Bitcoin

PPKE, ITK
Csapodi Márton

Bitcoin book

Andreas M. Antonopoulos: Mastering Bitcoin

First edition (2014)

Second edition (2017) online:
https://github.com/bitcoinbook/bitcoinbook/blob/develop/book.asciidoc

Must read (learn):
1. Introduction
2. How bitcoin works
4. Keys, Addresses (some)
6. Transactions (some more)

Quick Start

Chose your wallet:

- platform: desktop, mobile, web, hardware, paper wallet
- capabilities: full node (stores the whole blockchain), lightweight (creates and validates transactions), third-party API (uses third party to create and validate transactions)

Install and start your wallet:

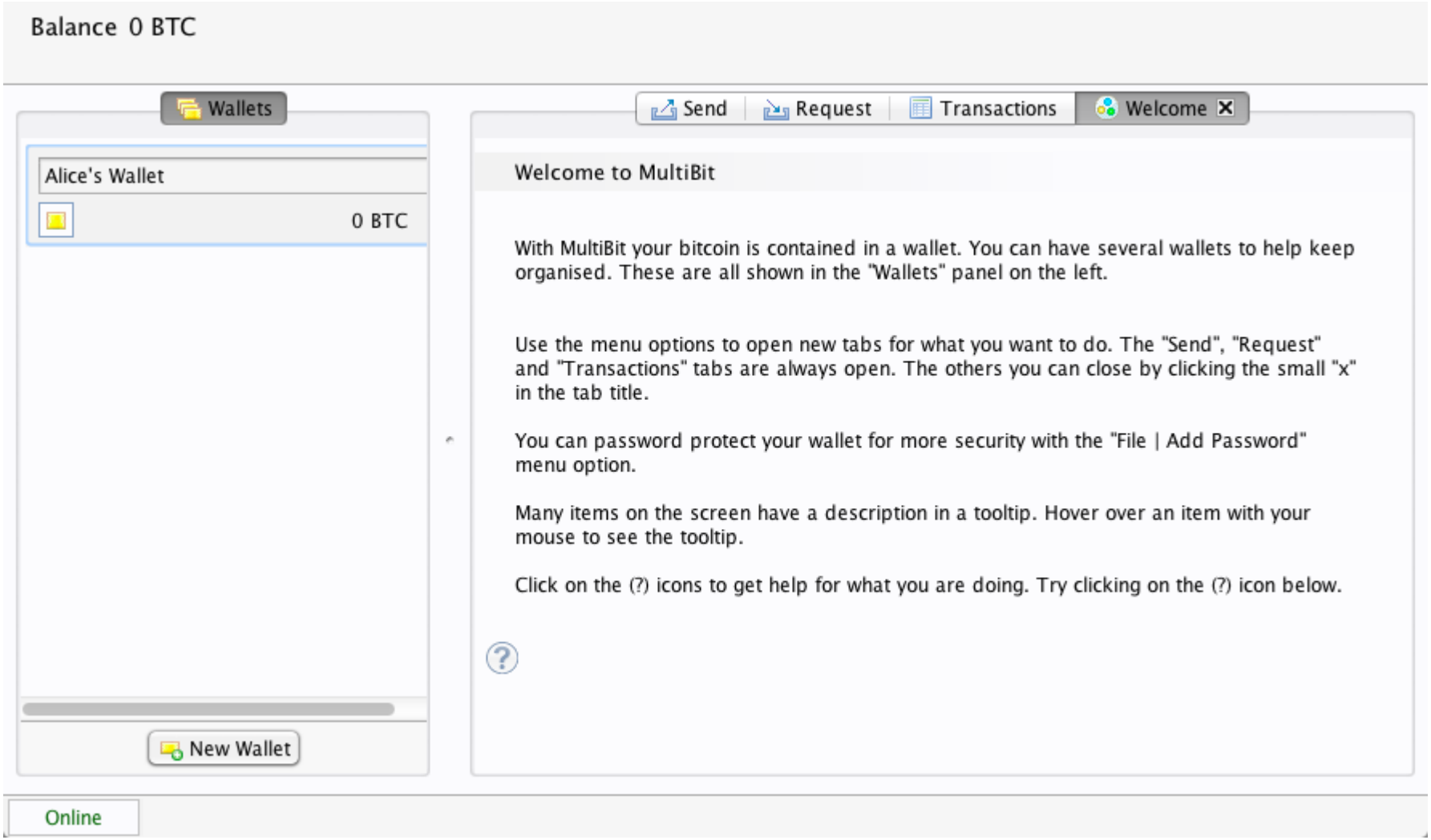
- bitcoin address and keys

Get your first bitcoin:

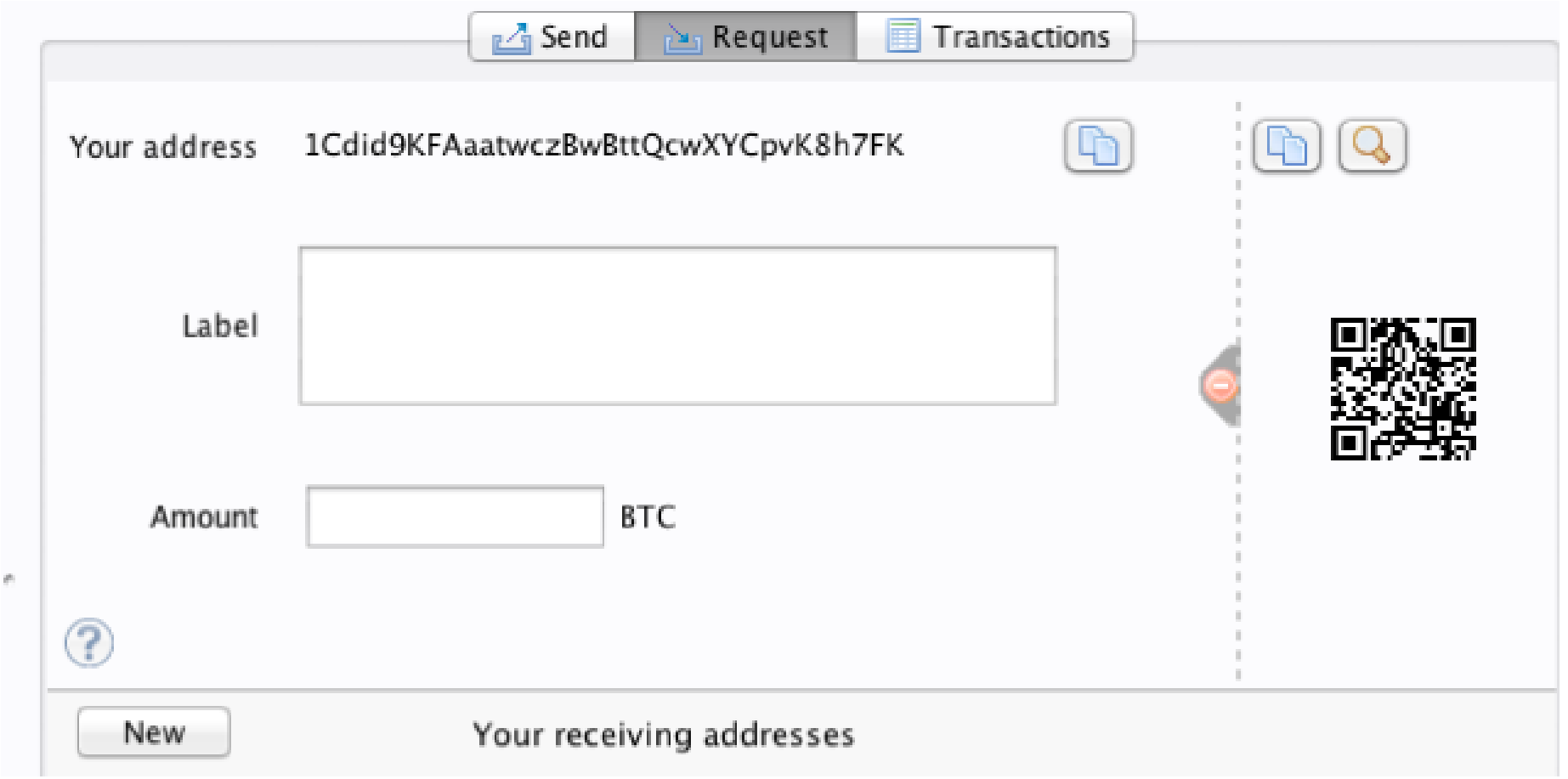
- buy (form friend, local seller, ATM, bitcoin exchange)
- earn (by selling a product/service)

Start sending and receiving bitcoins

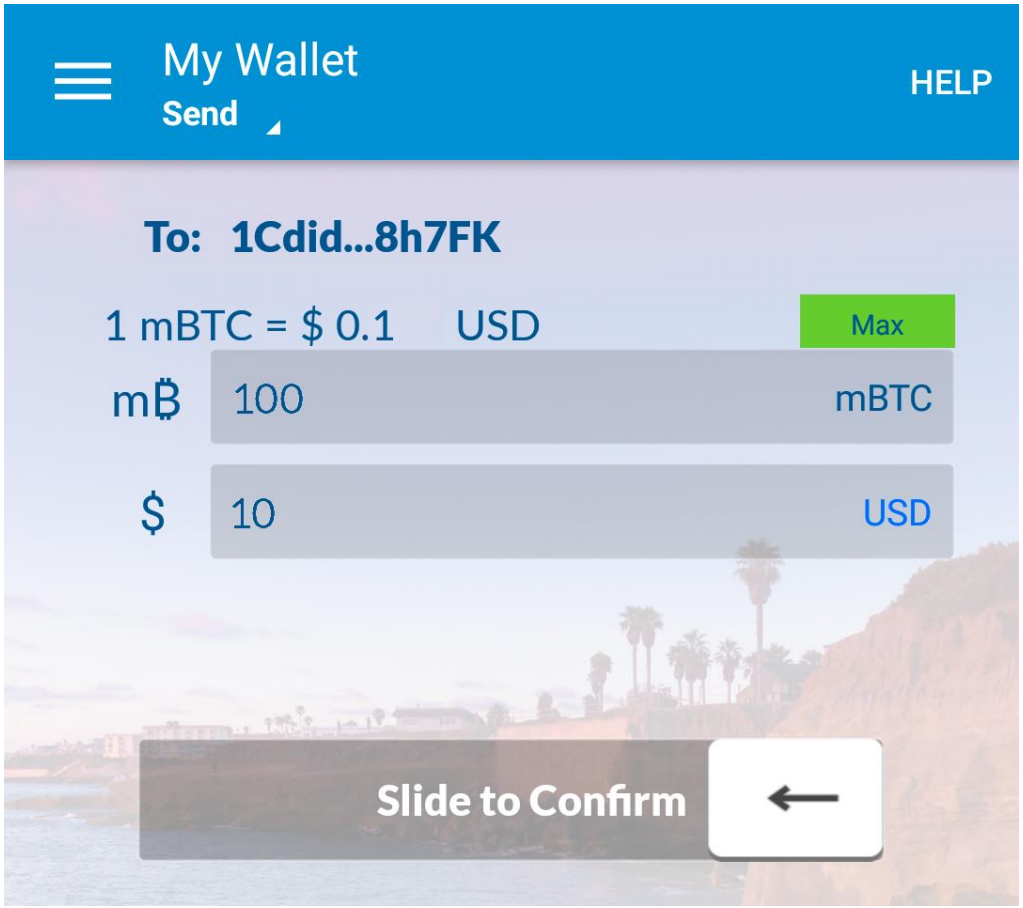
Bitcoin wallet



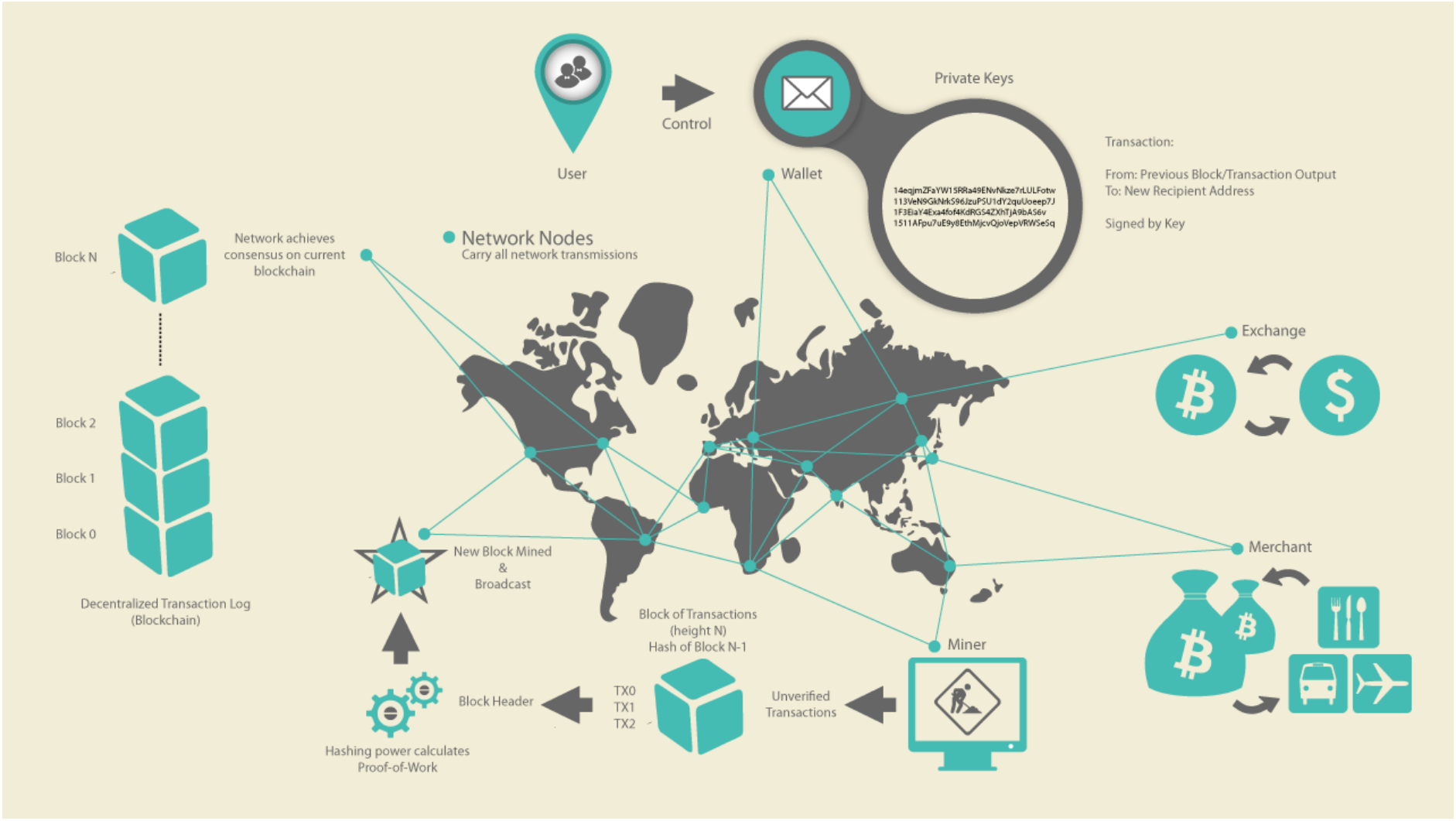
Bitcoin wallet



Bitcoin wallet



Overview


User
Control
Private Keys
Wallet
14eqjmZFaYW15RRa49ENvNkze7rLULFotw
113VeN9GkNrkS96JzuPSU1dY2quUoeep7J
1F3EiaY4Exa4fof4KdRGS4ZXhTjA9bAS6v
1511AFpu7uE9y8EthMjcvQjoVepVRWSeSq
Transaction:
From: Previous Block/Transaction Output
To: New Recipient Address
Signed by Key
Block N
Network achieves consensus on current blockchain
Network Nodes
Carry all network transmissions
Exchange
Block 2
Block 1
Block 0
Decentralized Transaction Log (Blockchain)
New Block Mined & Broadcast
Merchant
Block of Transactions (height N) Hash of Block N-1
Miner
Block Header
TX0
TX1
TX2
Unverified Transactions
Hashing power calculates Proof-of-Work

Buy a cup of coffee

Payment request QR code:

Encodes the following:

- A bitcoin address: "1GdK9UzpHBzqzX2A9JFP3Di4weBwqgmoQA"
- The payment amount: "0.015"
- A label for the recipient address: "Bob's Cafe"
- A description for the payment: "Purchase at Bob's Cafe"

View Alice’s transaction on a block explorer site (blockchain.info):

https://blockchain.info/tx/0627052b6f28912f2703066a912ea577f2ce4da4caa5a5fbd8a57286c345c2f2

