BITCOIN : A PEER-TO-PEER ELECTRONIC CASH SYSTEM

Outline

- Background
- Introduction
- Transaction
- Blockchain
- Network
- Incentives
- SPV

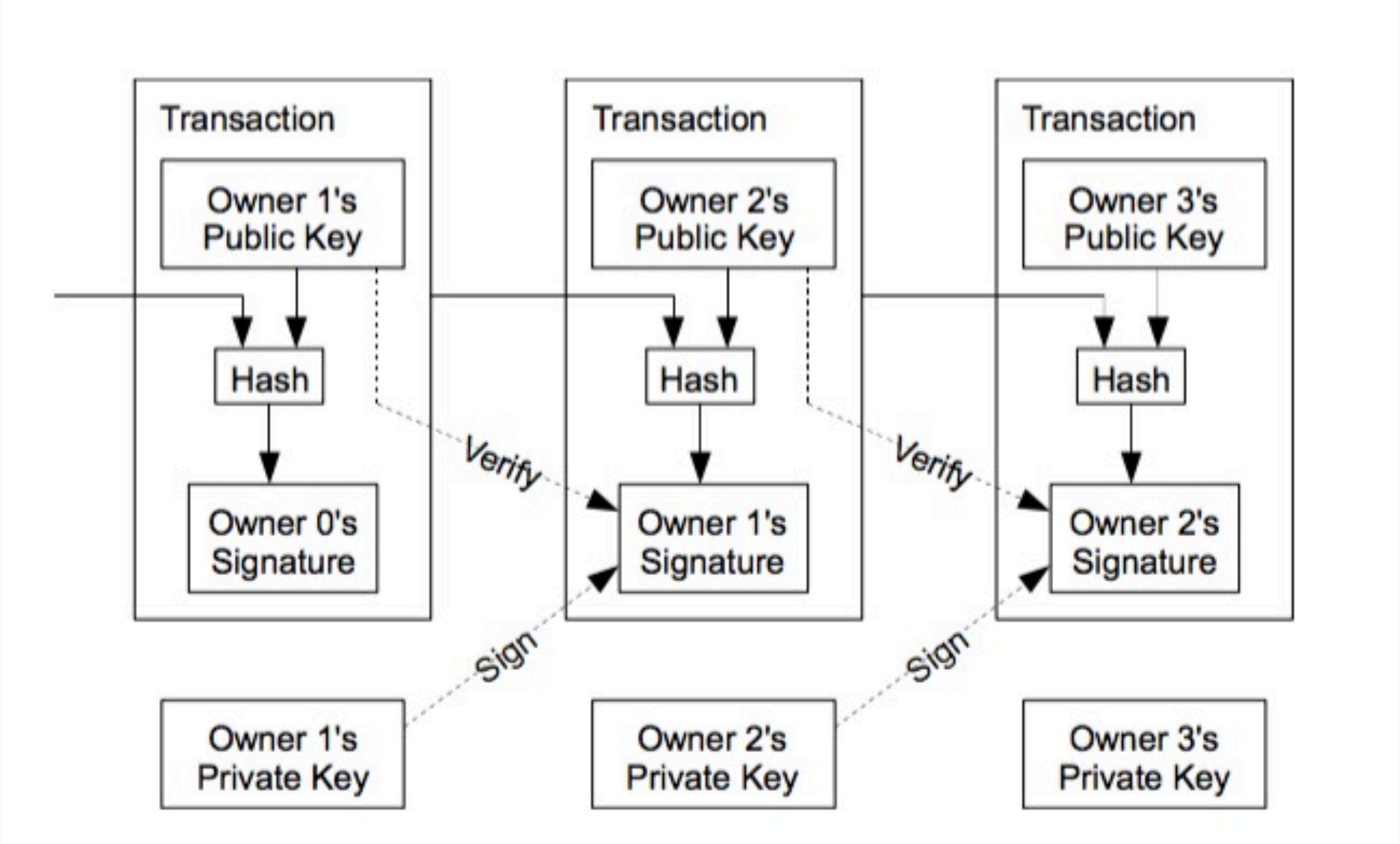
Background

- P2P Electronic Cash System
- No trusted 3rd Parties
- Completely non-reversible
- Avoid double-spending problem

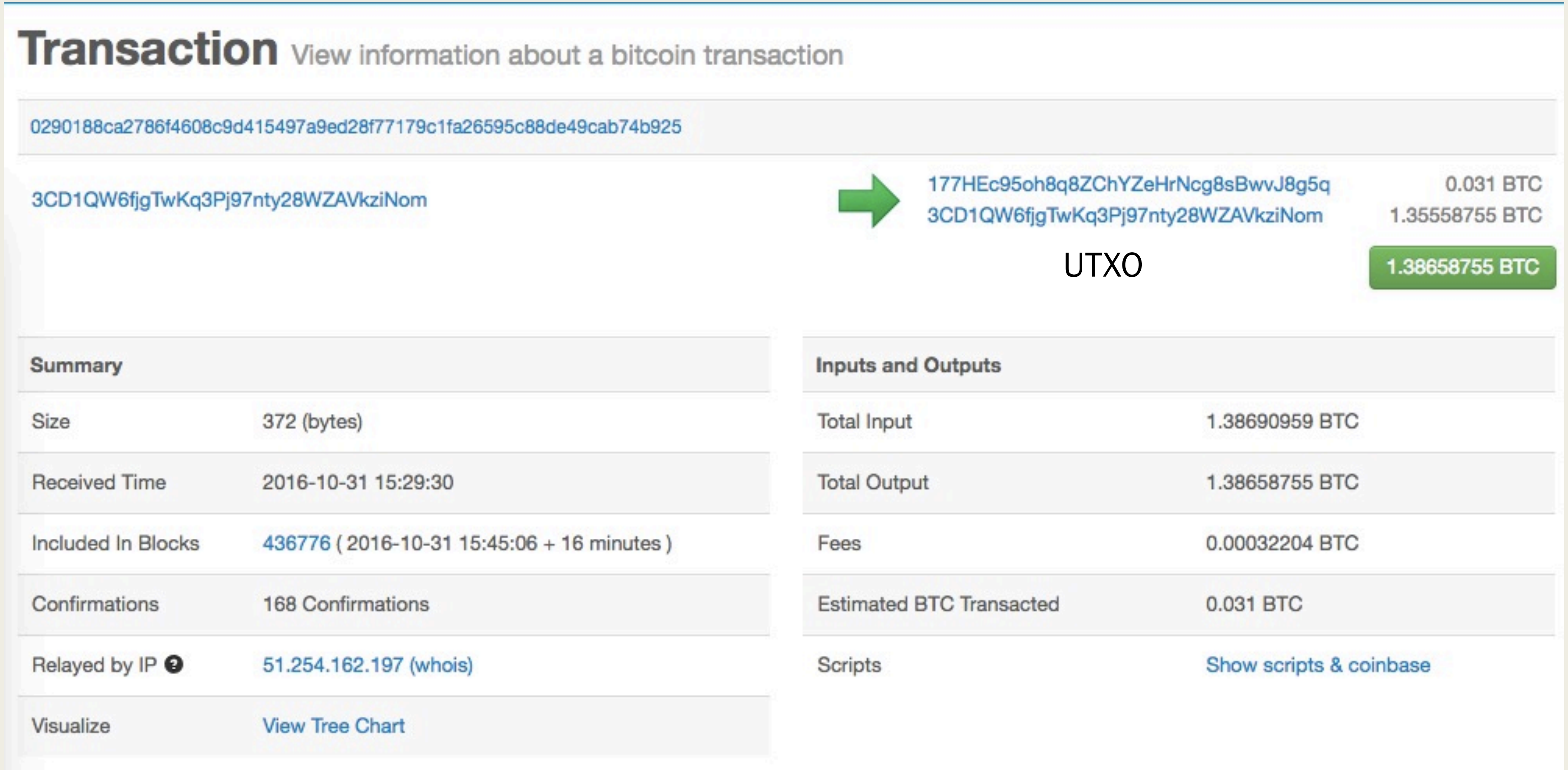
Introduction

- Digital signature as coin
- Blockchain as ledger
- Proof-of-work as consensus

Transaction



Transaction



Transaction View information about a bitcoin transaction

0290188ca2786f4608c9d415497a9ed28f77179c1fa26595c88de49cab74b925

3CD1QW6fjgTwKq3Pj97nty28WZAVkziNom →

177HEc95oh8q8ZChYZeHrNcg8sBwvJ8g5q	0.031 BTC
3CD1QW6fjgTwKq3Pj97nty28WZAVkziNom	1.35558755 BTC

