of bitcoin
- ❑ Exchange markets
- ❑ Attacks on bitcoin

- ❑ Lecture slides from BLOCKCHAIN @ BERKELEY

- ❑ Mastering Bitcoin,
<https://github.com/bitcoinbook/bitcoinbook>

- ❑ <https://steemit.com/blockchain/@niipoong>

Q & A