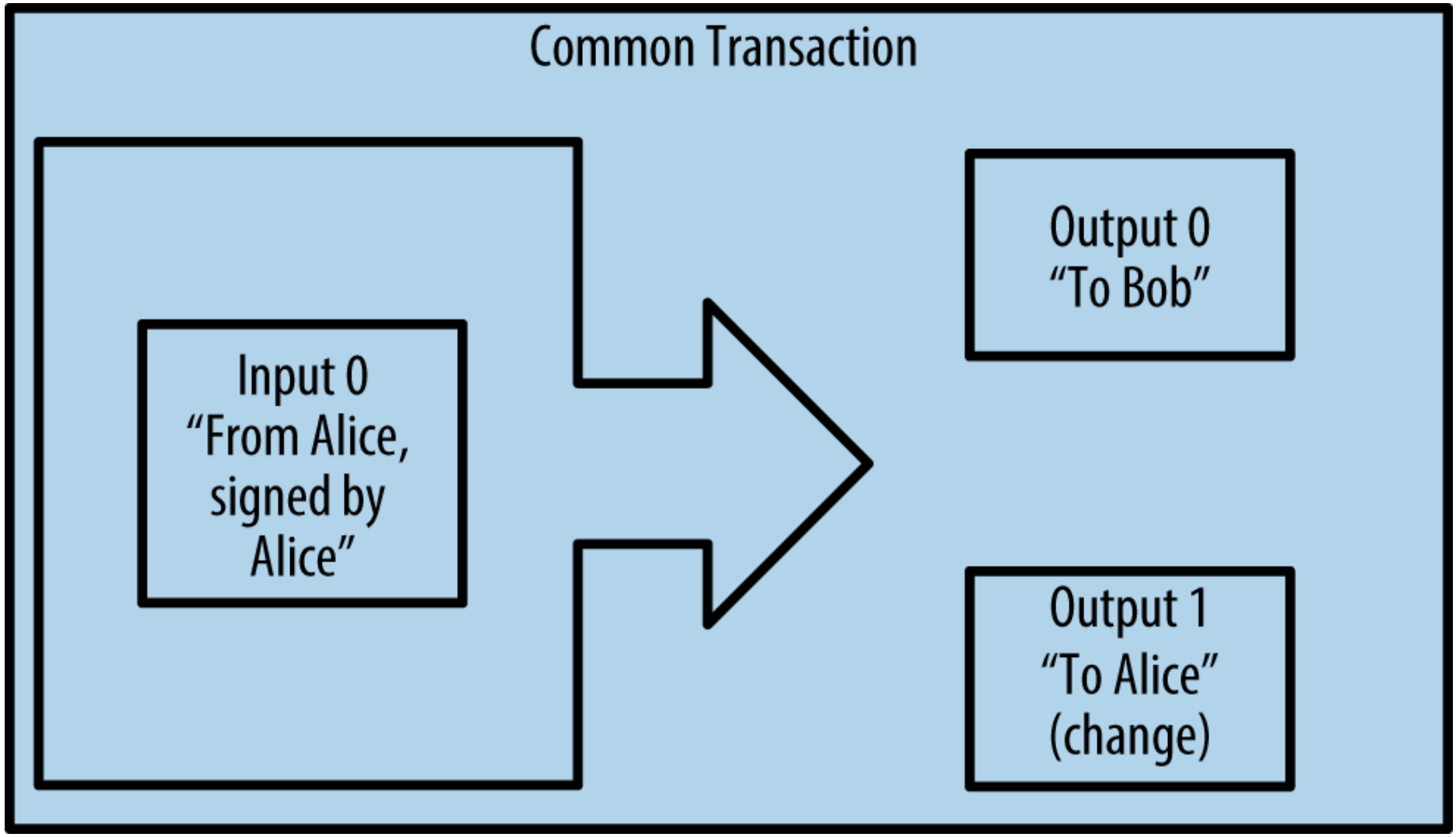
Transaction bookkeeping

Transaction as Double-Entry Bookkeeping

Inputs	Value	Outputs	Value
Input 1	0.10 BTC	Output 1	0.10 BTC
Input 2	0.20 BTC	Output 2	0.20 BTC
Input 3	0.10 BTC	Output 3	0.20 BTC
Input 4	0.15 BTC		
Total Inputs:	0.55 BTC	Total Outputs:	0.50 BTC

	Inputs	*0.55 BTC*
-	*Outputs*	*0.50 BTC*
	Difference	*0.05 BTC (implied transaction fee)*

Transaction1: pay + change



Pay and receive change

Transaction inputs cannot be divided.

If you buy an item that costs 5 bitcoin but only had a 20 bitcoin input to use:

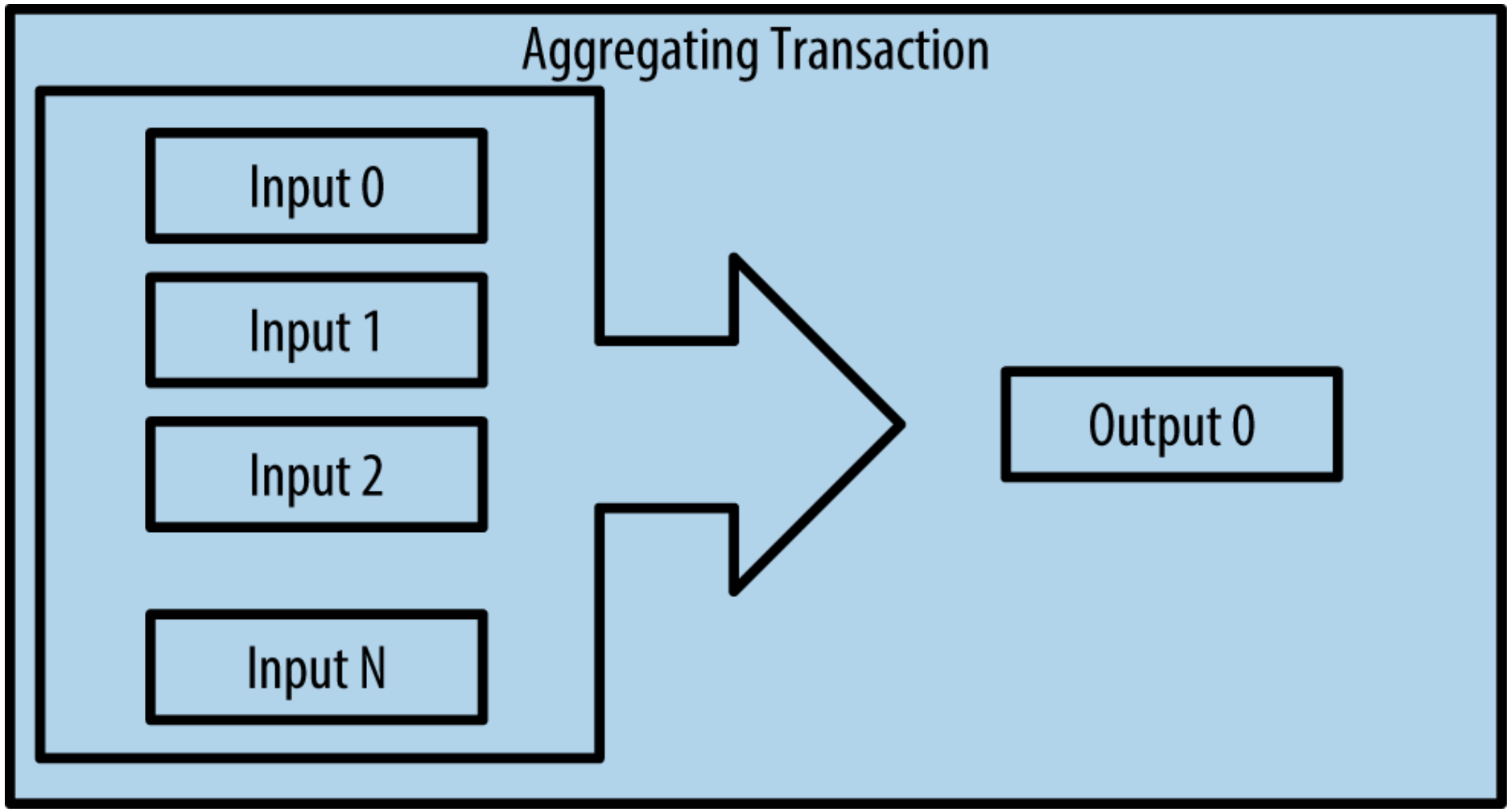
- you send one output of 5 bitcoin to the store owner and
- one output of 15 bitcoin back to yourself as change (or a little less: transaction fee)

Outputs add up to slightly less than inputs:

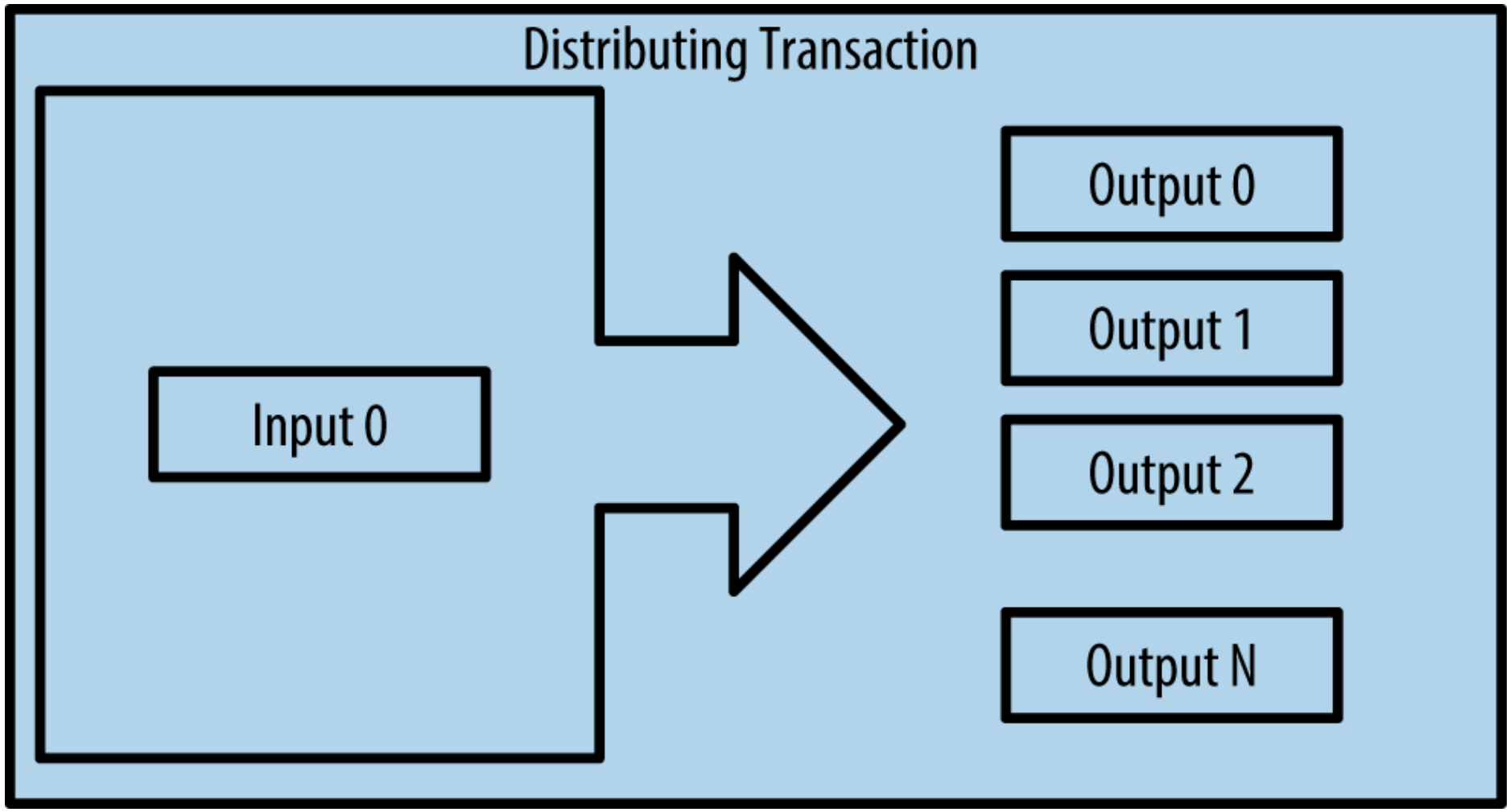
- the difference is the transaction fee, a small payment collected by the miner who includes the transaction in the ledger

Fees also serve as a security mechanism, by making it economically infeasible for attackers to flood the network with transactions.

Transaction2: clean up small amounts



Transaction3: multiple recipients



Create a transaction

Transaction View information about a bitcoin transaction

0627052b6f28912f2703066a912ea577f2ce4da4caa5a5fbd8a57286c345c2f2

1Cdid9KFAaatwczBwBttQcwXYCpvK8h7FK (0.1 BTC - Output)

1GdK9UzpHBzqzX2A9JFP3Di4weBwqgmoQA - (Unspent) 0.015 BTC

1Cdid9KFAaatwczBwBttQcwXYCpvK8h7FK - (Unspent) 0.0845 BTC

97 Confirmations | 0.0995 BTC

Summary	
Size	258 (bytes)
Received Time	2013-12-27 23:03:05
Included In Blocks	277316 (2013-12-27 23:11:54 +9 minutes)

Inputs and Outputs	
Total Input	0.1 BTC
Total Output	0.0995 BTC
Fees	0.0005 BTC
Estimated BTC Transacted	0.015 BTC

Find inputs

Keep track of your unspent coins:

- Full node wallet has all information
- Lightweight wallet keeps track of available outputs belonging to addresses in the wallet
- Or query the bitcoin network to retrieve this information

Look up all the unspent outputs for Alice's bitcoin address:

https://blockchain.info/unspent?active=1Cdid9KFAaatwczBwBttQcwXYCpvK8h7FK

Response includes:

- the reference to the transaction in which this unspent output is contained
- its value in satoshis (the smallest unit of the bitcoin currency, one hundred millionth of a single bitcoin, or 0.00000001 BTC)

Create outputs

First output: Payable to whoever can present a signature from the key corresponding to Bob's public address. This is Bob.

Second output: Change. Alice's wallet breaks her funds into two payments: one to Bob and one back to herself. She can then use (spend) the change output in a subsequent transaction.

For the transaction to be processed by the network in a timely fashion, Alice's wallet application will add a small fee. This is not explicit in the transaction; it is implied by the difference between inputs and outputs. The transaction fee is collected by the miner as a fee for validating and including the transaction in a block to be recorded on the blockchain.

The resulting transaction:

https://www.blockchain.com/btc/tx/0627052b6f28912f2703066a912ea577f2ce4da4caa5a5fbd8a57286c345c2f2

How the transaction propagates

The transaction contains all the information necessary to process, it does not matter how or where it is transmitted to the bitcoin network

The bitcoin network is a peer-to-peer network, with each bitcoin client participating by connecting to several other bitcoin clients. The purpose of the bitcoin network is to propagate transactions (and blocks) to all participants.

Any bitcoin node that receives a valid transaction it has not seen before will immediately forward it to all other nodes to which it is connected. This propagation technique is known as flooding. The transaction rapidly propagates out across the peer-to-peer network, reaching a large percentage of the nodes within a few seconds.

When the transaction (through other nodes) reaches Bob’s wallet, it checks for being an incoming transaction and verifies inputs. If the transaction is well formed, uses previously unspent inputs and contains sufficient transaction fees to be included in the next block, Bob can assume, with little risk, that the transaction will shortly be included in a block.

Small value transactions can be accepted without delay (a new block is created every 10 minutes).

Mining

The transaction (after propagation) becomes part of the blockchain by mining a new block.

The trust in bitcoin is based on computation. Mining a new block of transactions requires an enormous amount of computation, but the block can be easily verified. (like sudoku)

Mining nodes validate the transactions and receive mining reward (diminishes with time) plus the transaction fees.

The difficulty of mining is adjusted so that it takes approximately 10 minutes to find a solution.

The mining involves repeatedly hashing the header of the block and a random number with the SHA256 cryptographic algorithm until a solution matching a predetermined pattern emerges. Finding a solution (the so-called Proof-of-Work, or PoW) requires quadrillions of hashing operations per second across the entire bitcoin network. The first miner to find such a solution wins the round of competition and publishes that block into the blockchain.