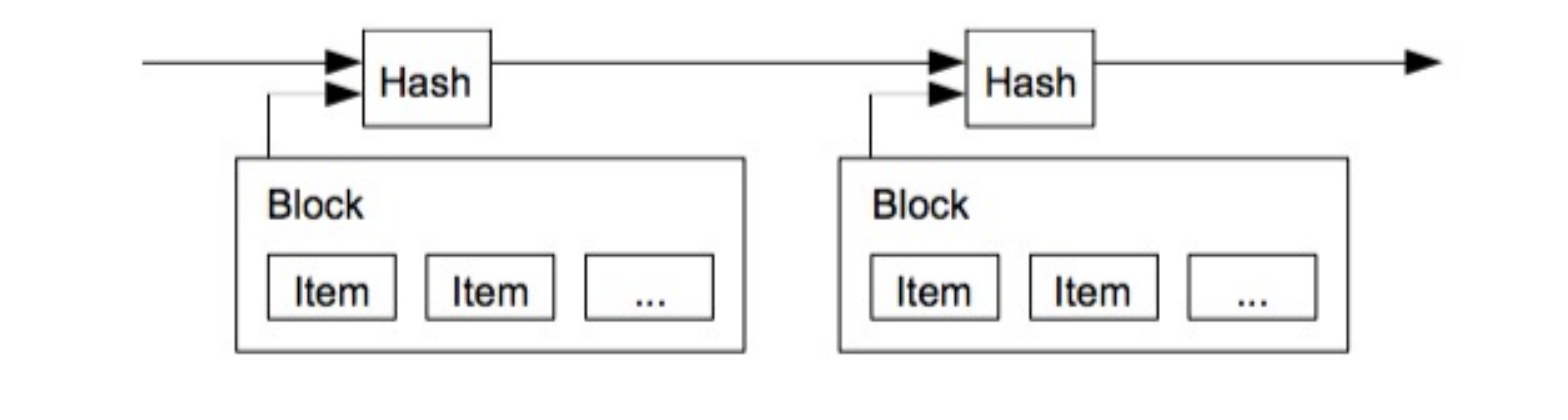
UTXO

1.38658755 BTC

Summary	
Size	372 (bytes)
Received Time	2016-10-31 15:29:30
Included In Blocks	436776 (2016-10-31 15:45:06 + 16 minutes)
Confirmations	168 Confirmations
Relayed by IP ❓	51.254.162.197 (whois)
Visualize	View Tree Chart

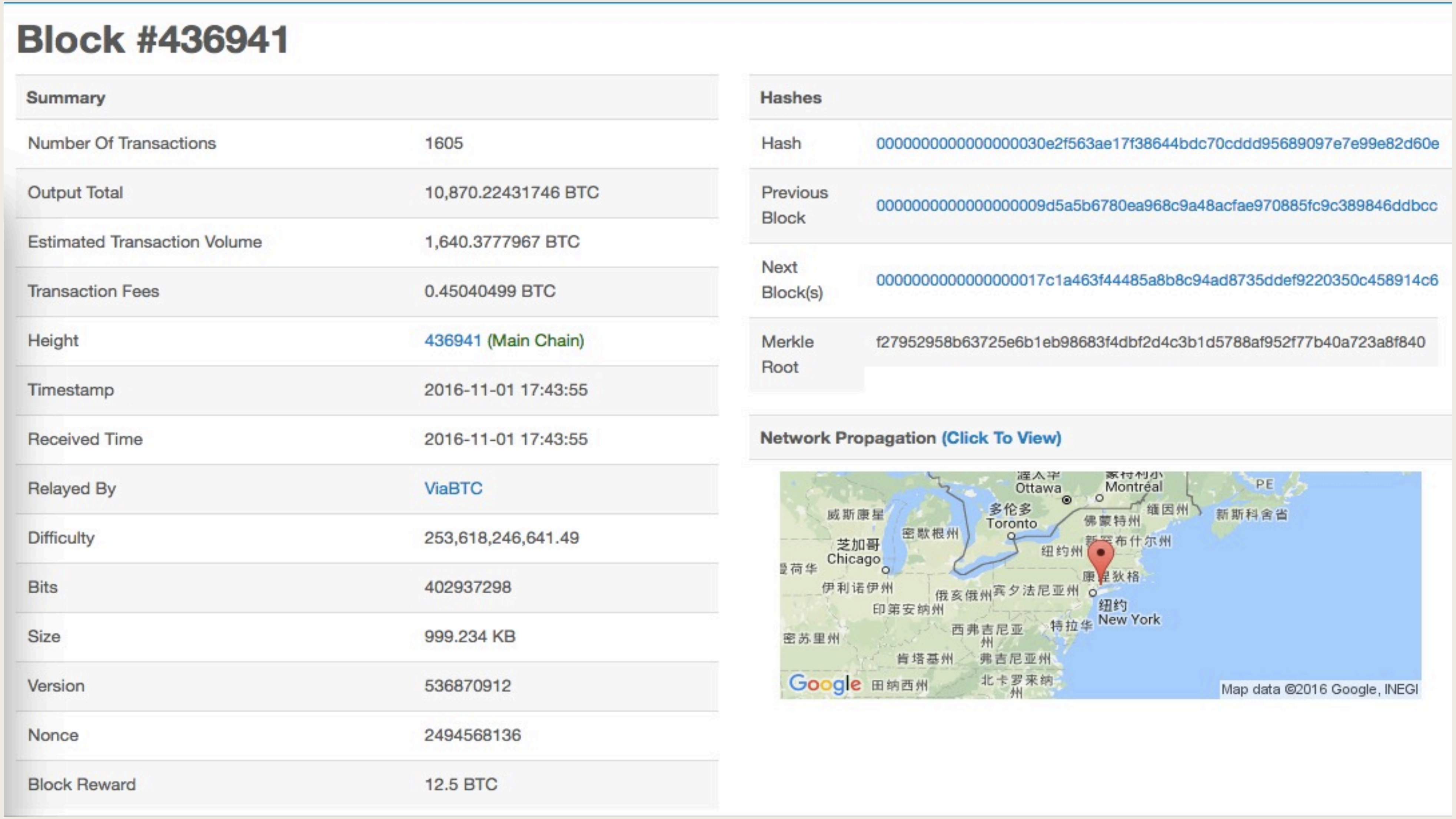
Inputs and Outputs	
Total Input	1.38690959 BTC
Total Output	1.38658755 BTC
Fees	0.00032204 BTC
Estimated BTC Transacted	0.031 BTC
Scripts	Show scripts & coinbase

Block



- One block contains many transactions
- Timestamp server (based on PKI)
- Hash
- Blockchain

Block



Block #436941

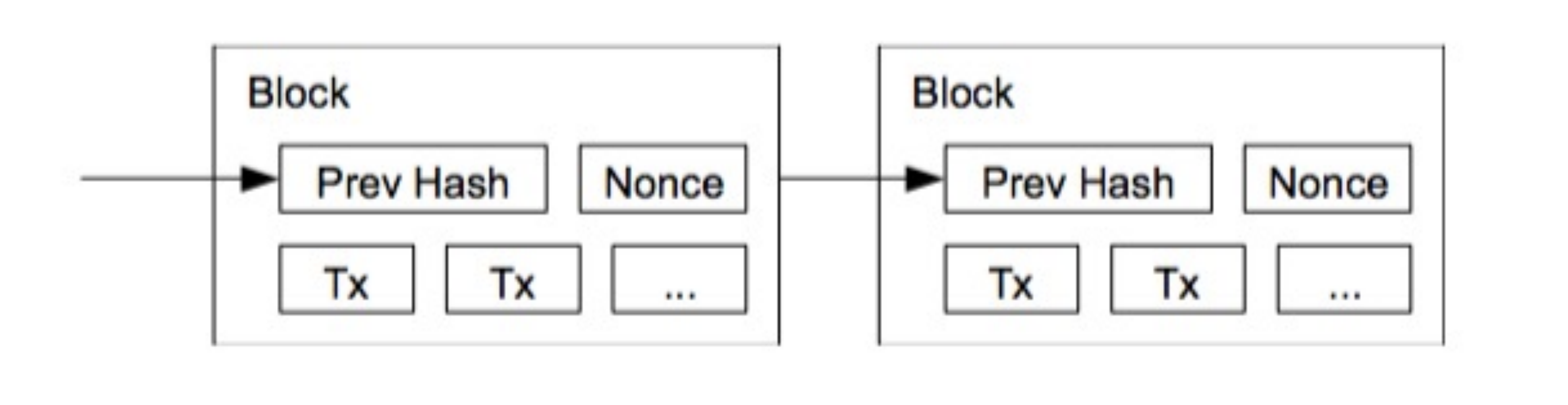
Summary	
Number Of Transactions	1605
Output Total	10,870.22431746 BTC
Estimated Transaction Volume	1,640.3777967 BTC
Transaction Fees	0.45040499 BTC
Height	436941 (Main Chain)
Timestamp	2016-11-01 17:43:55
Received Time	2016-11-01 17:43:55
Relayed By	ViaBTC
Difficulty	253,618,246,641.49
Bits	402937298
Size	999.234 KB
Version	536870912
Nonce	2494568136
Block Reward	12.5 BTC