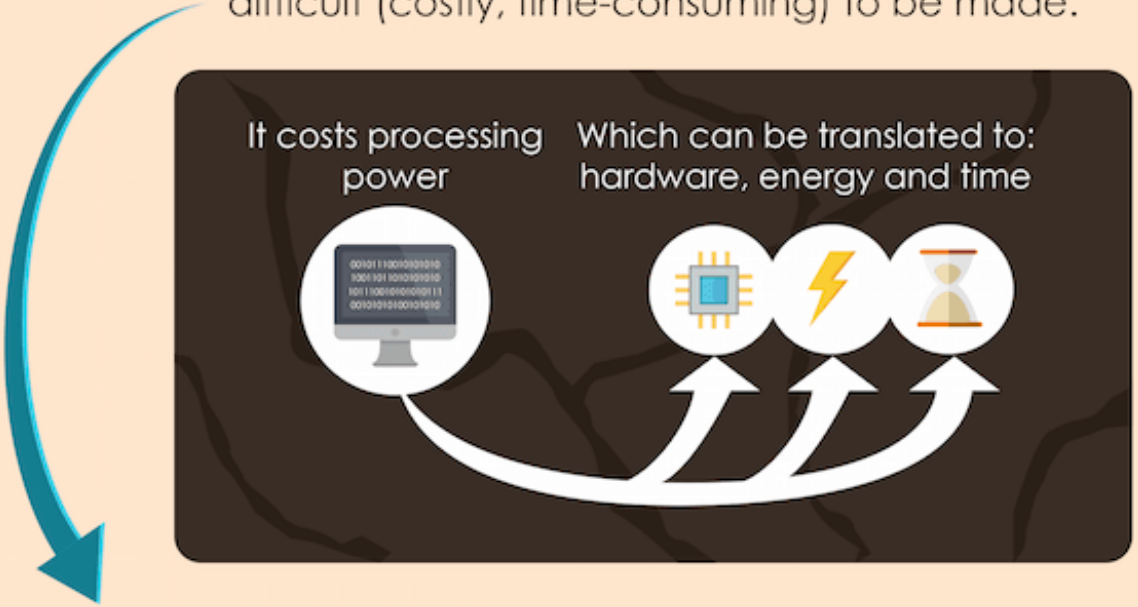
Proof of work

THE BITCOIN MINING SAGA - PART II

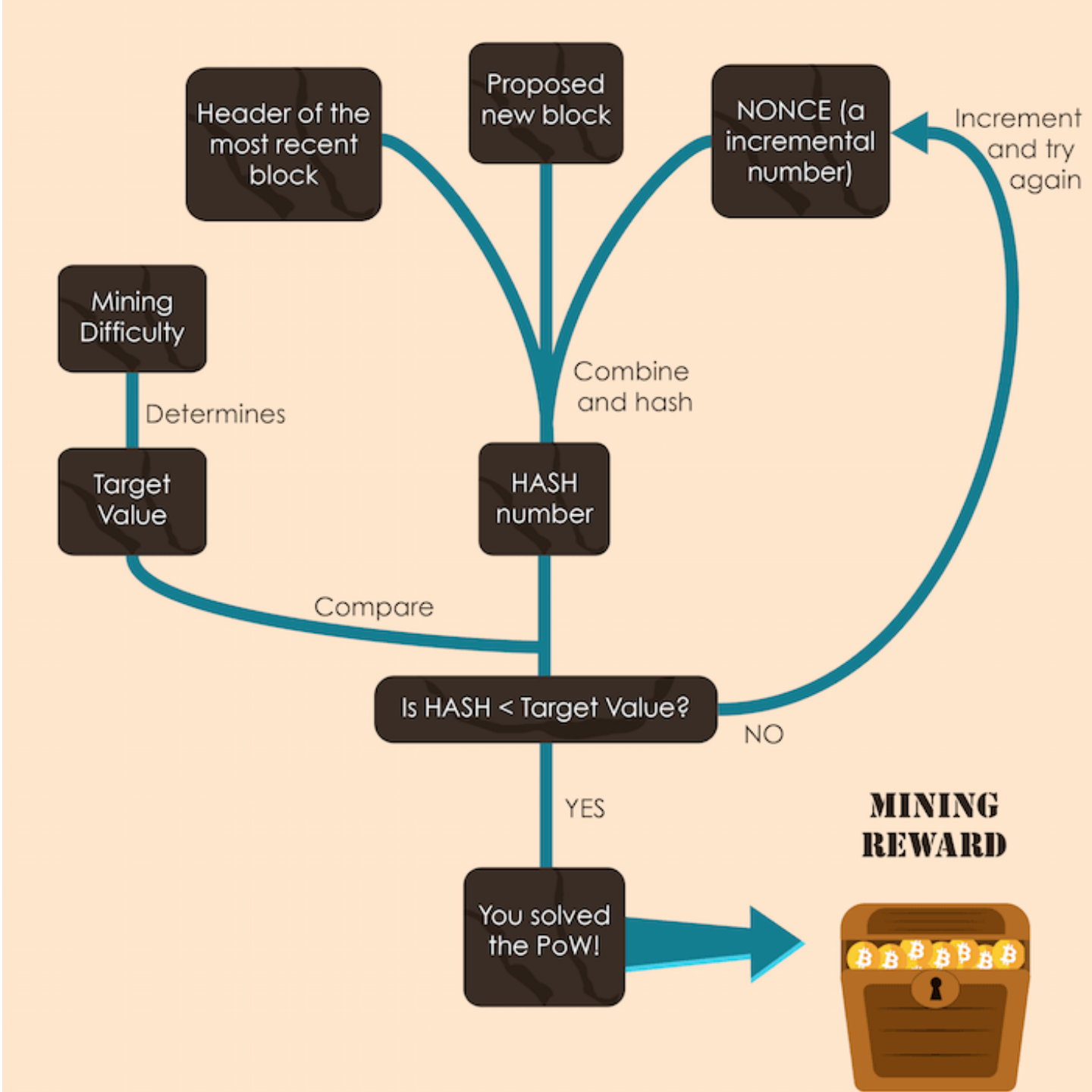
By Patrícia Estevão

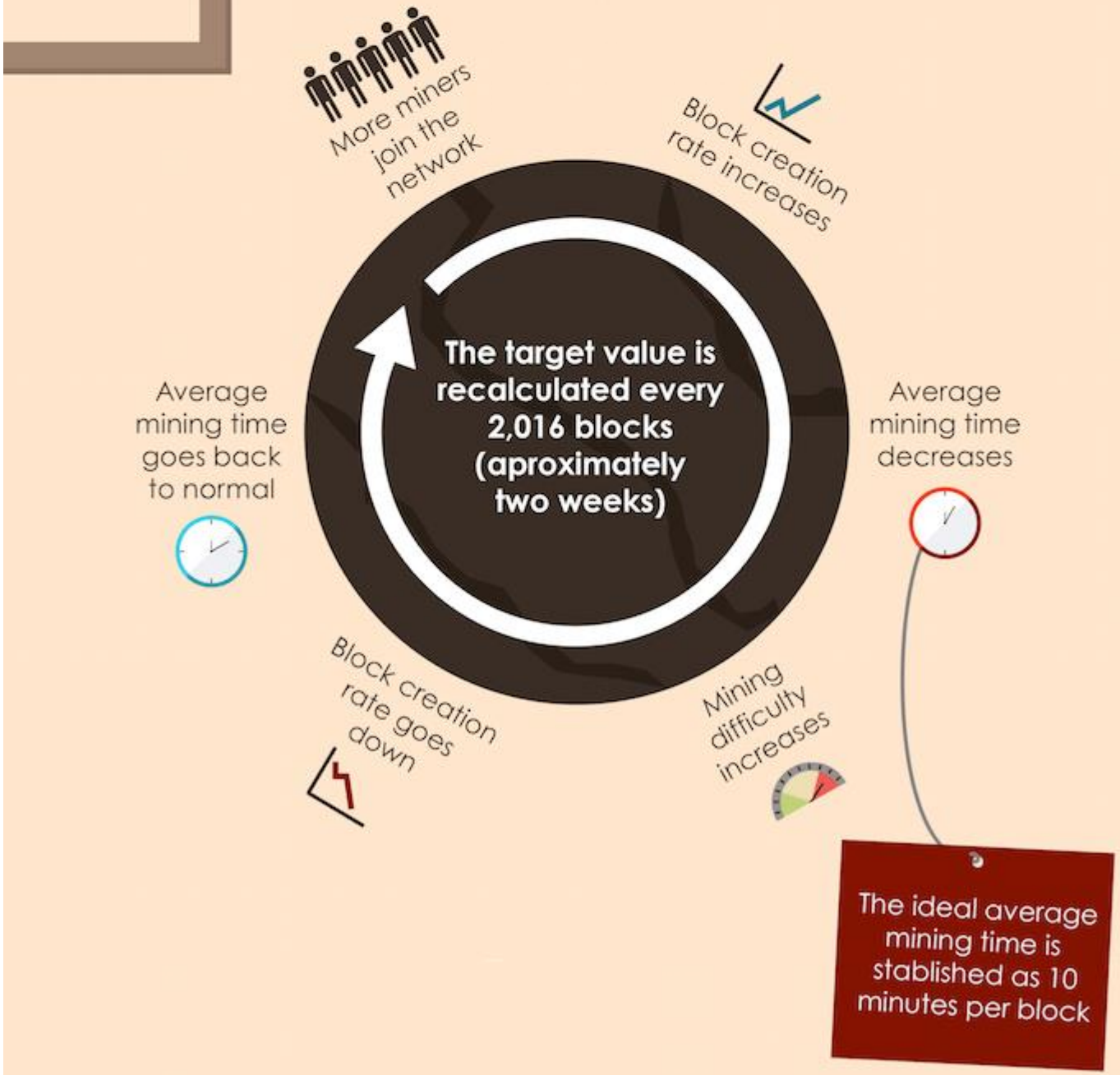
What is Proof of Work (PoW)?

It's a method to ensure that the information (the new block) was difficult (costly, time-consuming) to be made.

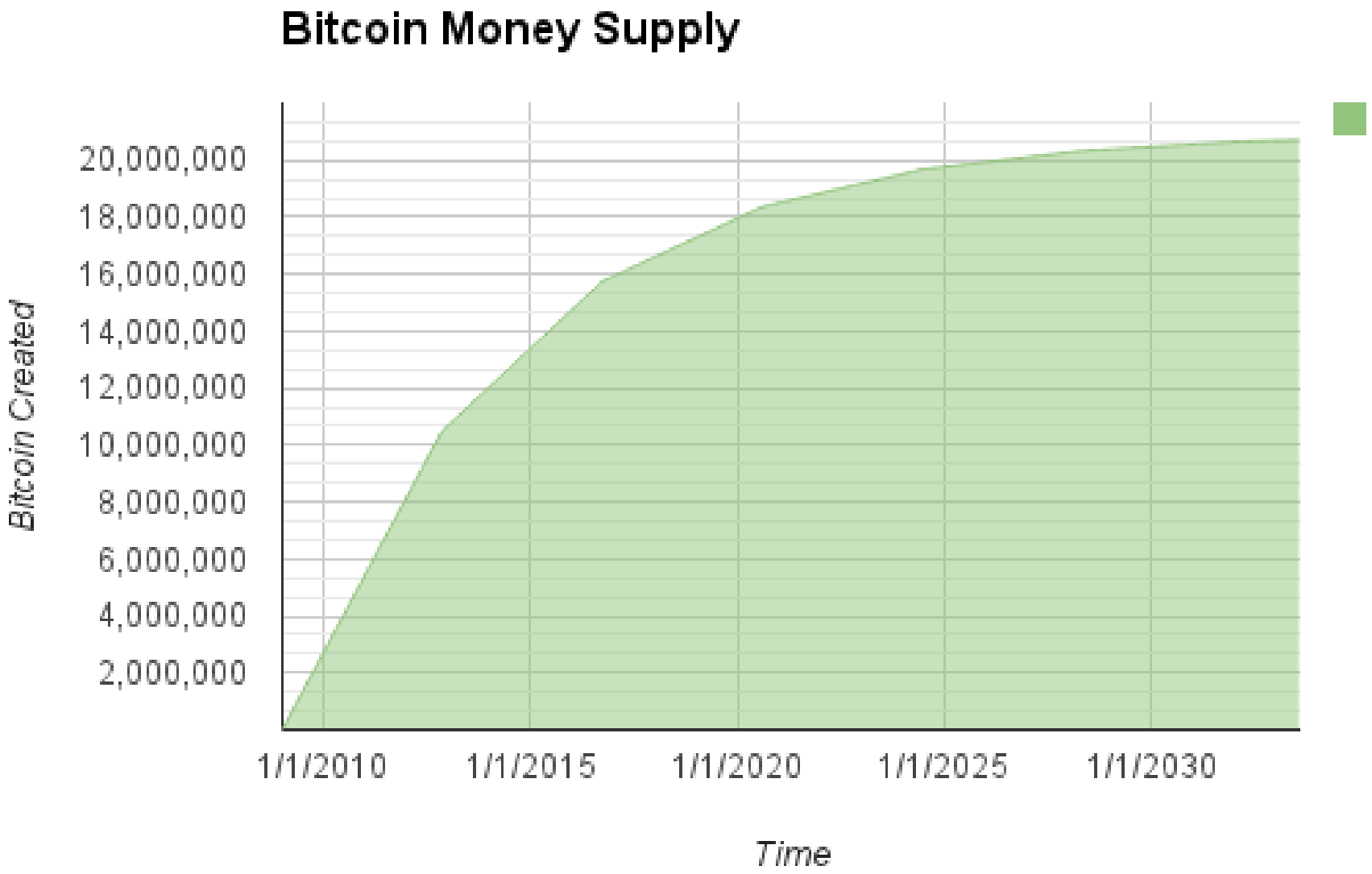


It's easy, on the other hand, for others to check if the requirements were met.

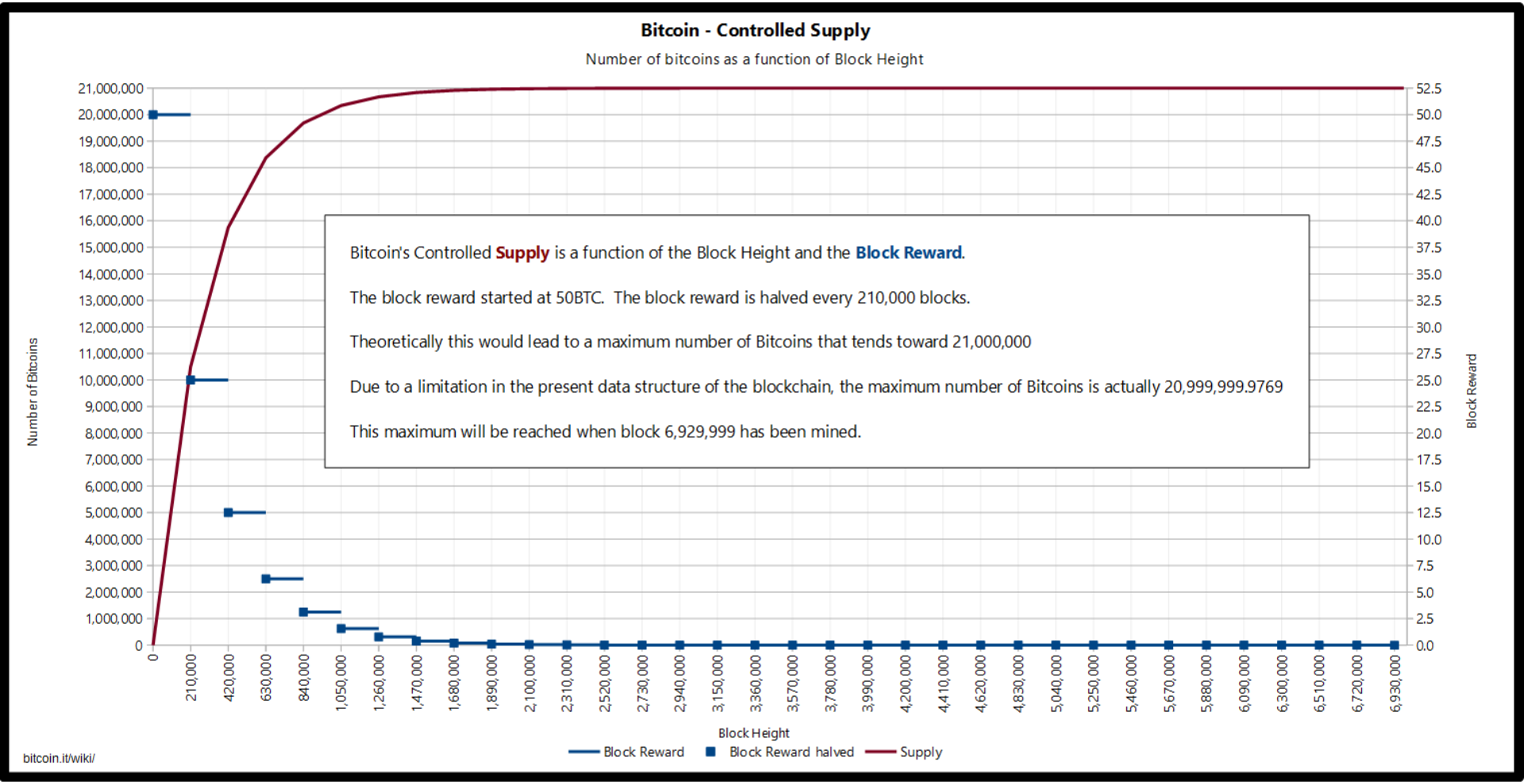

Header of the most recent block
Proposed new block
NONCE (a incremental number)
Increment and try again
Mining Difficulty
Determines
Combine and hash
Target Value
HASH number
Compare
Is HASH < Target Value?
NO
YES
MINING REWARD
You solved the PoW!


More miners join the network
Block creation rate increases
The target value is recalculated every 2,016 blocks (aproximately two weeks)
Average mining time goes back to normal
Average mining time decreases
Block creation rate goes down
Mining difficulty increases
The ideal average mining time is stablished as 10 minutes per block

Mining


Bitcoin Money Supply
20,000,000
18,000,000
16,000,000
14,000,000
12,000,000
10,000,000
8,000,000
6,000,000
4,000,000
2,000,000
Bitcoin Created
1/1/2010
1/1/2015
1/1/2020
1/1/2025
1/1/2030
Time

Mining



https://www.bitcoinblockhalf.com/

How the transaction becomes part of a block

Miners start the process of mining a new block of transactions as soon as they receive the previous block from the network.

New transactions are constantly flowing into the network, they get added to a temporary pool of unverified transactions maintained by each node.

Miners add unverified transactions (highest-fee first) from this pool to a new block, include a special transaction paying the block reward (currently 12.5 newly created bitcoin) plus the sum of transaction fees from all the transactions included in the block, and then attempt to mine the new block (candidate block).

The winning block becames part of the blockchain. The block containing Alice’s transaction is counted as one "confirmation" of that transaction.

The block that includes Alice’s transaction:

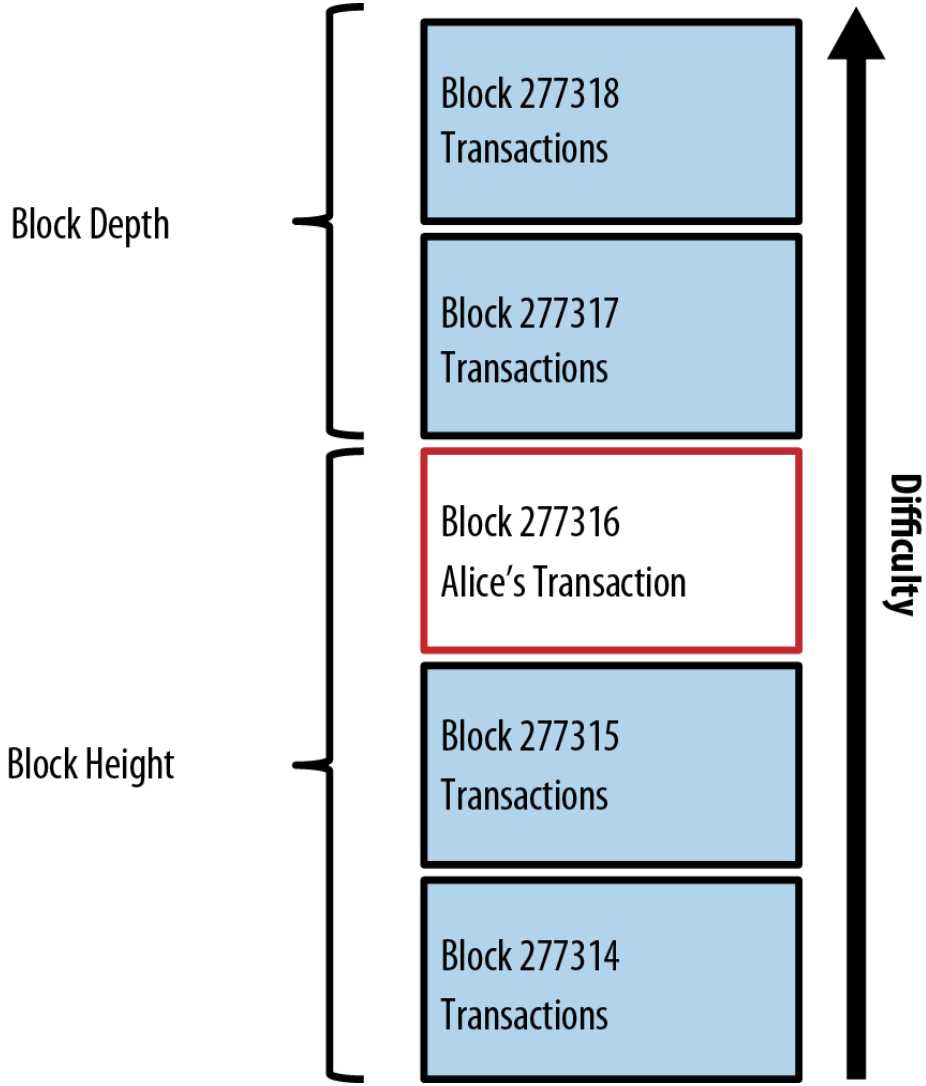
https://www.blockchain.com/btc/block/277316

How the transaction becomes part of a block

Later, a new block is mined by another miner. Because this new block is built on top of the block that contained Alice's transaction, it added even more computation to the blockchain, thereby strengthening the trust in those transactions.

Each block mined on top of the one containing the transaction counts as an additional confirmation for Alice's transaction. As the blocks pile on top of each other, it becomes exponentially harder to reverse the transaction, thereby making it more and more trusted by the network.

By convention, any block with more than six confirmations is considered irrevocable, because it would require an immense amount of computation to invalidate and recalculate six blocks.



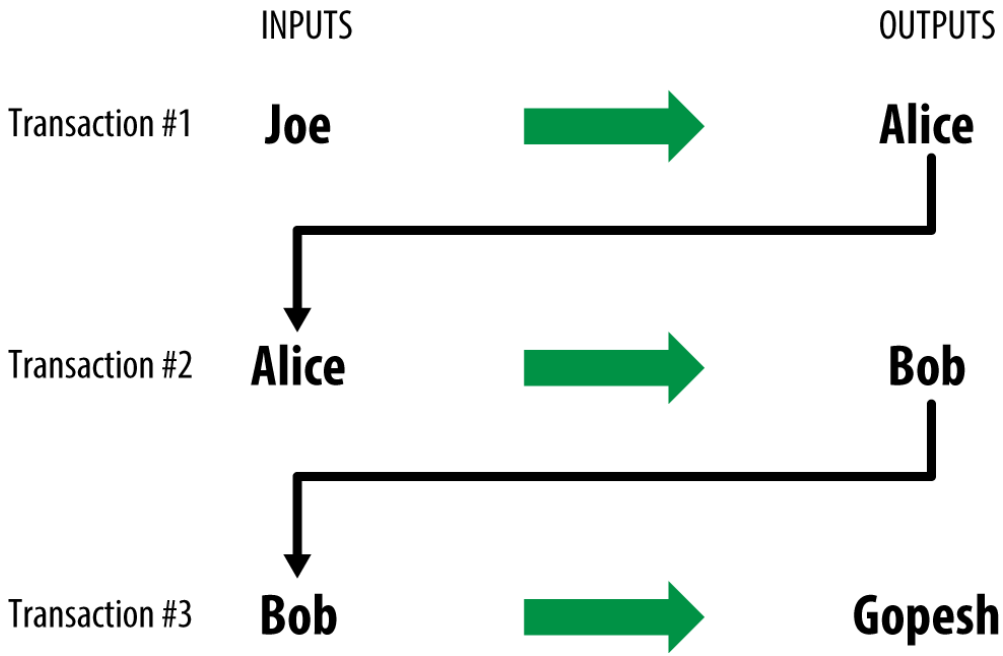
Valid and spendable transactions

As the transaction is embedded in the blockchain as part of a block, it is part of the distributed ledger of bitcoin and visible to all bitcoin applications. Each bitcoin client can independently verify the transaction as valid and spendable:

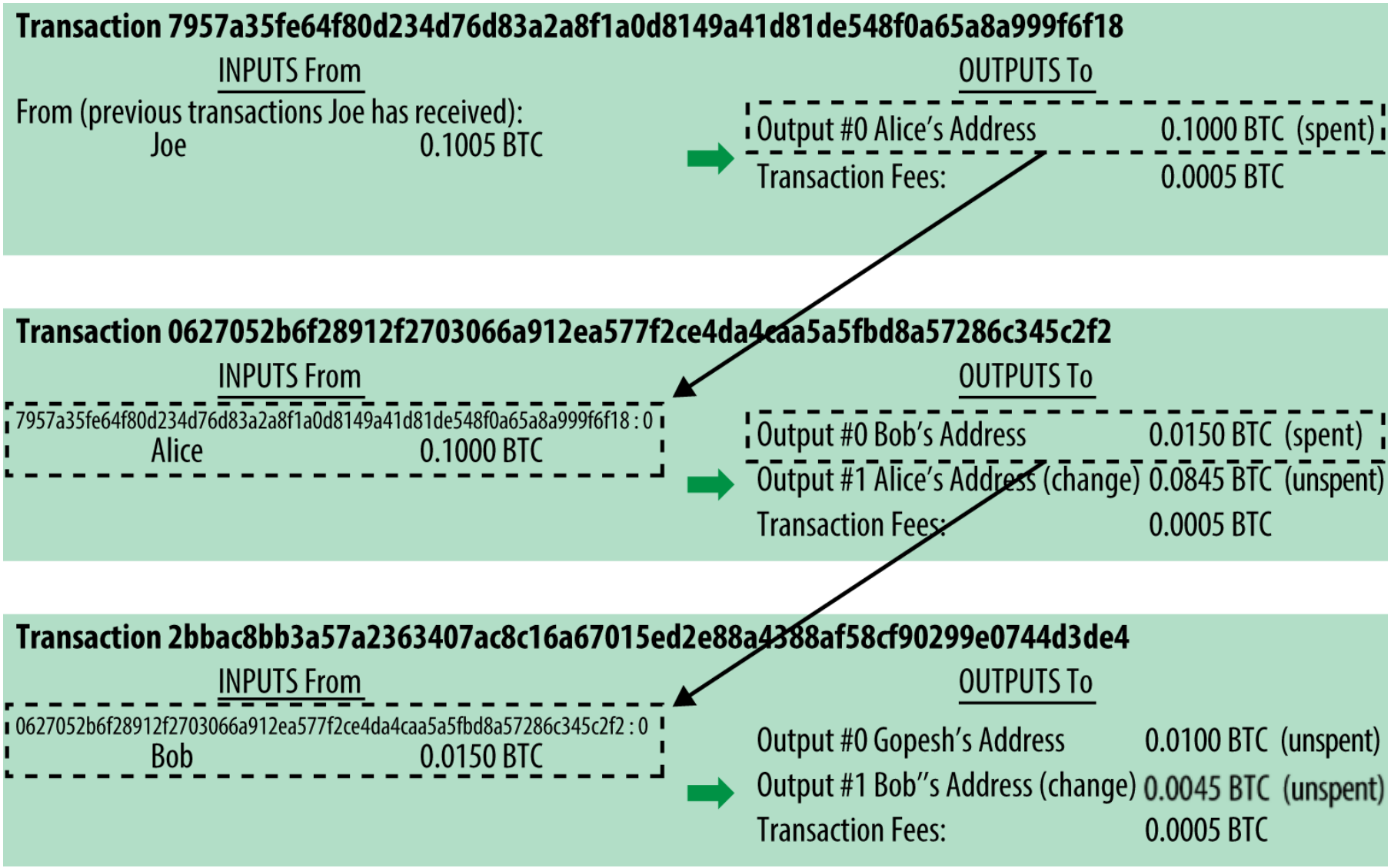
Full-node clients can track the source of the funds from the moment the bitcoin were first generated in a block, from transaction to transaction, until they reach the last transaction.

Lightweight clients can do a simplified payment verification: confirm that the transaction is in the blockchain and has several blocks mined after it.

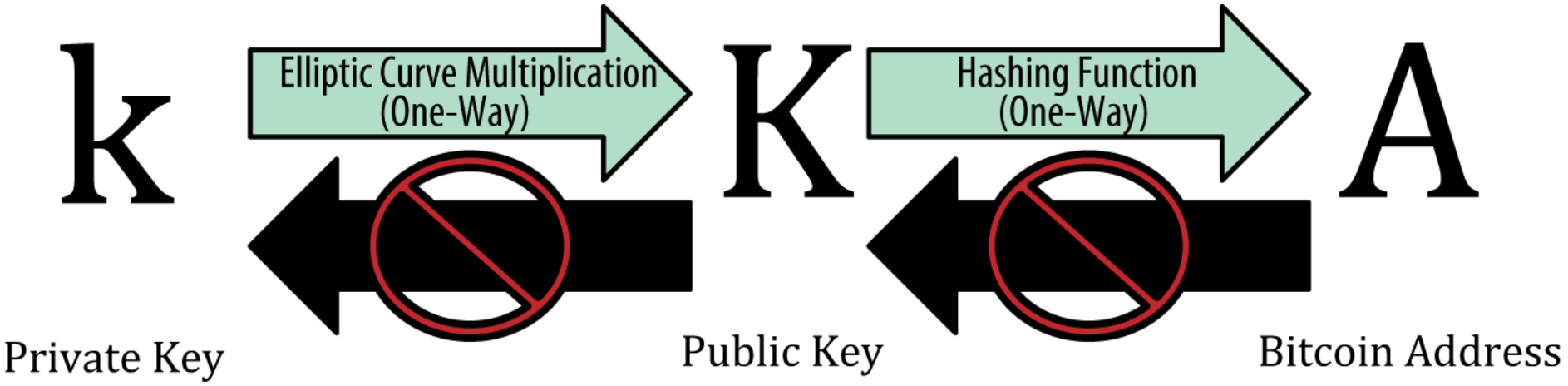
Bob can now spend the output from this and other spendable transactions:



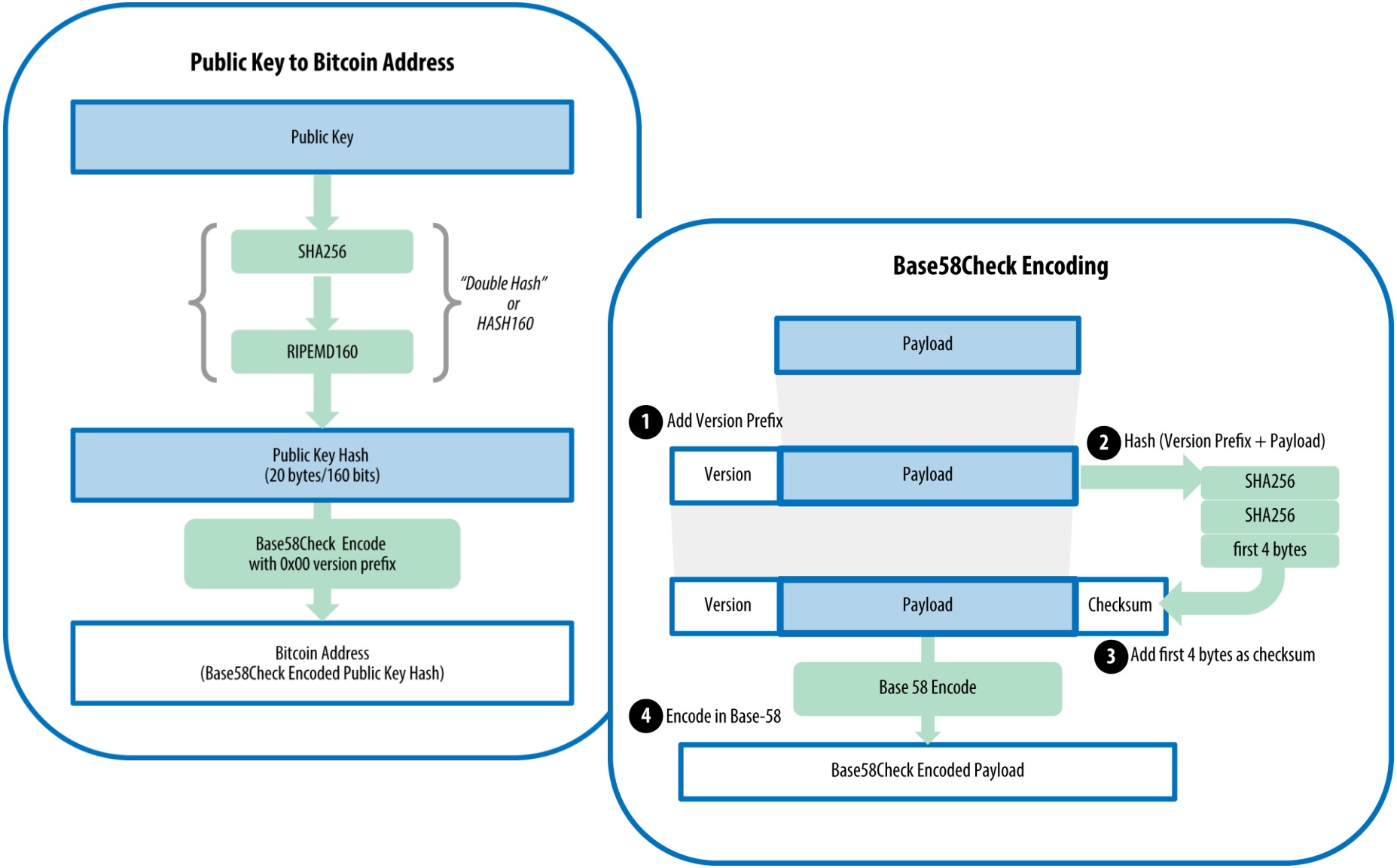
Transaction chain



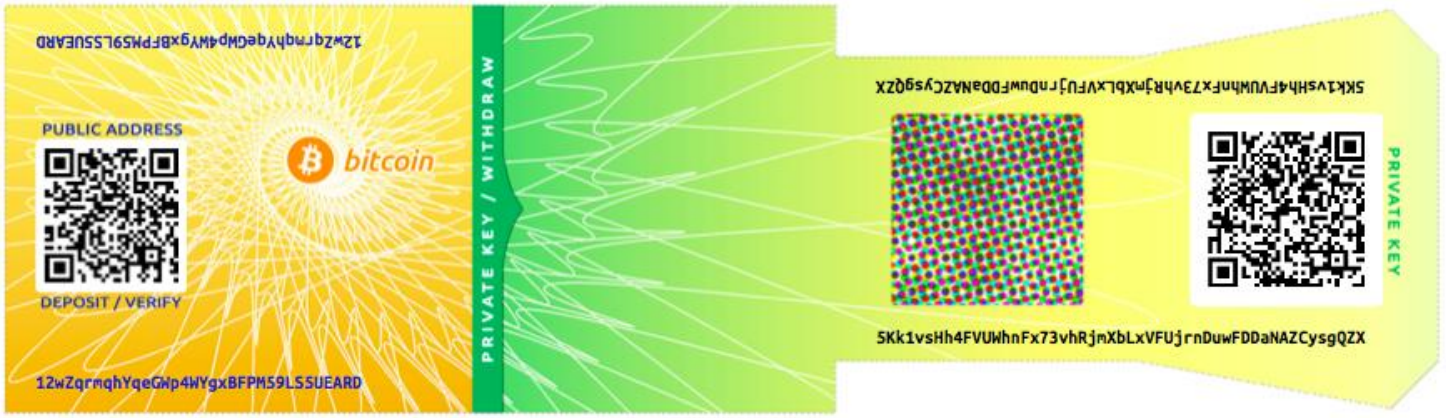
Key pair & Bitcoin address



Generate address



Private key backup ("paper wallet")