Hashes	
Hash	00000000000000000030e2f563ae17f38644bdc70cddd95689097e7e99e82d60e
Previous Block	0000000000000000009d5a5b6780ea968c9a48acfae970885fc9c389846ddbcc
Next Block(s)	00000000000000000017c1a463f44485a8b8c94ad8735ddef9220350c458914c6
Merkle Root	f27952958b63725e6b1eb98683f4dbf2d4c3b1d5788af952f77b40a723a8f840

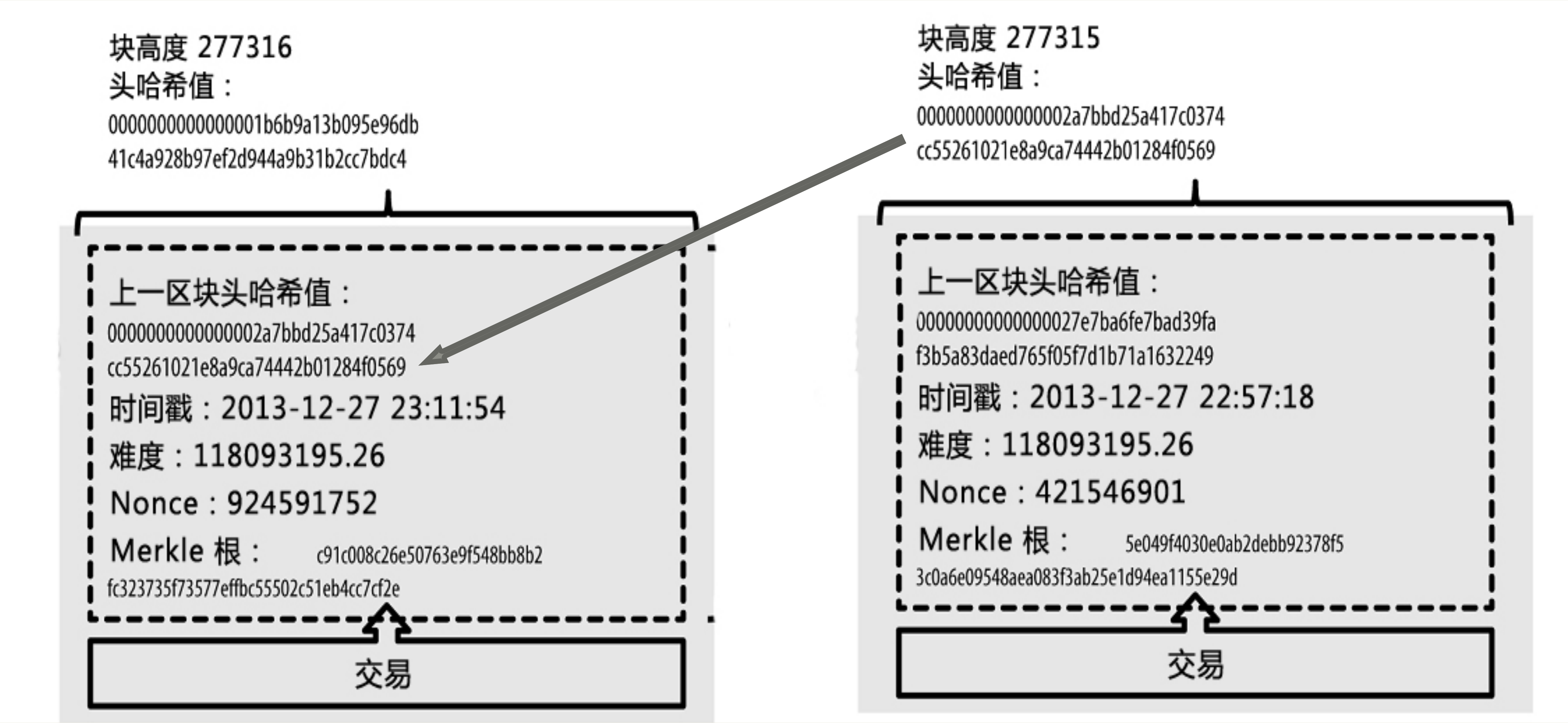
Network Propagation (Click To View)

Proof-of-work

- Consensus
- Byzantine Generals Problem



Proof-of-work



块高度 277316
头哈希值：
0000000000000001b6b9a13b095e96db
41c4a928b97ef2d944a9b31b2cc7bdc4

上一区块头哈希值：
0000000000000002a7bbd25a417c0374
cc55261021e8a9ca74442b01284f0569
时间戳：2013-12-27 23:11:54
难度：118093195.26
Nonce：924591752
Merkle 根： c91c008c26e50763e9f548bb8b2
fc323735f73577effbc55502c51eb4cc7cf2e

交易

块高度 277315
头哈希值：
0000000000000002a7bbd25a417c0374
cc55261021e8a9ca74442b01284f0569

上一区块头哈希值：
00000000000000027e7ba6fe7bad39fa
f3b5a83daed765f05f7d1b71a1632249
时间戳：2013-12-27 22:57:18
难度：118093195.26
Nonce：421546901
Merkle 根： 5e049f4030e0ab2debb92378f5
3c0a6e09548aea083f3ab25e1d94ea1155e29d

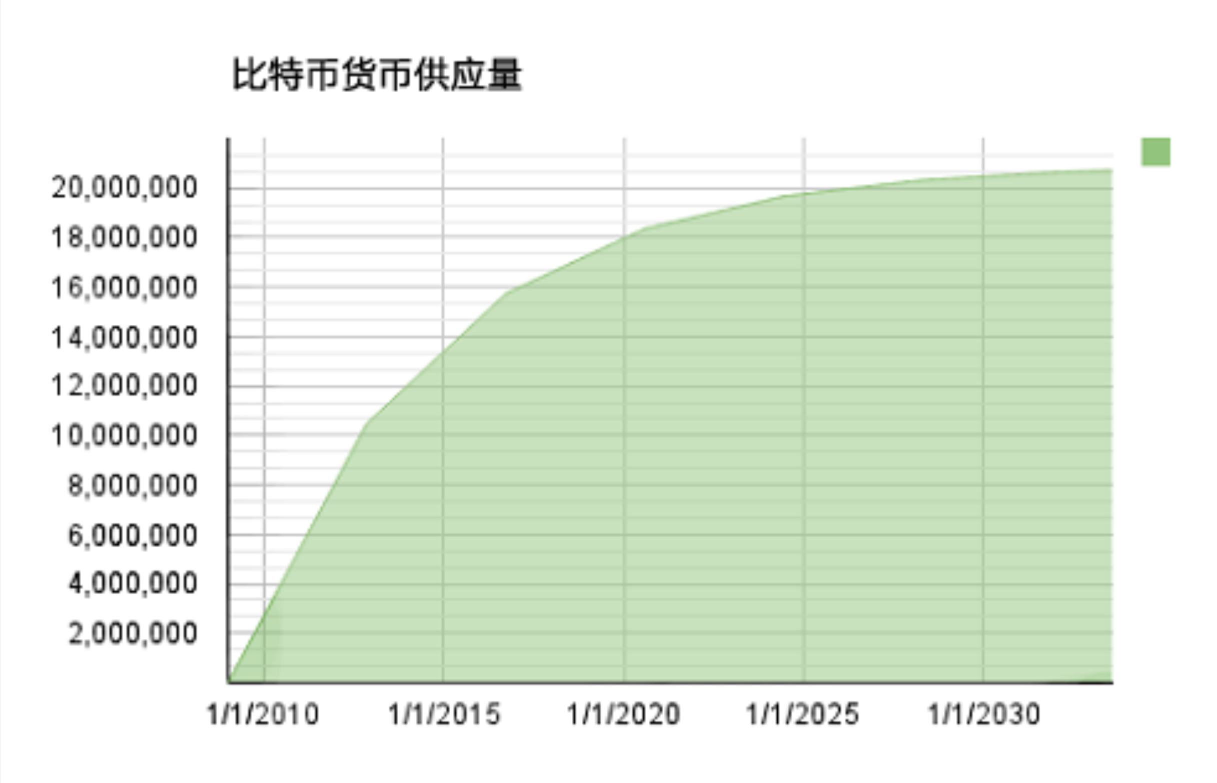
交易

Network

- New transactions are broadcast to all nodes.
- Each node collects new transactions into a block.
- Each node works on finding a difficult proof-of-work for its block.
- When a node finds a proof-of-work, it broadcasts the block to all nodes.
  - *what if two nodes find their own proof-of-work at the same time*
- Nodes accept the block only if all transactions in it are valid and not already spent.
  - *what & how to verify*
- Nodes express their acceptance of the block by working on creating the next block in the chain, using the hash of the accepted block as the previous hash.