Transactions - behind the scenes

Alice's transaction:


```
{
  "version": 1,
  "locktime": 0,
  "vin": [
    {
      "txid": "7957a35fe64f80d234d76d83a2a8f1a0d8149a41d81de548f0a65a8a999f6f18",
      "vout": 0,
      "scriptSig" :
          "3045022100884d142d86652a3f47ba4746ec719bbfbd040a570b1deccbb6498c75c4ae24cb02204b9f039ff08df09cbe9f6addac960298cad530a8
          63ea8f53982c09db8f6e3813[ALL]
          0484ecc0d46f1918b30928fa0e4ed99f16a0fb4fde0735e7ade8416ab9fe423cc5412336376789d172787ec3457eee41c04f4938de5cc17b4a10fa3
          36a8d752adf",
      "sequence": 4294967295
    }
  ],
  "vout": [
    {
      "value": 0.01500000,
      "scriptPubKey": "OP_DUP OP_HASH160 ab68025513c3dbd2f7b92a94e0581f5d50f654e7 OP_EQUALVERIFY OP_CHECKSIG"
    },
    {
      "value": 0.08450000,
      "scriptPubKey": "OP_DUP OP_HASH160 7f9b1a7fb68d60c536c2fd8aeaa53a8f3cc025a8 OP_EQUALVERIFY OP_CHECKSIG",
    }
  ]
}
```

UTXO: unspent transaction outputs

Transaction outputs are indivisible chunks of bitcoin currency, recorded on the blockchain, and recognized as valid by the entire network.

Bitcoin full nodes track all available and spendable outputs, known as unspent transaction outputs, or UTXO.

The UTXO set grows as new UTXO is created and shrinks when UTXO is consumed. Every transaction represents a change (state transition) in the UTXO set.

When we say that a user’s wallet has "received" bitcoin, what we mean is that the wallet has detected an UTXO that can be spent with one of the keys controlled by that wallet.

A user’s bitcoin "balance" is the sum of all UTXO that user’s wallet can spend.

Transaction outputs

Transaction outputs consist of two parts:

- An amount of bitcoin, denominated in satoshis, the smallest bitcoin unit
- A cryptographic puzzle that determines the conditions required to spend the output

"vout": [
  {
    "value": 0.01500000,
    "scriptPubKey": "OP_DUP OP_HASH160 ab68025513c3dbd2f7b92a94e0581f5d50f654e7
      OP_EQUALVERIFY OP_CHECKSIG"
  },
  {
    "value": 0.08450000,
    "scriptPubKey": "OP_DUP OP_HASH160 7f9b1a7fb68d60c536c2fd8aeaa53a8f3cc025a8
      OP_EQUALVERIFY OP_CHECKSIG",
  }
]

Transaction inputs

Transaction inputs identify which UTXO will be consumed and provide proof of ownership.


```
"vin": [
  {
    "txid": "7957a35fe64f80d234d76d83a2a8f1a0d8149a41d81de548f0a65a8a999f6f18",
    "vout": 0,
    "scriptSig" :
      "3045022100884d142d86652a3f47ba4746ec719bbfbd040a570b1deccbb6498c75c4ae24cb02204b9f0
      39ff08df09cbe9f6addac960298cad530a863ea8f53982c09db8f6e3813[ALL]
      0484ecc0d46f1918b30928fa0e4ed99f16a0fb4fde0735e7ade8416ab9fe423cc5412336376789d172787
      ec3457eee41c04f4938de5cc17b4a10fa336a8d752adf",
    "sequence": 4294967295
  }
]
```


- transaction ID, referencing the transaction that contains the UTXO being spent
- output index, identifying which UTXO from that transaction is used (first one is zero)
- scriptSig, which satisfies the conditions placed on the UTXO, unlocking it for spending
- sequence number

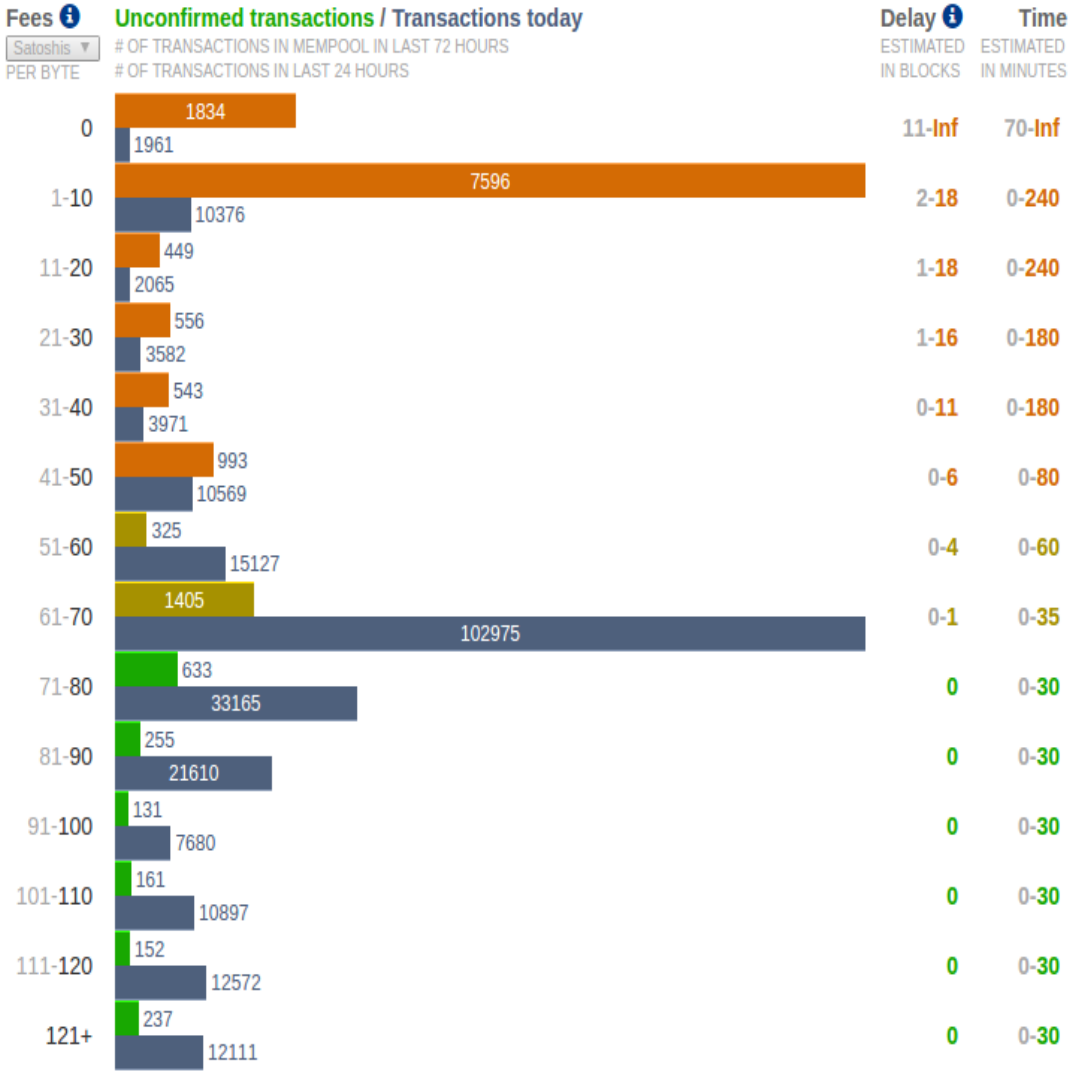
Fees ("keep the change")

Transaction fees serve as an incentive to include (mine) a transaction into the next block. Transaction fees are collected by the miner who mines the block that records the transaction on the blockchain.

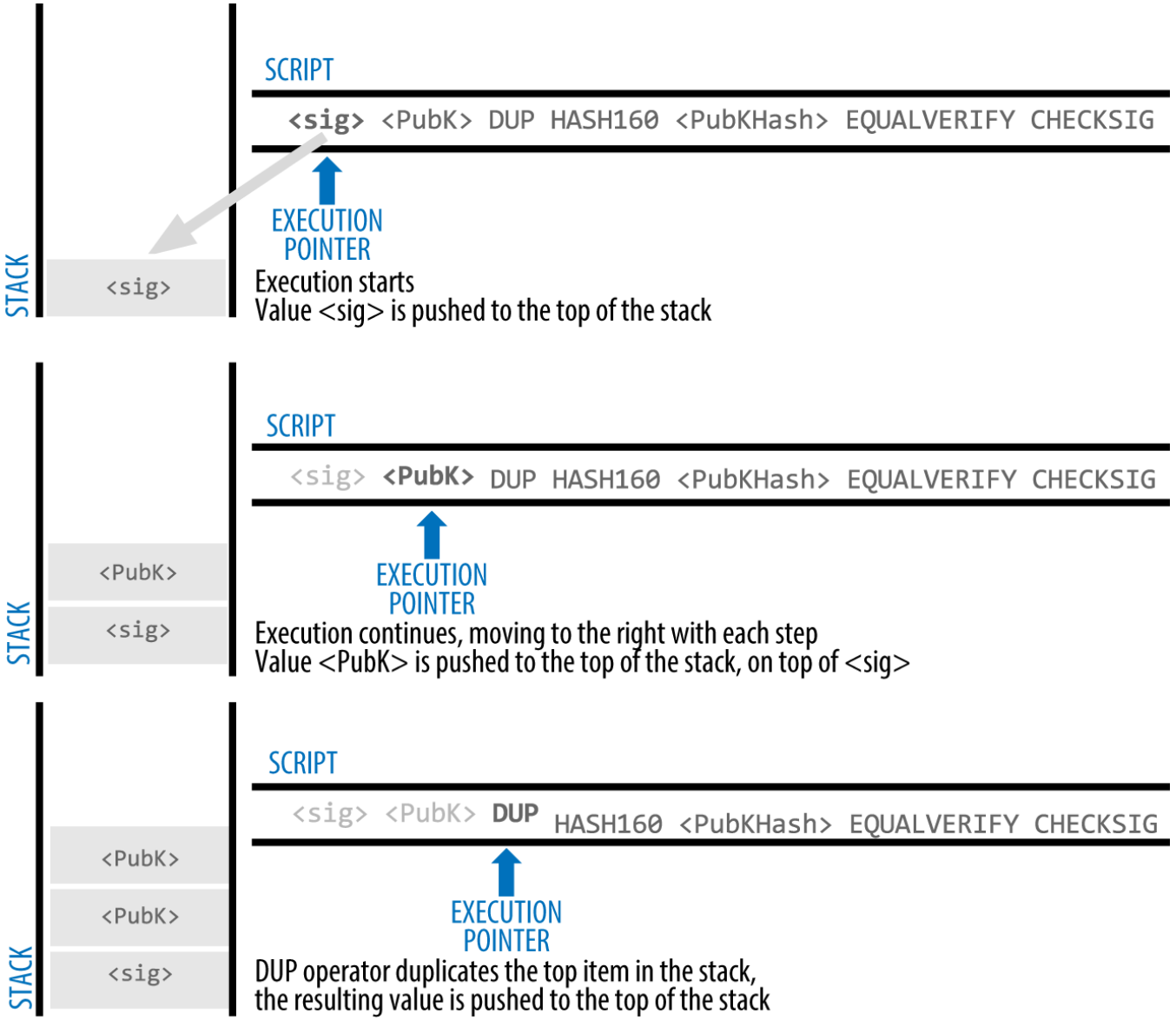
Also as a disincentive against abuse of the system by imposing a small cost on every transaction.

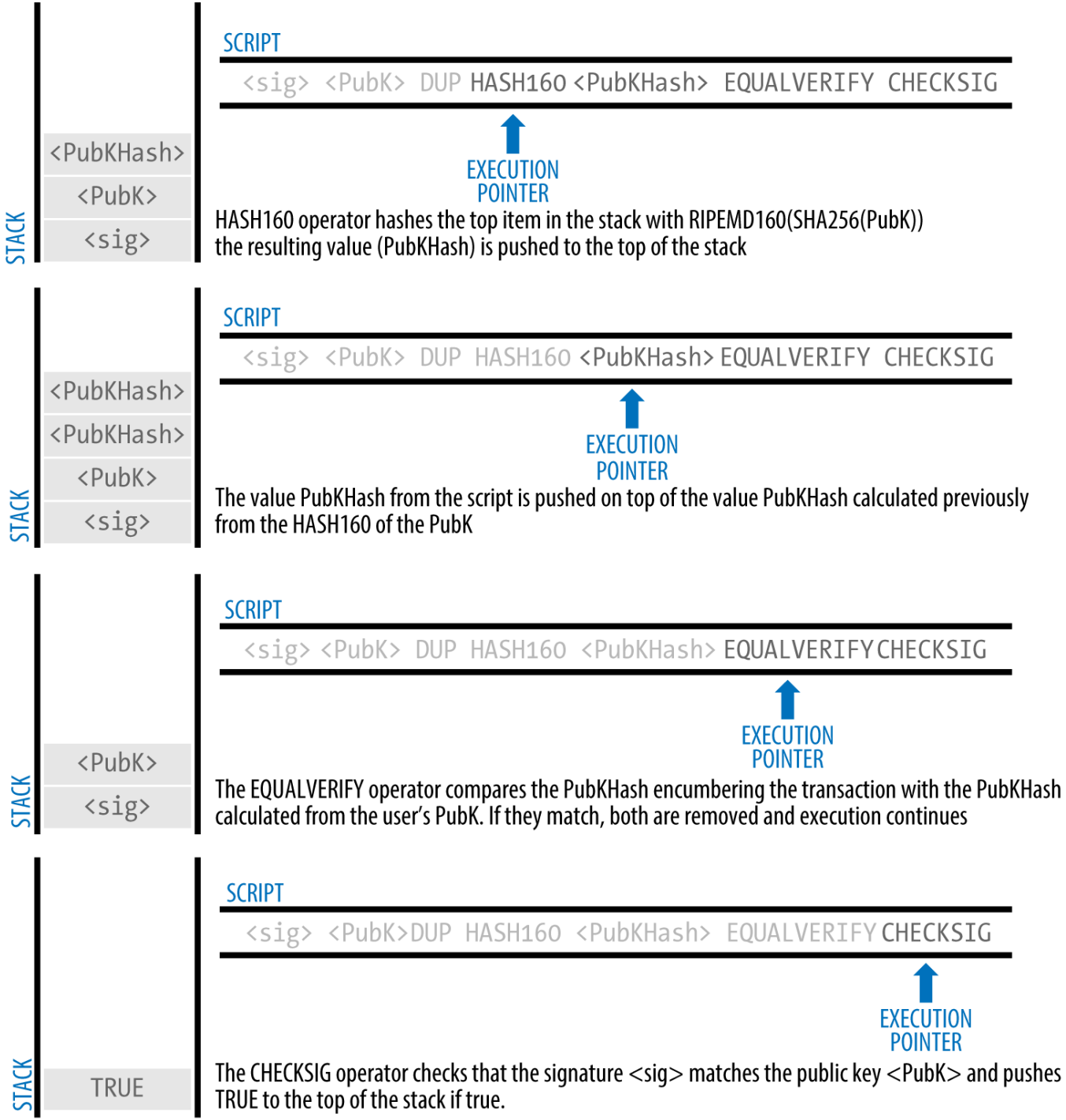
Transaction fees are calculated based on the size of the transaction in kilobytes, not the value of the transaction in bitcoin.

https://bitcoinfees.earn.com/



Script language




STACK
<PubKHash>
<PubK>
<sig>
SCRIPT
<sig> <PubK> DUP HASH160 <PubKHash> EQUALVERIFY CHECKSIG
EXECUTION POINTER
HASH160 operator hashes the top item in the stack with RIPEMD160(SHA256(PubK)) the resulting value (PubKHash) is pushed to the top of the stack
STACK
<PubKHash>
<PubKHash>
<PubK>
<sig>
SCRIPT
<sig> <PubK> DUP HASH160 <PubKHash> EQUALVERIFY CHECKSIG
EXECUTION POINTER
The value PubKHash from the script is pushed on top of the value PubKHash calculated previously from the HASH160 of the PubK
STACK
<PubK>
<sig>
SCRIPT
<sig> <PubK> DUP HASH160 <PubKHash> EQUALVERIFY CHECKSIG
EXECUTION POINTER
The EQUALVERIFY operator compares the PubKHash encumbering the transaction with the PubKHash calculated from the user's PubK. If they match, both are removed and execution continues
STACK
TRUE
SCRIPT
<sig> <PubK>DUP HASH160 <PubKHash> EQUALVERIFY CHECKSIG
EXECUTION POINTER
The CHECKSIG operator checks that the signature <sig> matches the public key <PubK> and pushes TRUE to the top of the stack if true.

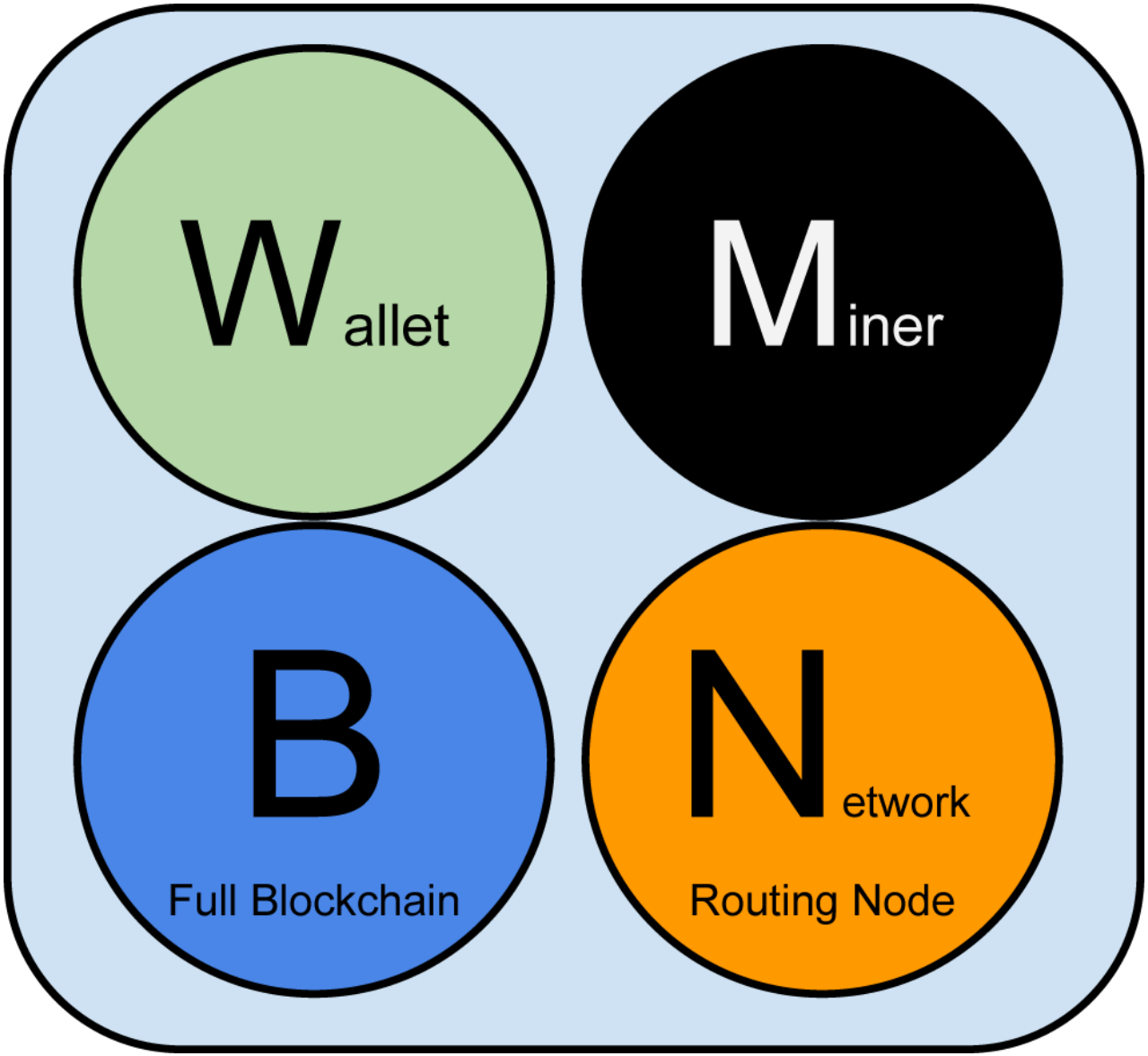
Transaction inputs

Transaction inputs identify which UTXO will be consumed and provide proof of ownership.

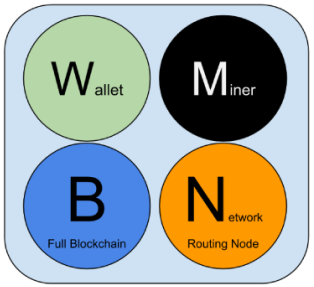

```
"vin": [
  {
    "txid": "7957a35fe64f80d234d76d83a2a8f1a0d8149a41d81de548f0a65a8a999f6f18",
    "vout": 0,
    "scriptSig" :
      "3045022100884d142d86652a3f47ba4746ec719bbfbd040a570b1deccbb6498c75c4ae24cb02204b9f0
      39ff08df09cbe9f6addac960298cad530a863ea8f53982c09db8f6e3813[ALL]
      0484ecc0d46f1918b30928fa0e4ed99f16a0fb4fde0735e7ade8416ab9fe423cc5412336376789d172787
      ec3457eee41c04f4938de5cc17b4a10fa336a8d752adf",
    "sequence": 4294967295
  }
]
```


- transaction ID, referencing the transaction that contains the UTXO being spent
- output index, identifying which UTXO from that transaction is used (first one is zero)
- scriptSig, which satisfies the conditions placed on the UTXO, unlocking it for spending
- sequence number (not used)

Bitcoin network node functions

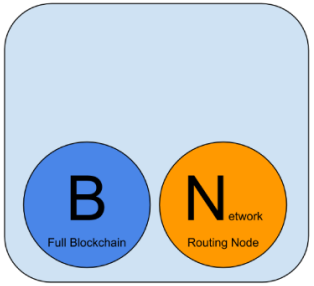


Bitcoin network node types



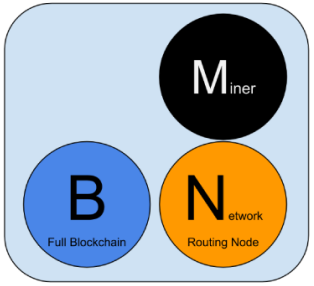
Reference Client (Bitcoin Core)

Contains a Wallet, Miner, full Blockchain database, and Network routing node on the bitcoin P2P network.



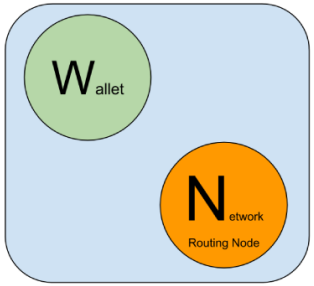
Full Block Chain Node

Contains a full Blockchain database, and Network routing node on the bitcoin P2P network.



Solo Miner

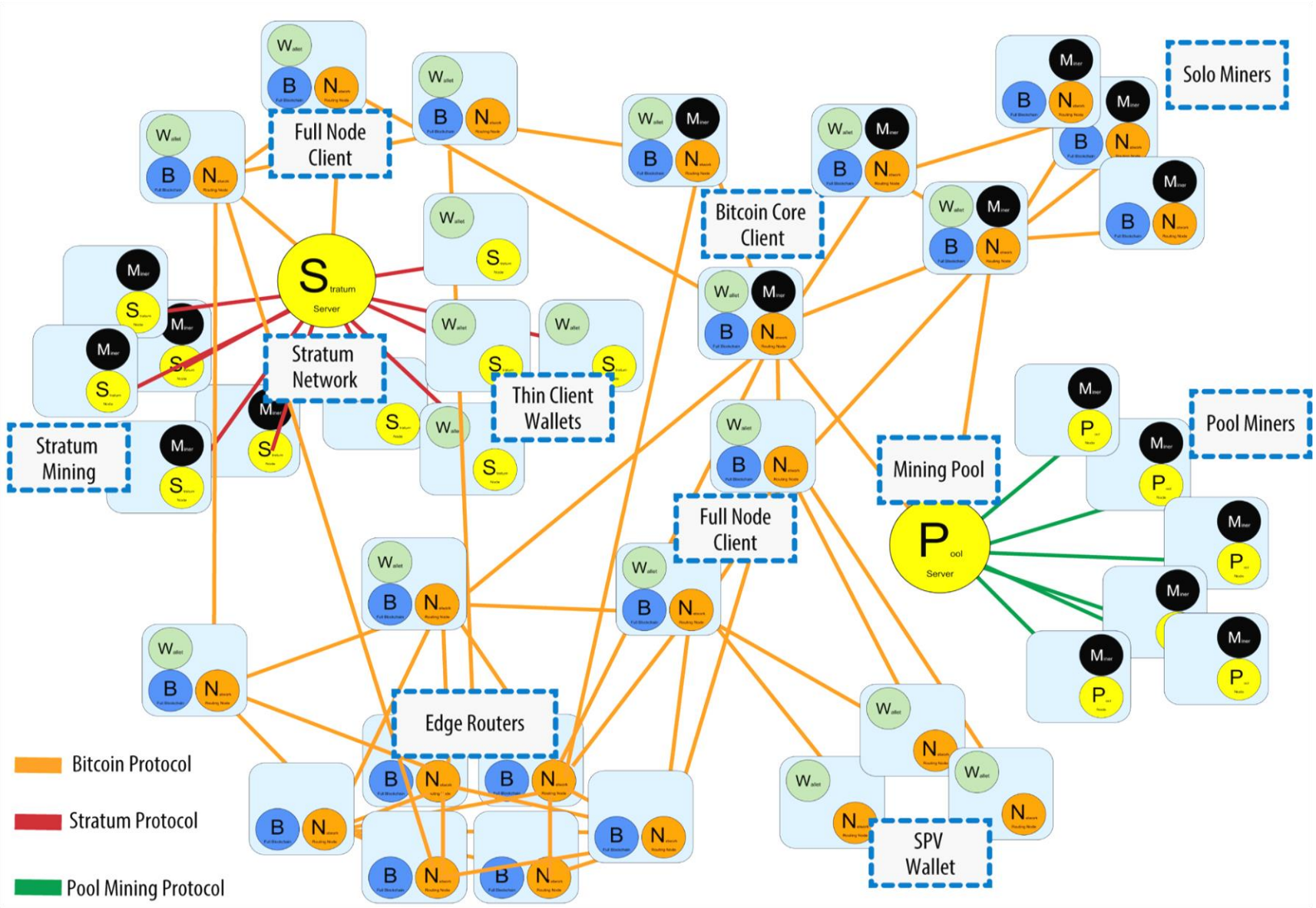
Contains a mining function with a full copy of the blockchain and a bitcoin P2P network routing node.



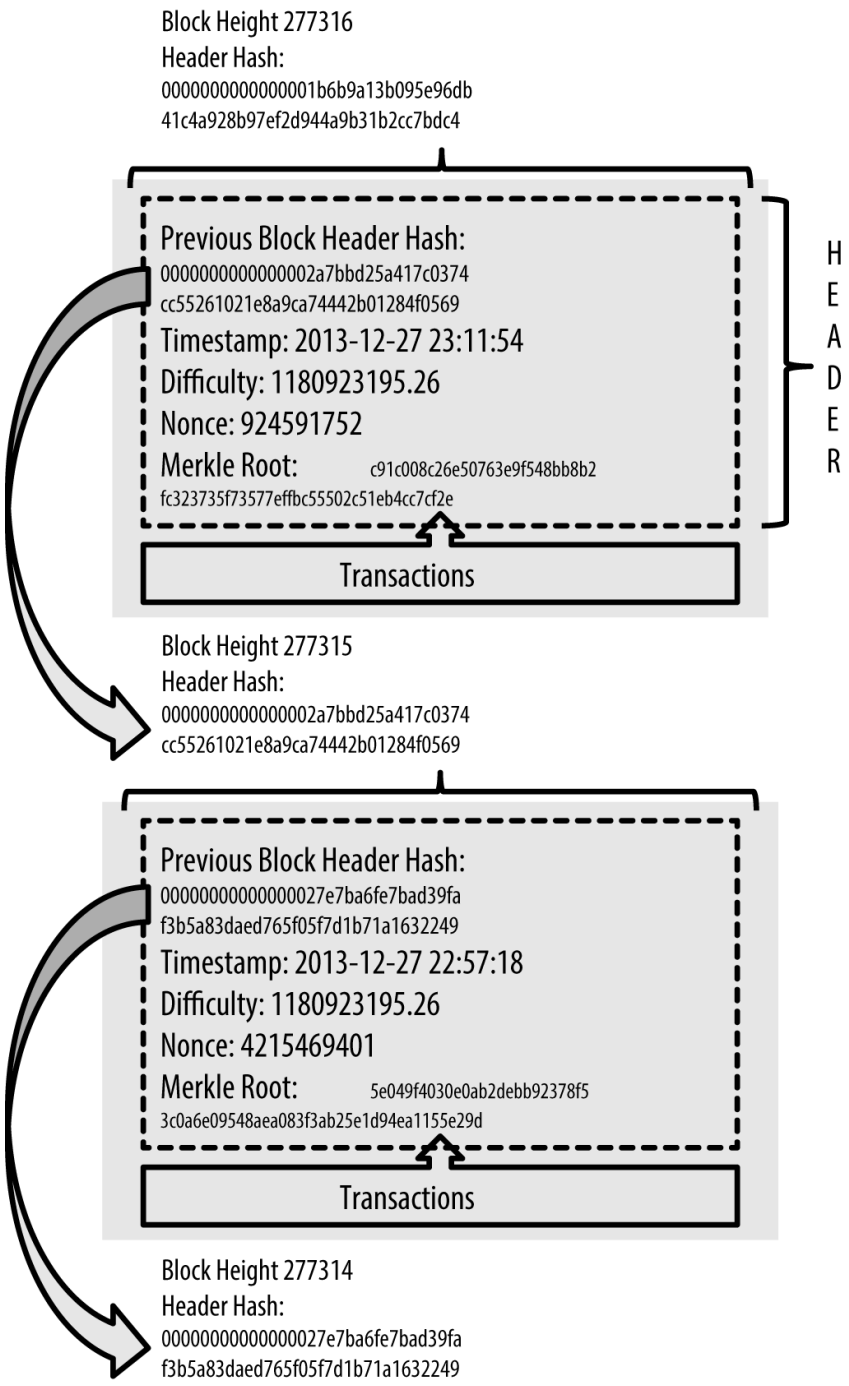
Lightweight (SPV) wallet

Contains a Wallet and a Network node on the bitcoin P2P protocol, without a blockchain.