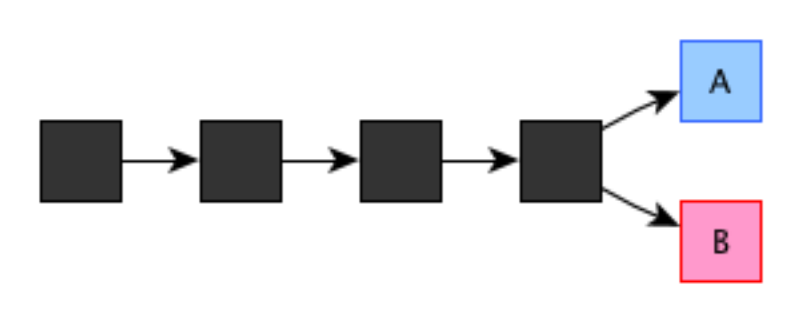
Incentives

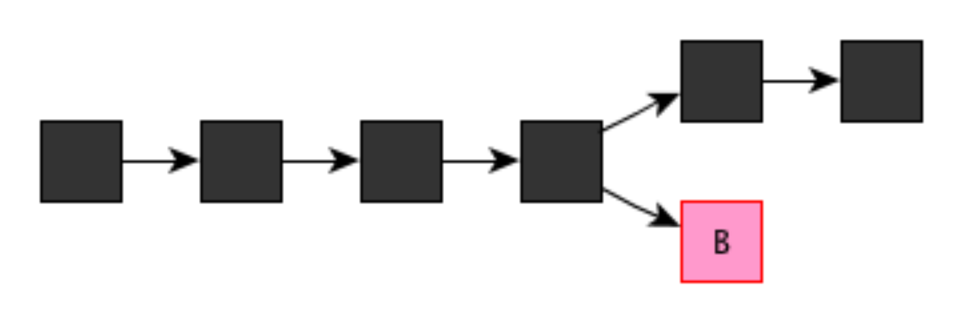
- Bitcoin issue
  - *coinbase : first transaction recorded in a block without input*
  - *halved every 210,000 block*
  - *totally 21,000,000*
- Transaction fees



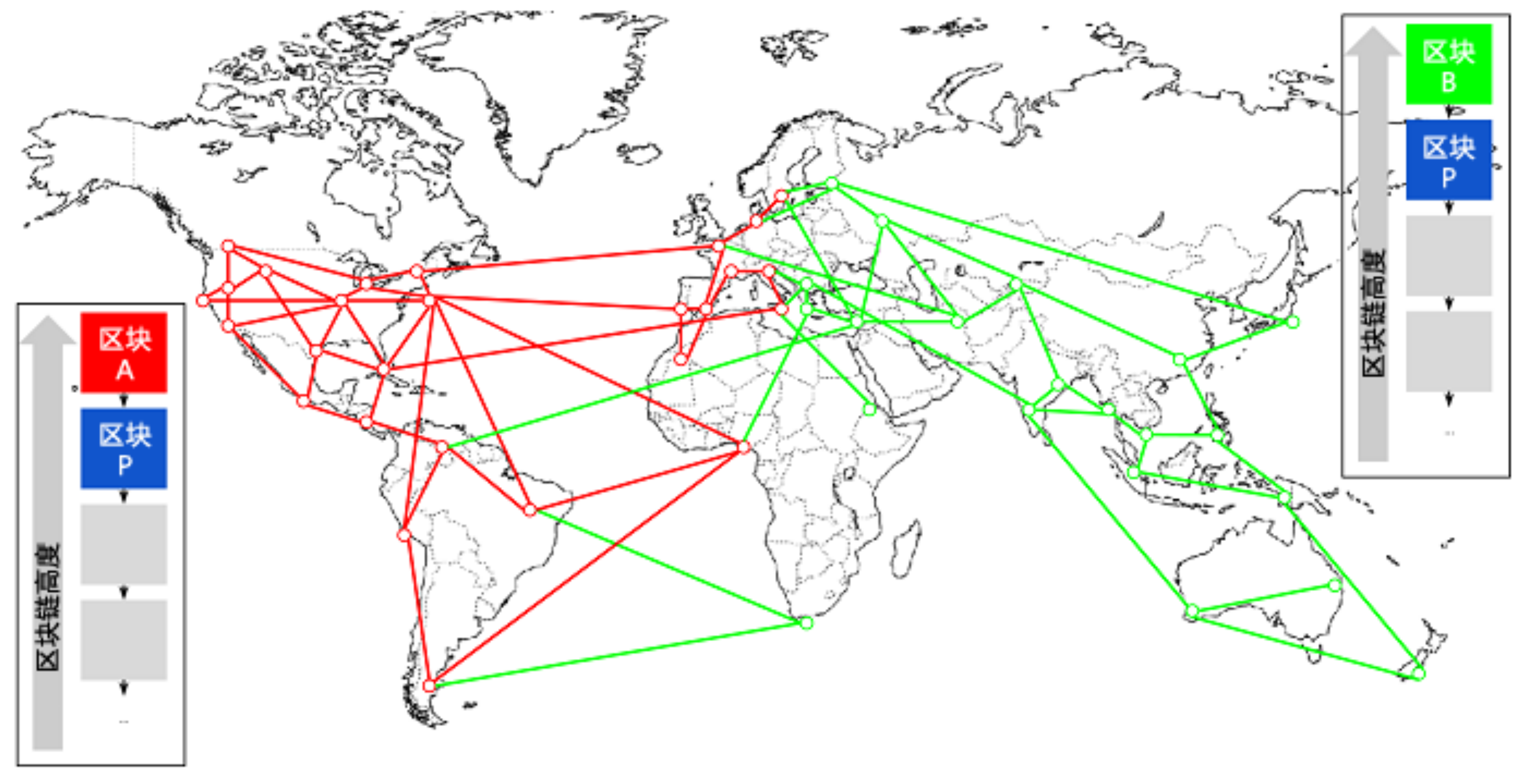
Branches in blockchain

- what if two nodes find their own proof-of-work at the same time
  - *save both*
  - *work on the sooner one*
  - *receive new block and check*
  - *always work on the longest chain*

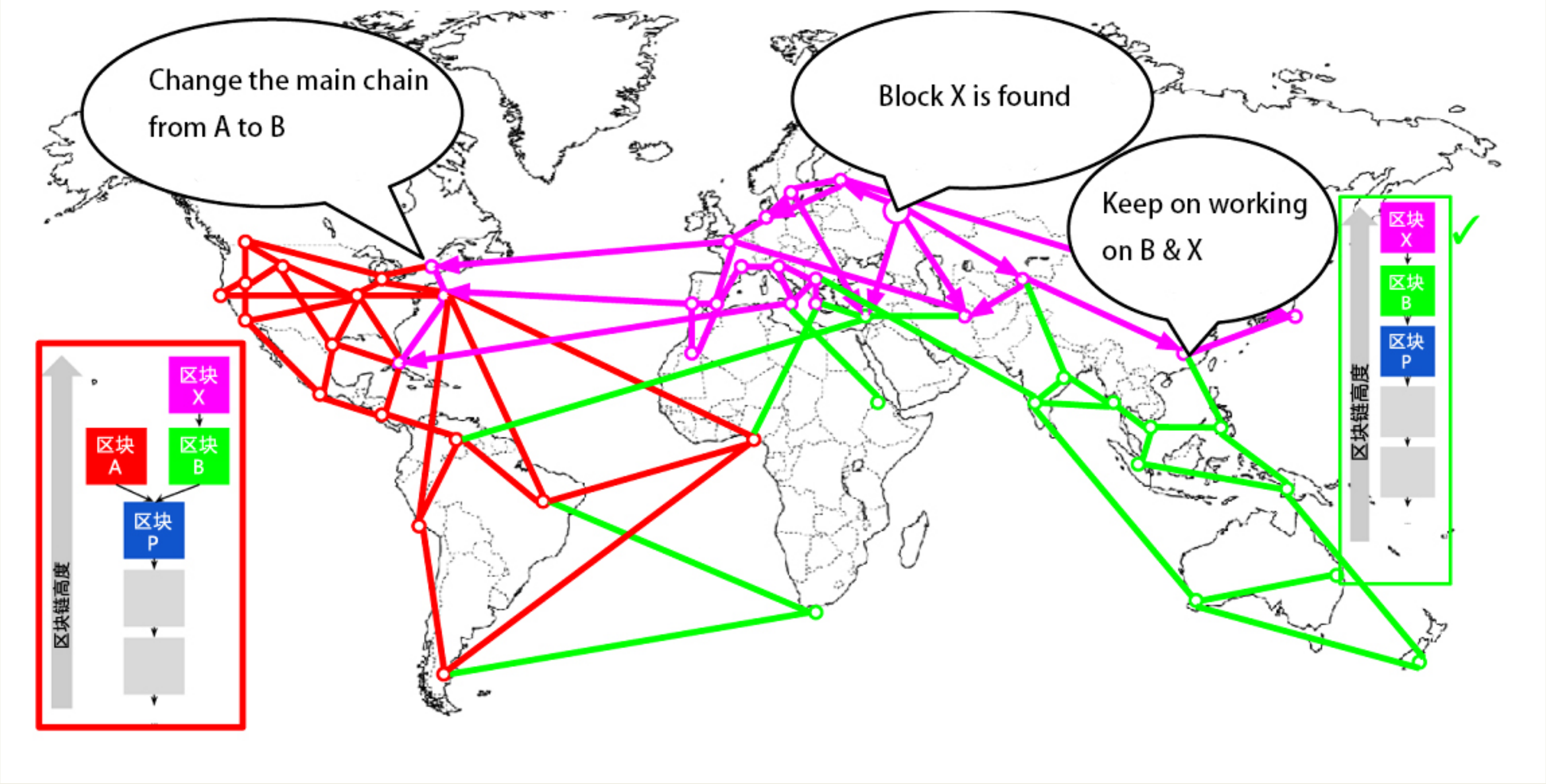




Branches in blockchain



Branches in blockchain



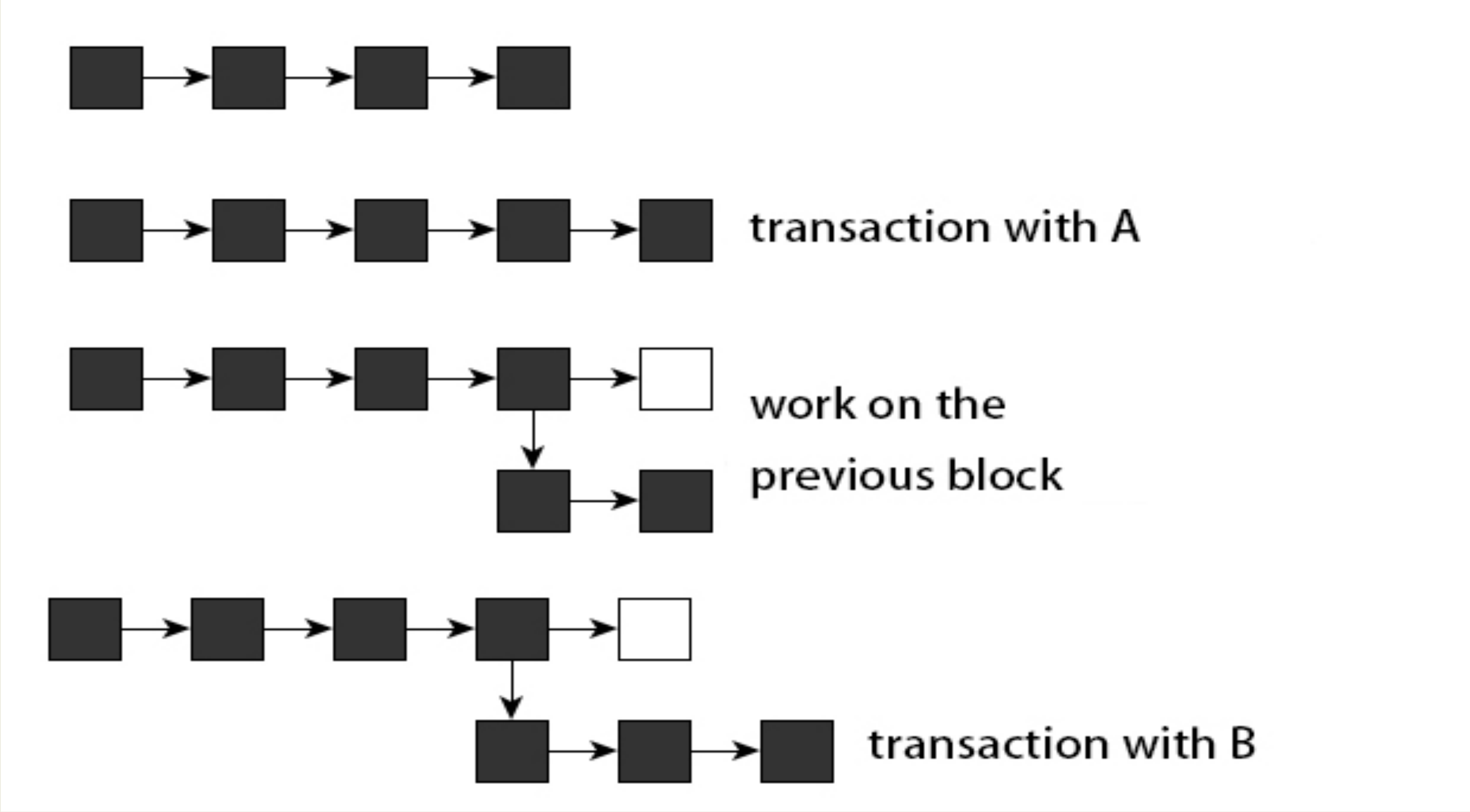
Change the main chain from A to B

Block X is found

Keep on working on B & X

Double-Spending

- work on the previous block to change the main chain
- Invalidate the transaction before

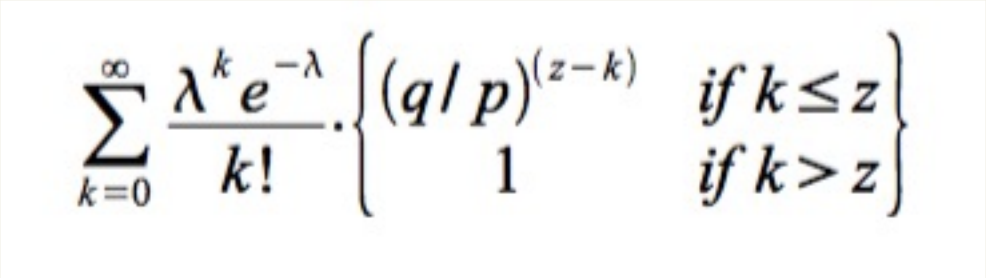


Probability Calculation

- p = probability an honest node finds the next block
  q = probability the attacker finds the next block
  q_z = probability the attacker will ever catch up from z blocks behind