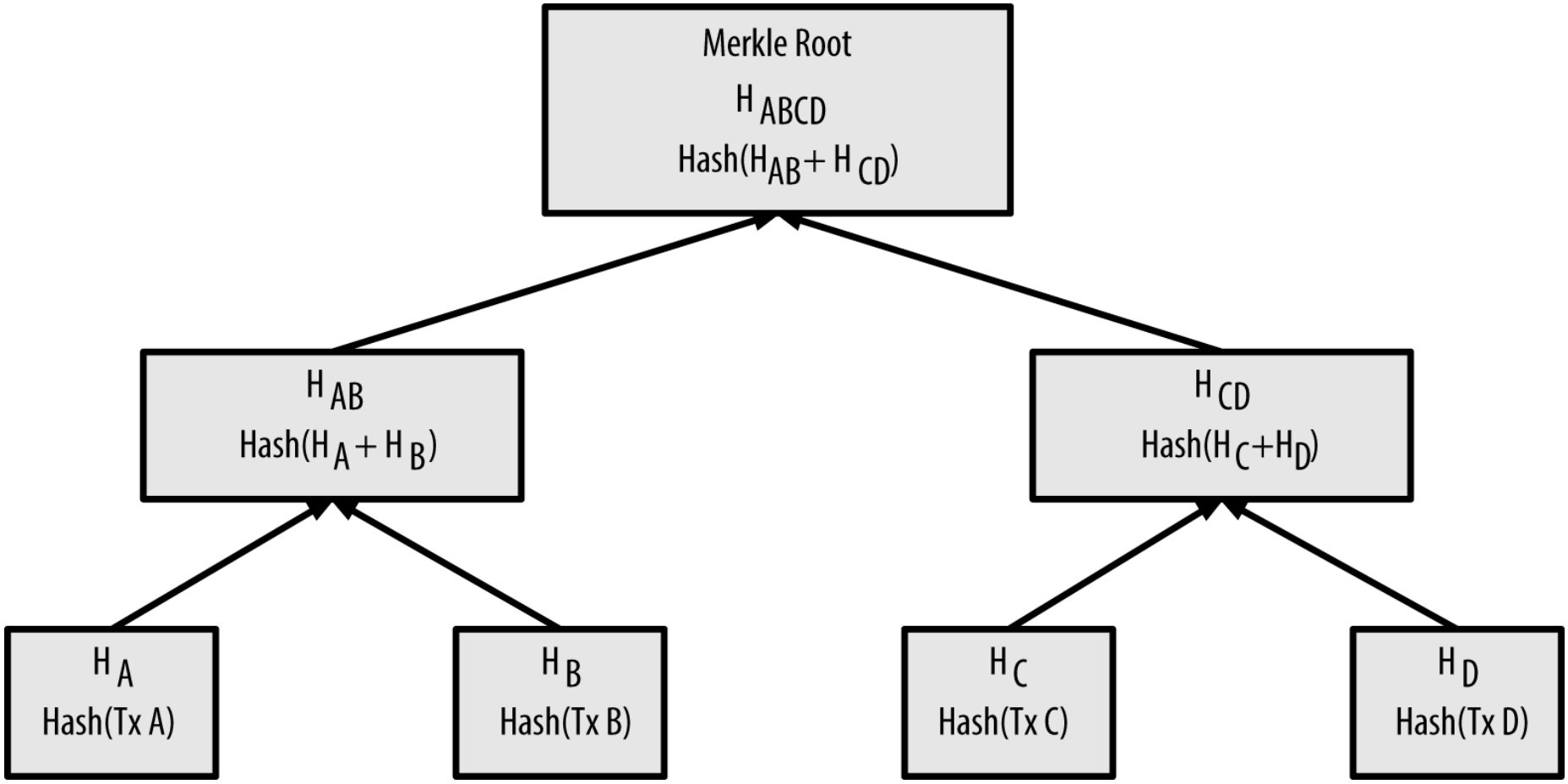
Bitcoin network



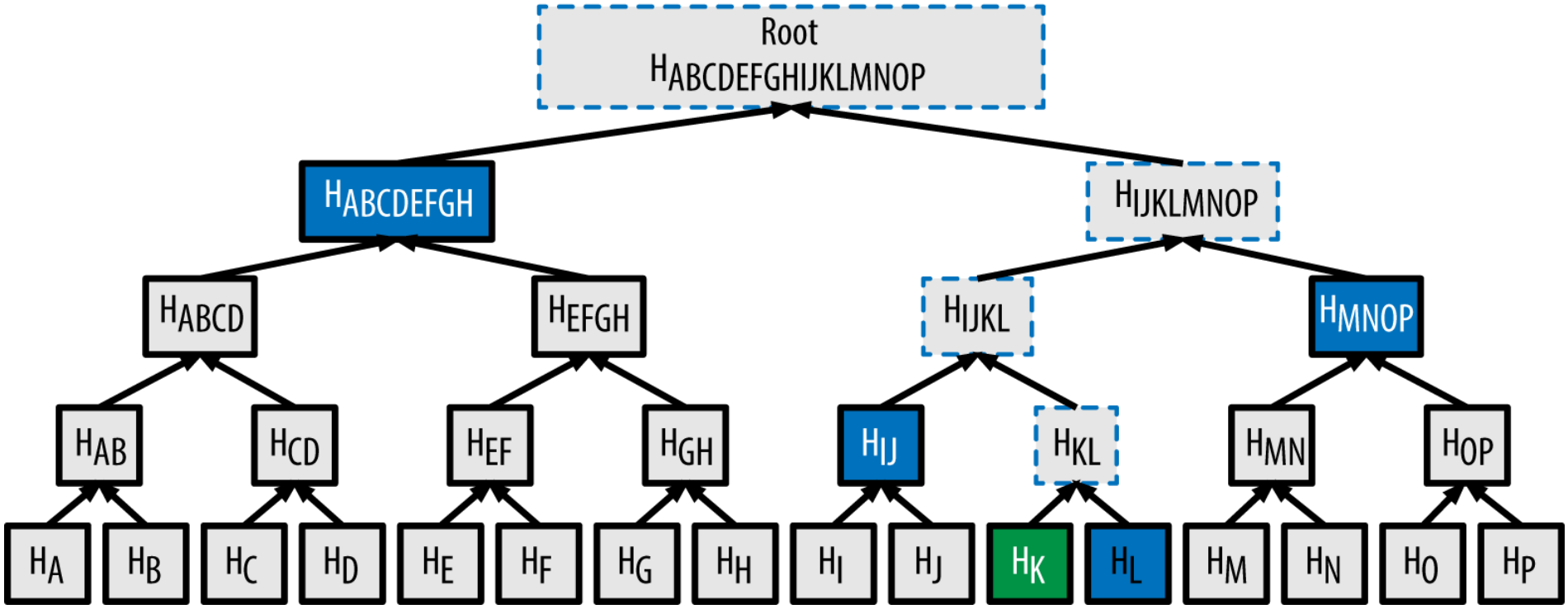
Blockchain


Block Height 277316
Header Hash:
000000000000000001b6b9a13b095e96db
41c4a928b97ef2d944a9b31b2cc7bdc4
Previous Block Header Hash:
000000000000000002a7bbd25a417c0374
cc55261021e8a9ca74442b01284f0569
Timestamp: 2013-12-27 23:11:54
Difficulty: 1180923195.26
Nonce: 924591752
Merkle Root: c91c008c26e50763e9f548bb8b2
fc323735f73577effbc55502c51eb4cc7cf2e
Transactions
HEADER
Block Height 277315
Header Hash:
000000000000000002a7bbd25a417c0374
cc55261021e8a9ca74442b01284f0569
Previous Block Header Hash:
000000000000000027e7ba6fe7bad39fa
f3b5a83daed765f05f7d1b71a1632249
Timestamp: 2013-12-27 22:57:18
Difficulty: 1180923195.26
Nonce: 4215469401
Merkle Root: 5e049f4030e0ab2debb92378f5
3c0a6e09548aea083f3ab25e1d94ea1155e29d
Transactions
Block Height 277314
Header Hash:
000000000000000027e7ba6fe7bad39fa
f3b5a83daed765f05f7d1b71a1632249

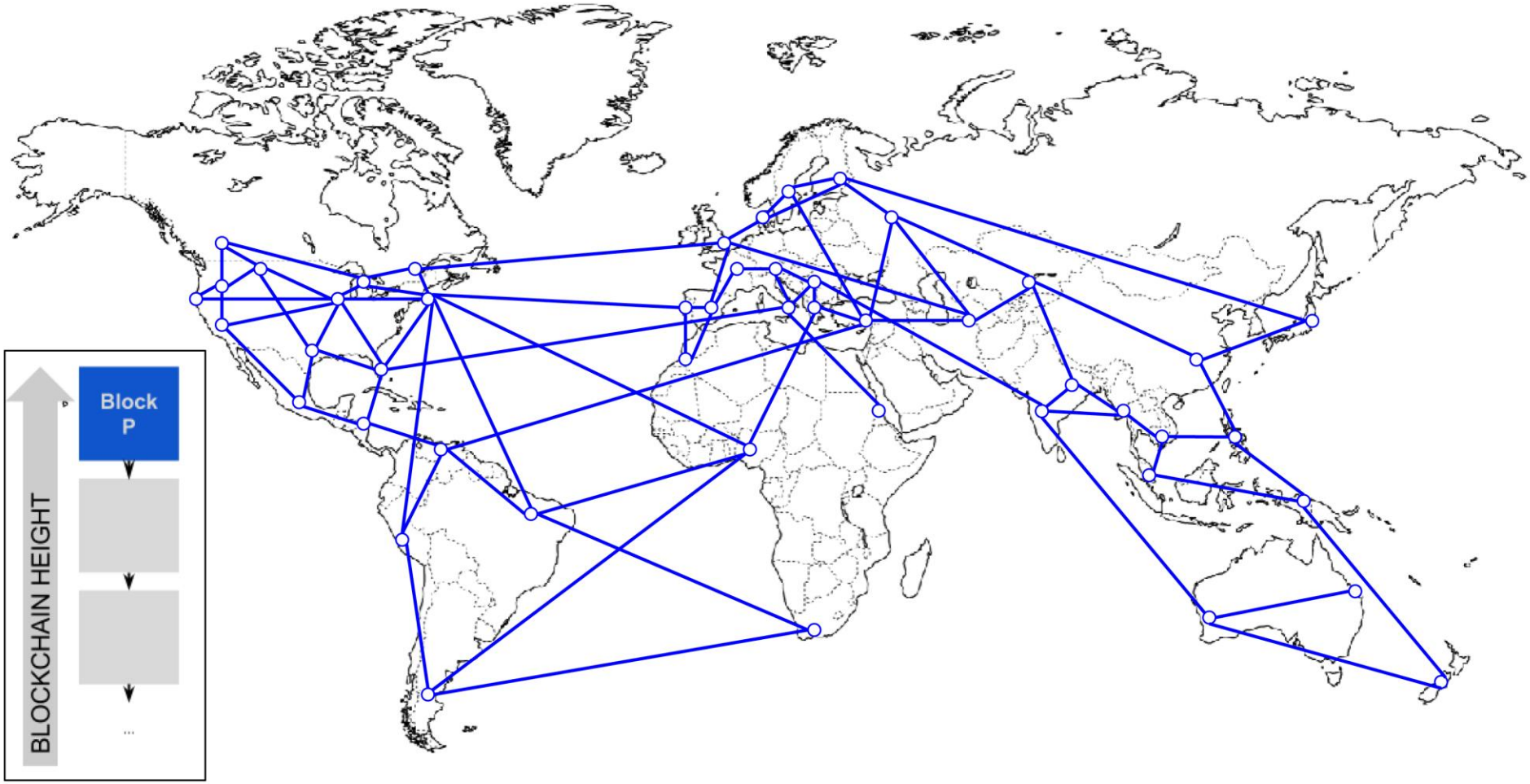
Merkle tree


Merkle Root
H ABCD
Hash(H AB + H CD)
H AB
Hash(H A + H B)
H CD
Hash(H C+H D)
H A
Hash(Tx A)
H B
Hash(Tx B)
H C
Hash(Tx C)
H D
Hash(Tx D)

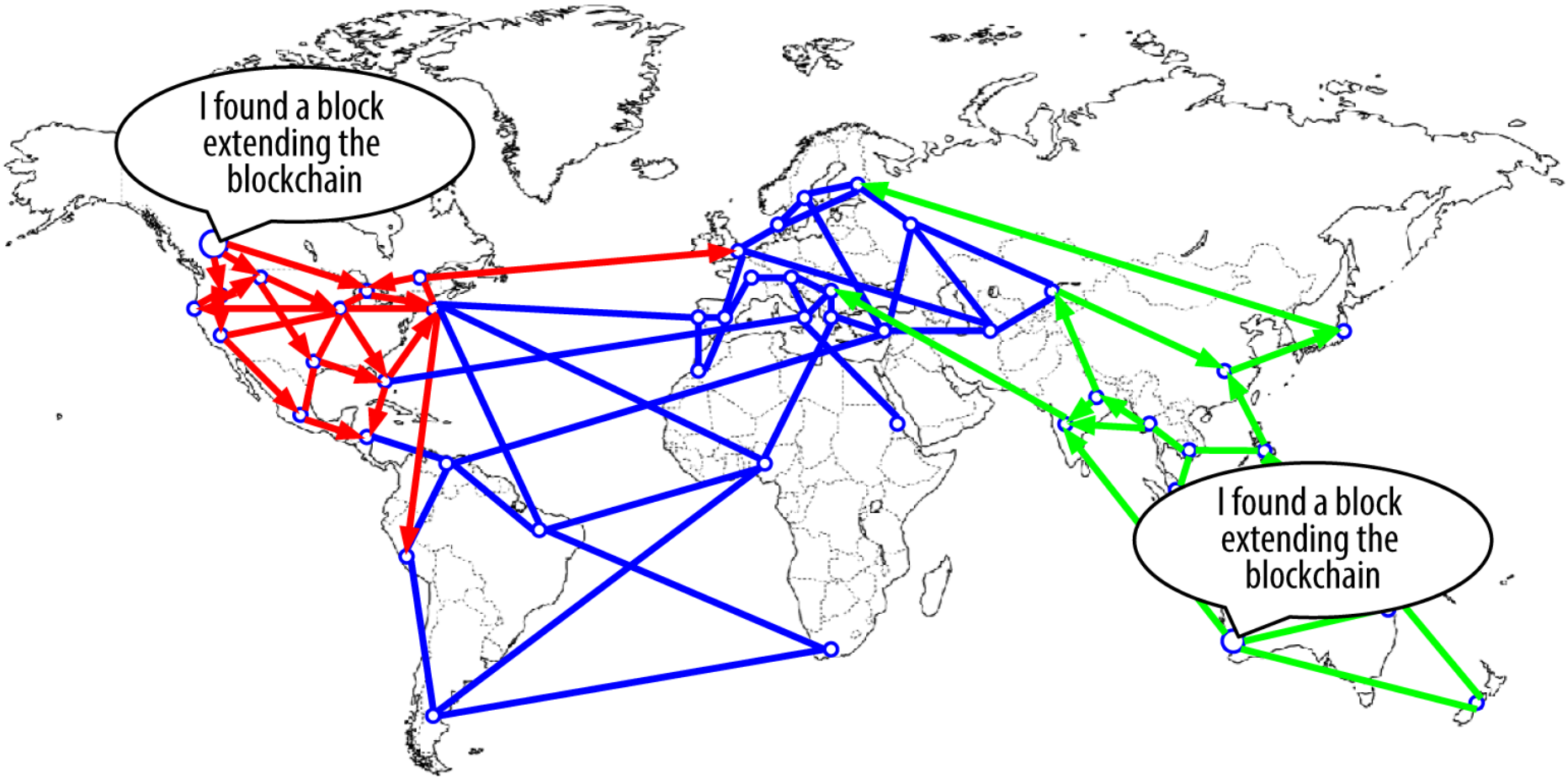
Merkle path


Root
HABCDEFGHIJKLMNOP
HABCDEFGH
HIJKLMNOP
HABCD
HEFGH
HIJKL
HMNOP
HAB
HCD
HEF
HGH
HIJ
HKL
HMN
HOP
HA
HB
HC
HD
HE
HF
HG
HH
HI
HJ
HK
HL
HM
HN
HO
HP