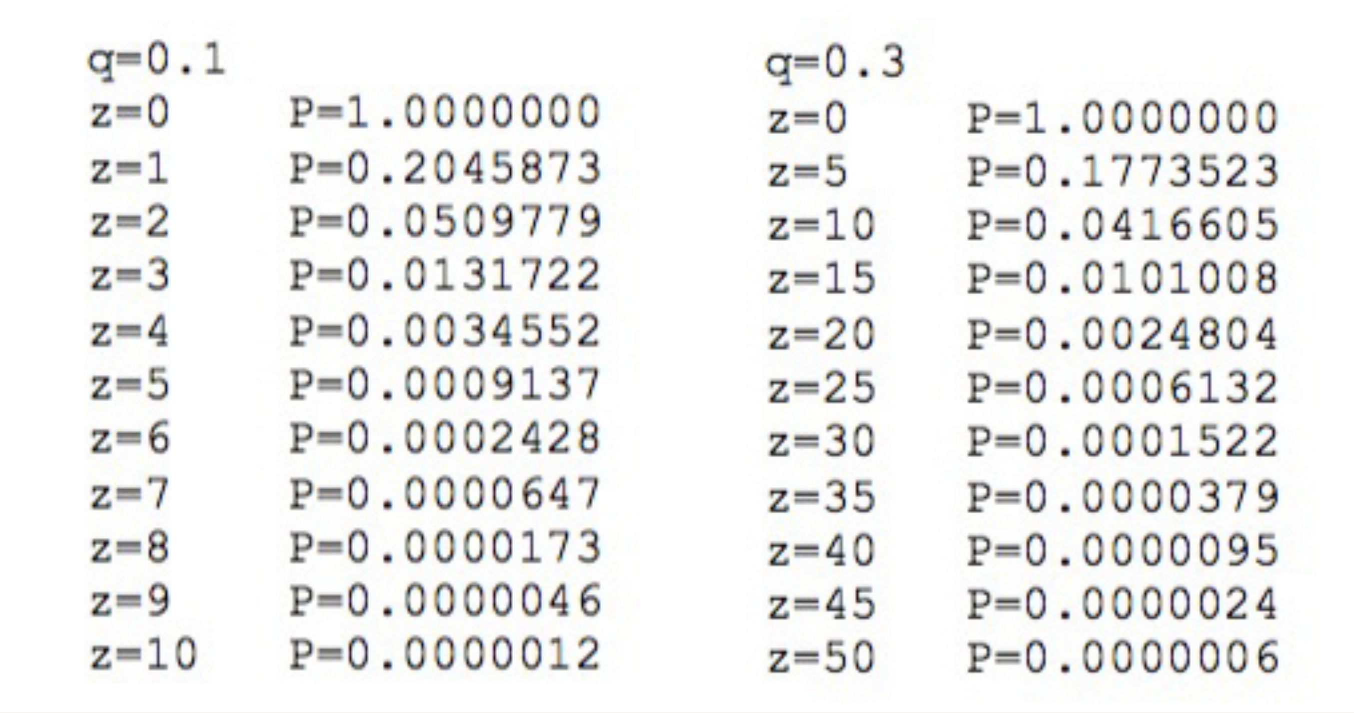
- $q_z = \begin{cases} 1 & if\ p \leq q \\ (\frac{q}{p})^z & if\ p \geq q \end{cases}$

- Poisson distribution $\lambda = \mathrm{z}\frac{q}{p}$



$$\sum_{k=0}^{\infty} \frac{\lambda^k e^{-\lambda}}{k!} \cdot \begin{Bmatrix} (q/p)^{(z-k)} & if\ k \leq z \\ 1 & if\ k > z \end{Bmatrix}$$

Probability Calculation



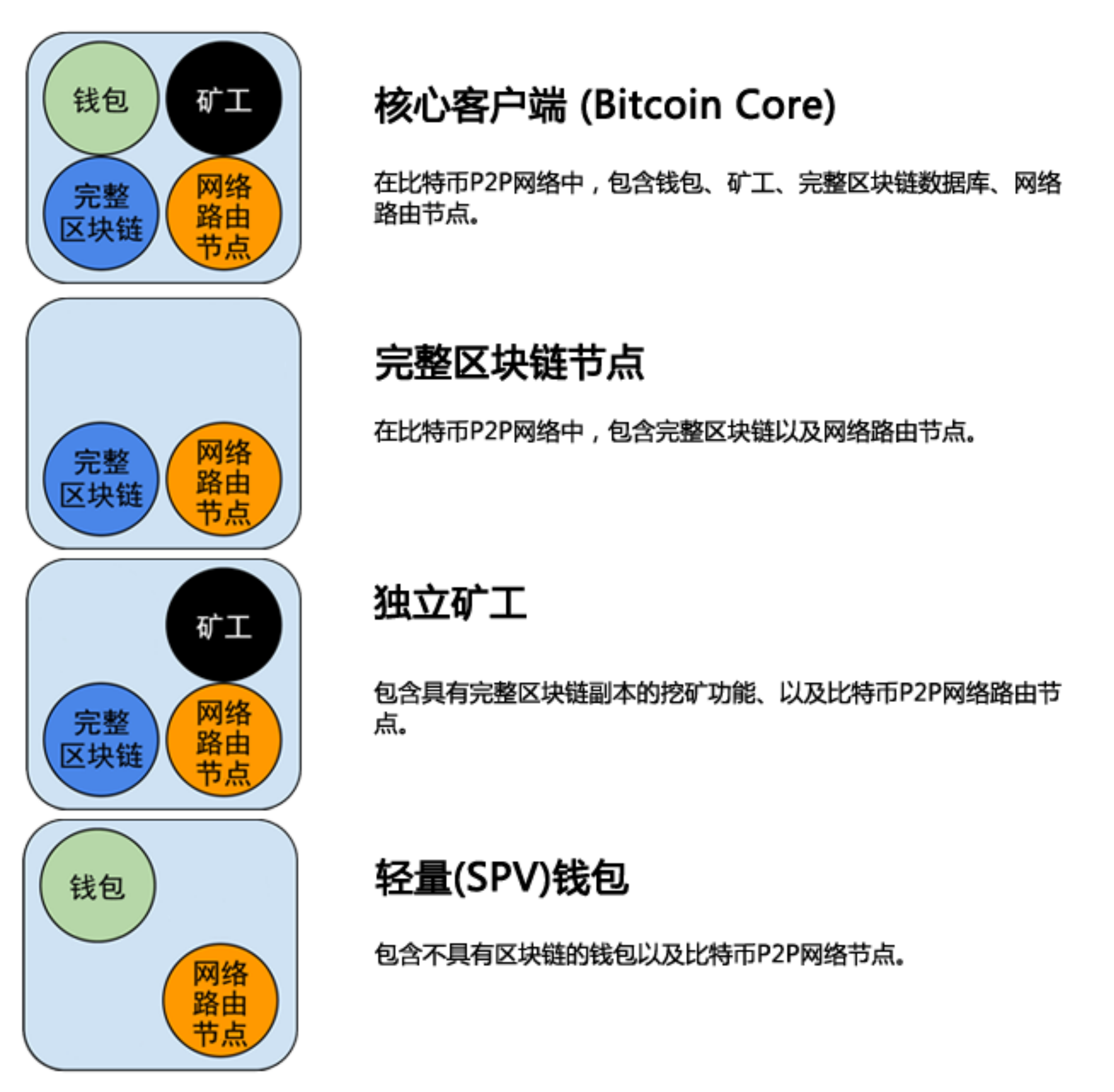
```
q=0.1                                q=0.3
z=0       P=1.0000000                z=0       P=1.0000000
z=1       P=0.2045873                z=5       P=0.1773523
z=2       P=0.0509779                z=10      P=0.0416605
z=3       P=0.0131722                z=15      P=0.0101008
z=4       P=0.0034552                z=20      P=0.0024804
z=5       P=0.0009137                z=25      P=0.0006132
z=6       P=0.0002428                z=30      P=0.0001522
z=7       P=0.0000647                z=35      P=0.0000379
z=8       P=0.0000173                z=40      P=0.0000095
z=9       P=0.0000046                z=45      P=0.0000024
z=10      P=0.0000012                z=50      P=0.0000006
```

DoS

- Denial of Service
- Fork intentionally
- Ignore certain transaction

Roles

- Bitcoin Core
- Full node
- Dependent miner
- SPV wallet



核心客户端 (Bitcoin Core)

在比特币P2P网络中，包含钱包、矿工、完整区块链数据库、网络路由节点。

完整区块链节点

在比特币P2P网络中，包含完整区块链以及网络路由节点。

独立矿工

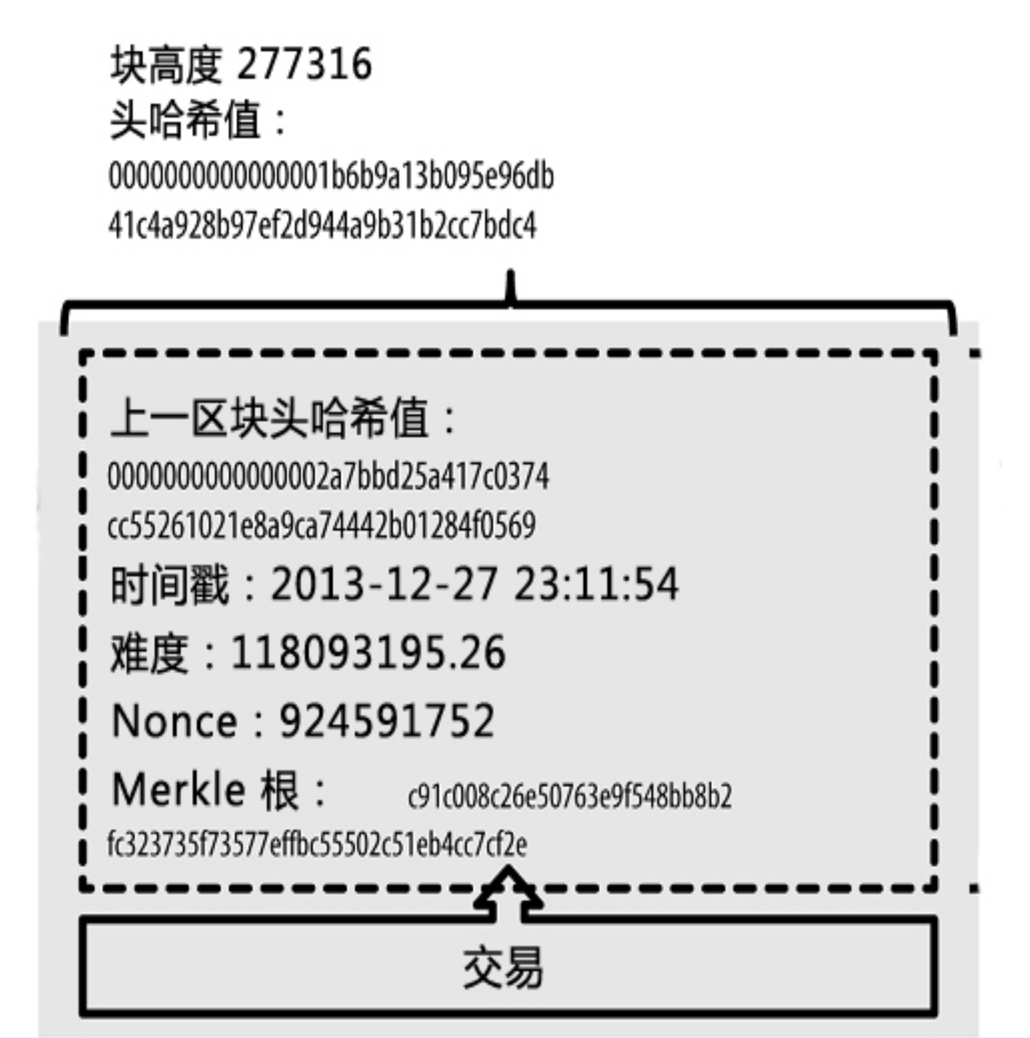
包含具有完整区块链副本的挖矿功能、以及比特币P2P网络路由节点。

轻量(SPV)钱包

包含不具有区块链的钱包以及比特币P2P网络节点。

Roles

- Bitcoin Core
- Full node
- Dependent miner
- SPV wallet



块高度 277316

头哈希值：

0000000000000001b6b9a13b095e96db
41c4a928b97ef2d944a9b31b2cc7bdc4

上一区块头哈希值：

0000000000000002a7bbd25a417c0374
cc55261021e8a9ca74442b01284f0569

时间戳：2013-12-27 23:11:54

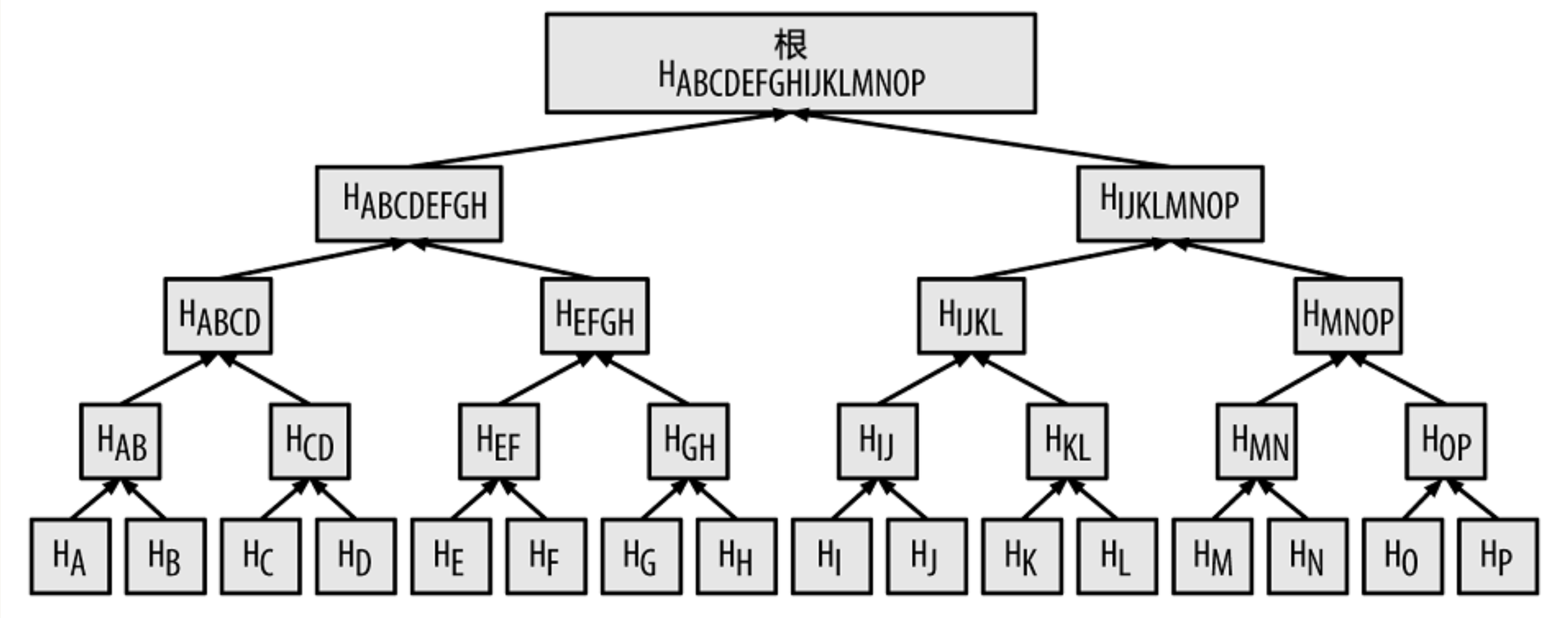
难度：118093195.26

Nonce：924591752

Merkle 根：c91c008c26e50763e9f548bb8b2
fc323735f73577effbc55502c51eb4cc7cf2e

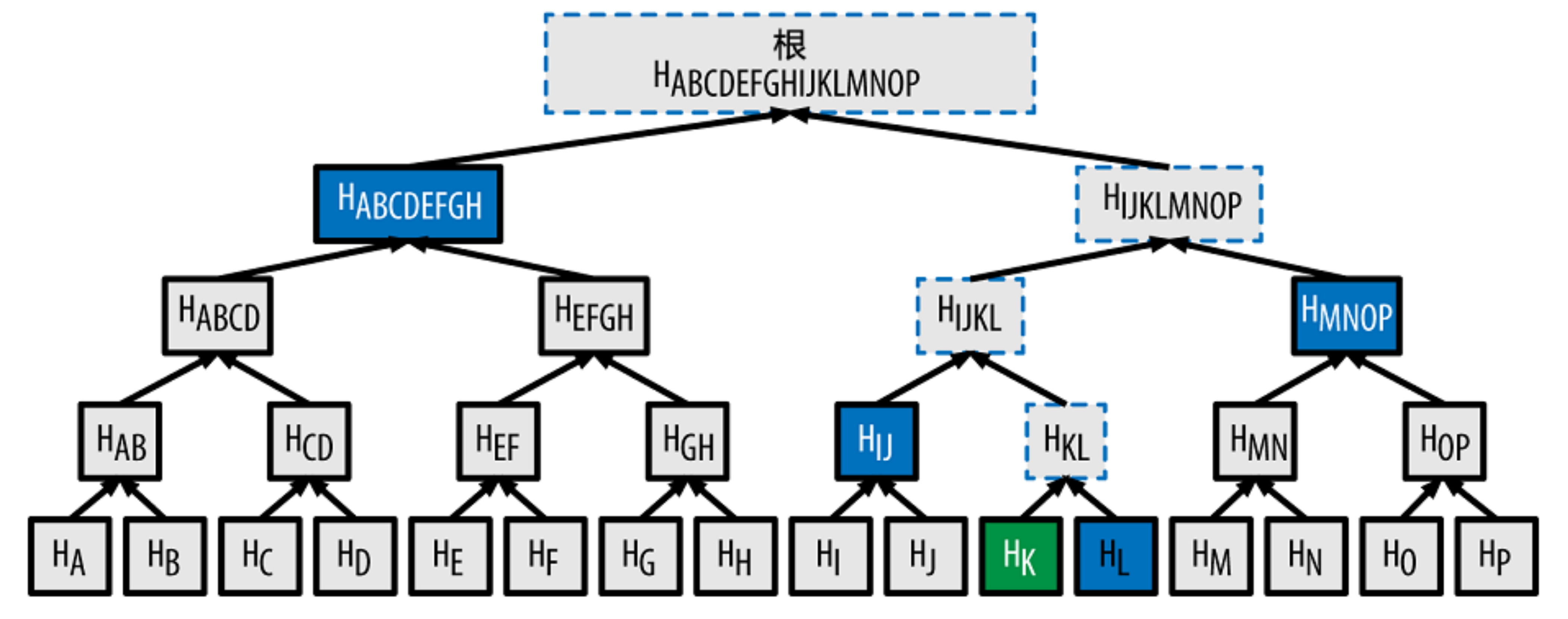
Merkle Tree

- Hash : double SHA-256
- H~AB=SHA256(SHA256(H~A + H~B))



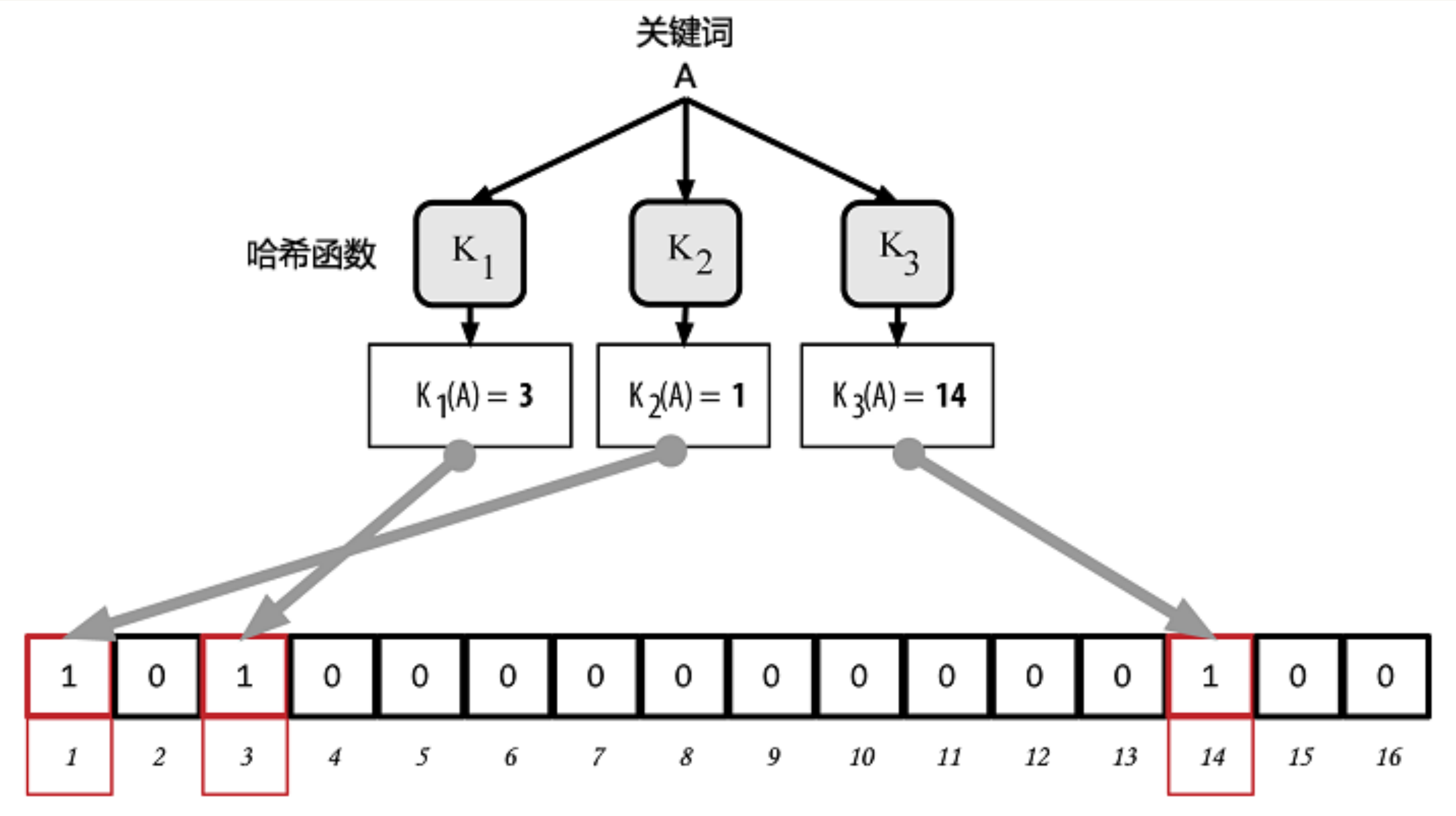
SPV

- Simplified Payment Verification



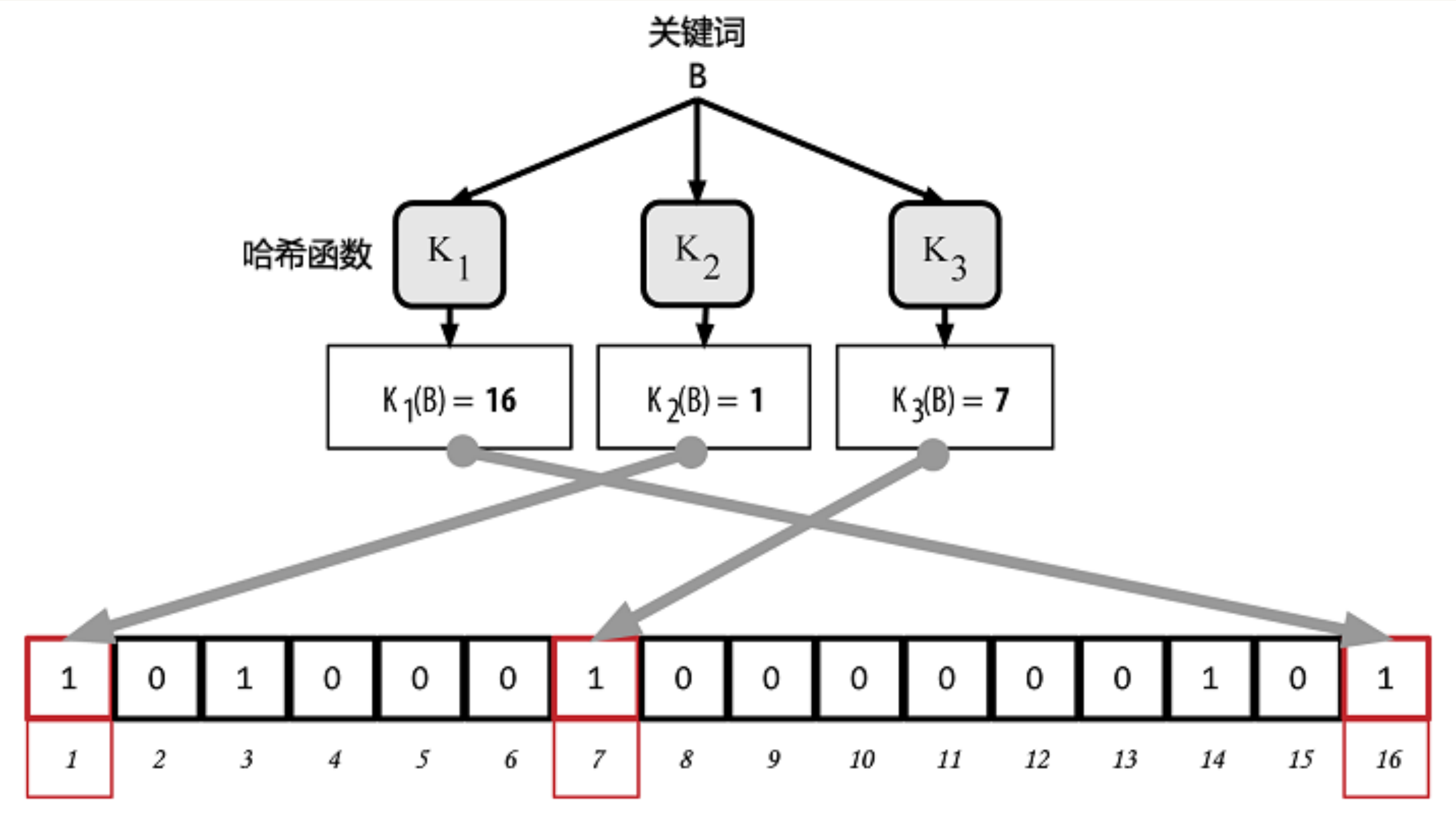
Bloom filter

- SPV query exposes personal information



Bloom filter

- SPV query exposes personal information



Blockchain 2.0

- Smart contract
- VM
- Decentralized app

——2016 Blockchain Whitepaper of China

Summary

- Cryptography
- Distributed system
- Game theory
- Genius combination

THANKS!