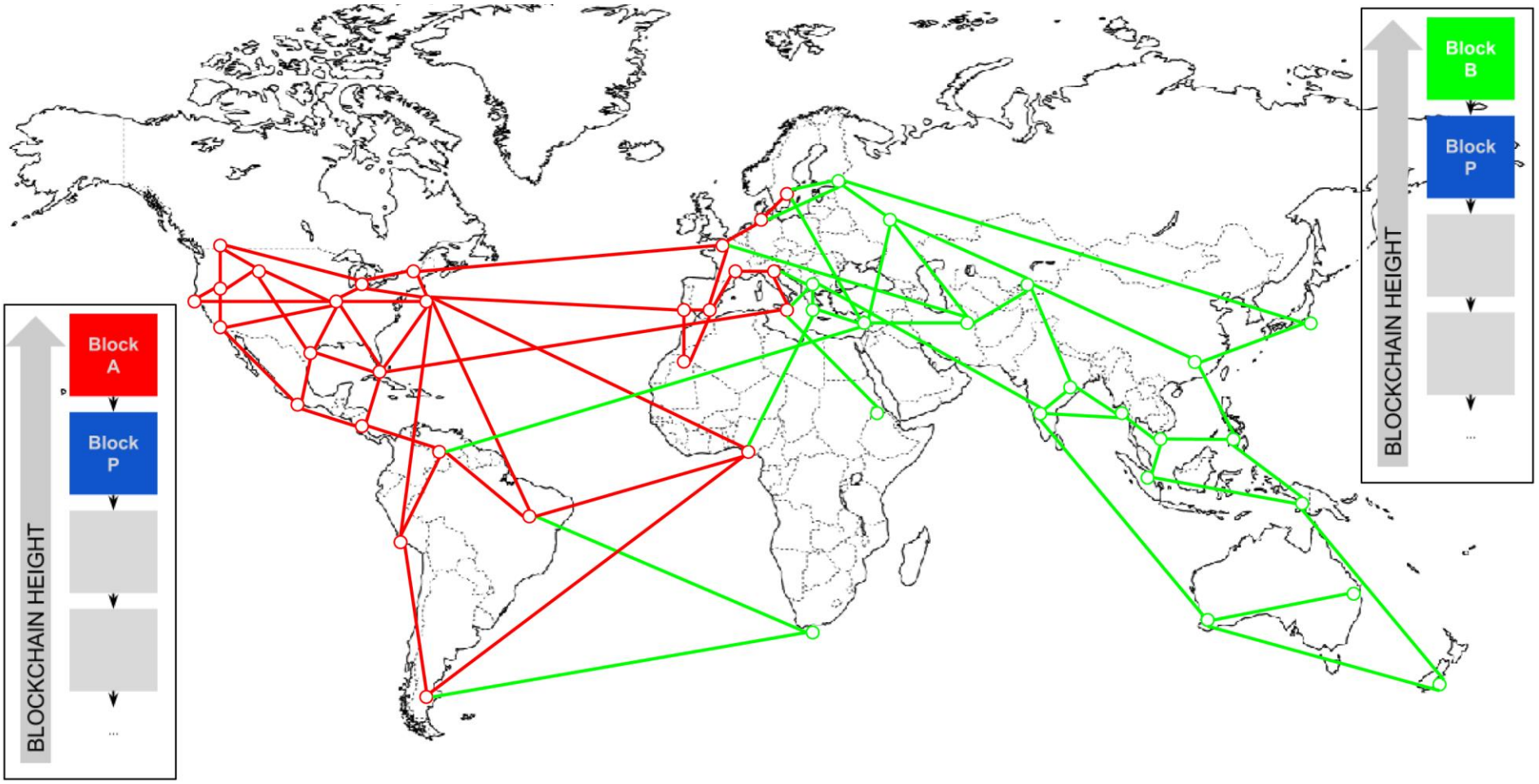
Consensus



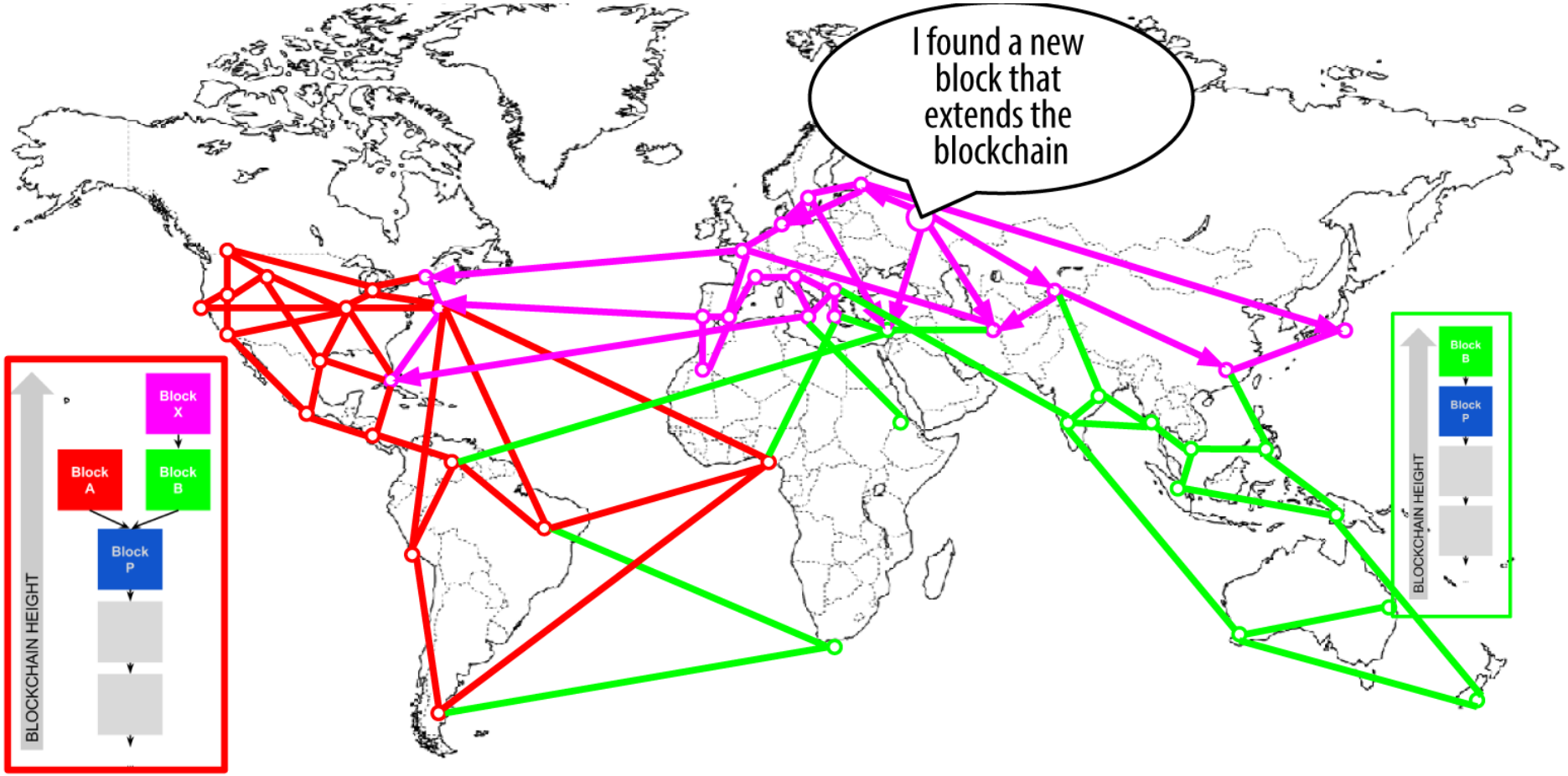
Consensus


I found a block extending the blockchain
I found a block extending the blockchain

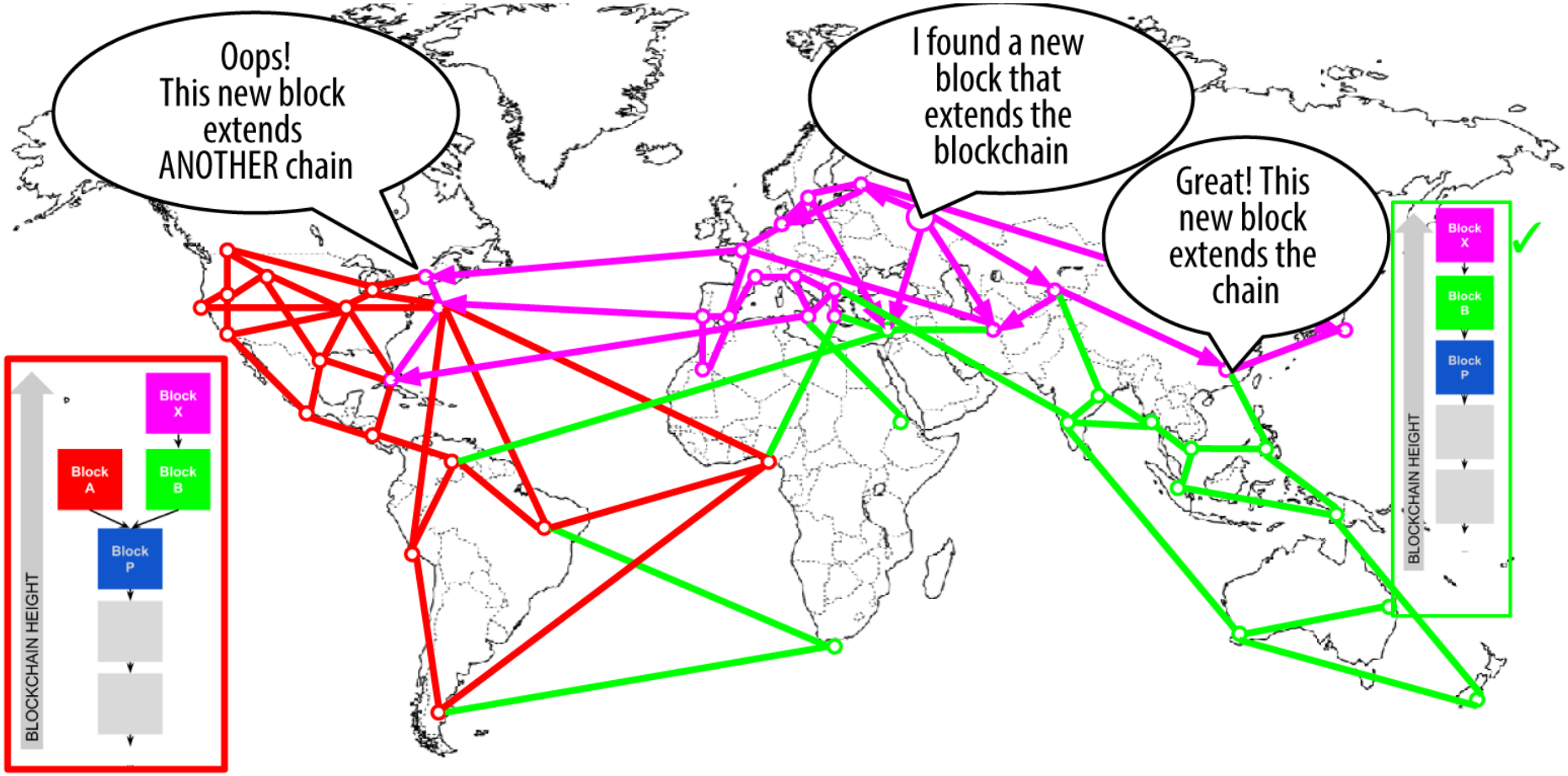
Consensus


Block
A
Block
P
...
BLOCKCHAIN HEIGHT
Block
B
Block
P
...
BLOCKCHAIN HEIGHT

Consensus


I found a new block that extends the blockchain
Block X
Block A
Block B
Block P
BLOCKCHAIN HEIGHT
Block B
Block P
BLOCKCHAIN HEIGHT

Consensus


Oops!
This new block
extends
ANOTHER chain
I found a new
block that
extends the
blockchain
Great! This
new block
extends the
chain
Block
X
Block
A
Block
B
Block
P
BLOCKCHAIN HEIGHT
Block
X
Block
B
Block
P
BLOCKCHAIN HEIGHT

Peer-to-peer network protocol

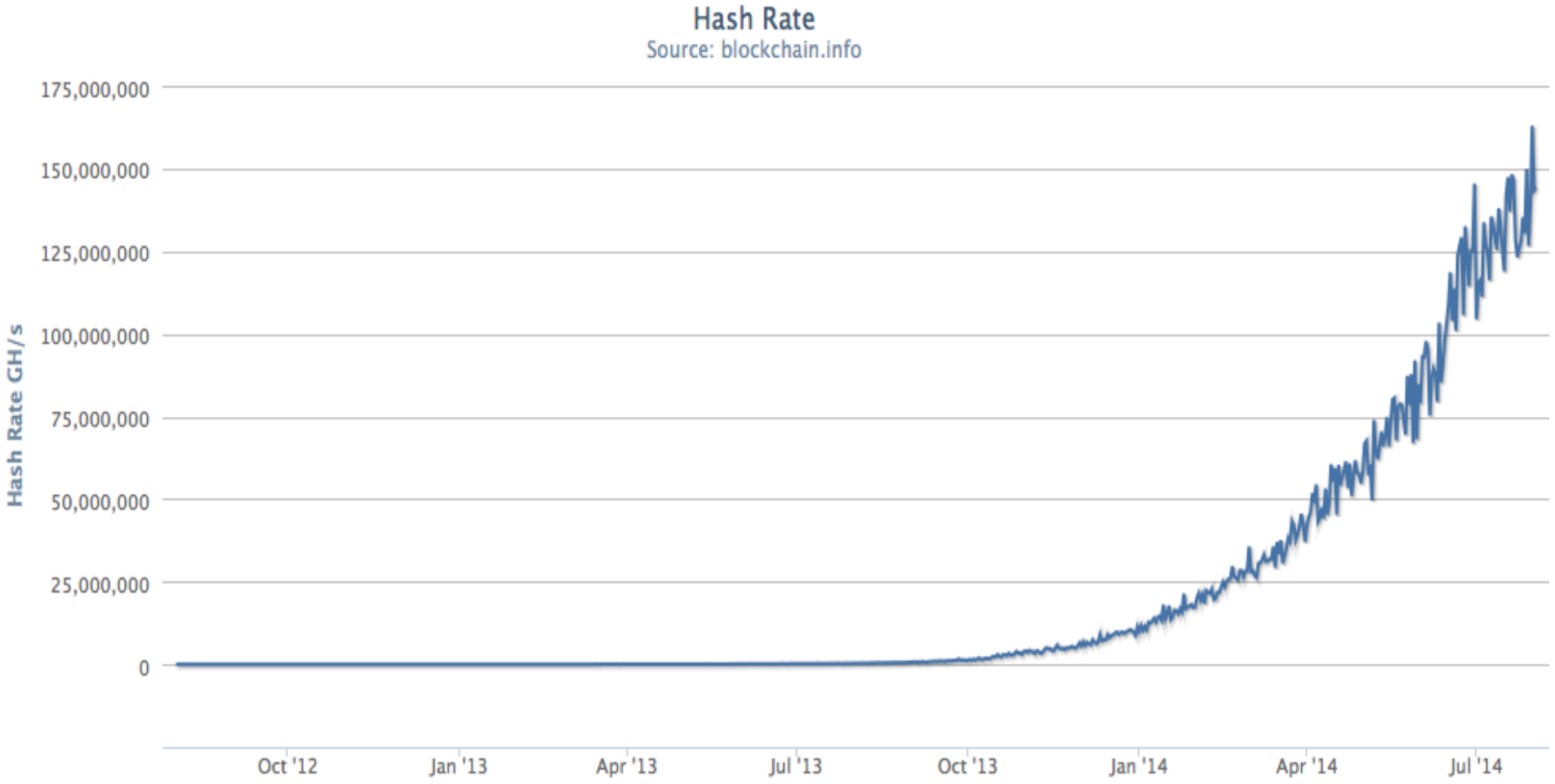
A peer-to-peer network is designed around the notion of equal peer nodes simultaneously functioning as both "clients" and "servers" to the other nodes on the network.

Peer-to-peer networks generally implement some form of virtual overlay network on top of the physical network topology, where the nodes in the overlay form a subset of the nodes in the physical network. Data is still exchanged directly over the underlying TCP/IP network, but at the application layer peers are able to communicate with each other directly, via the logical overlay links.

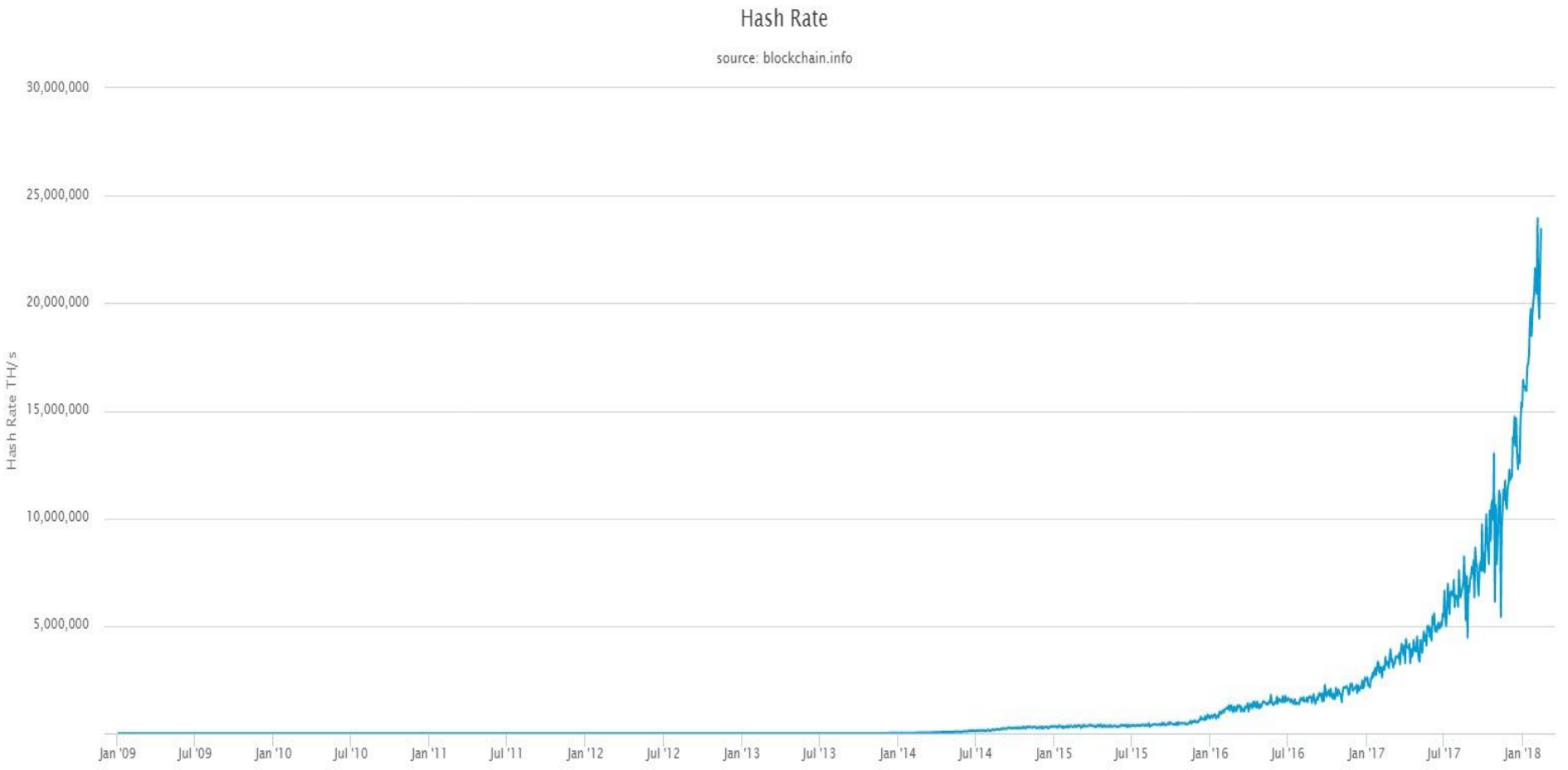
Bitcoin P2P network: https://bitcoin.org/en/p2p-network-guide

- Peer Discovery
- Connecting To Peers
- Initial Block Download
- Block Broadcasting
- Transaction Broadcasting
- Misbehaving Nodes
- Alerts

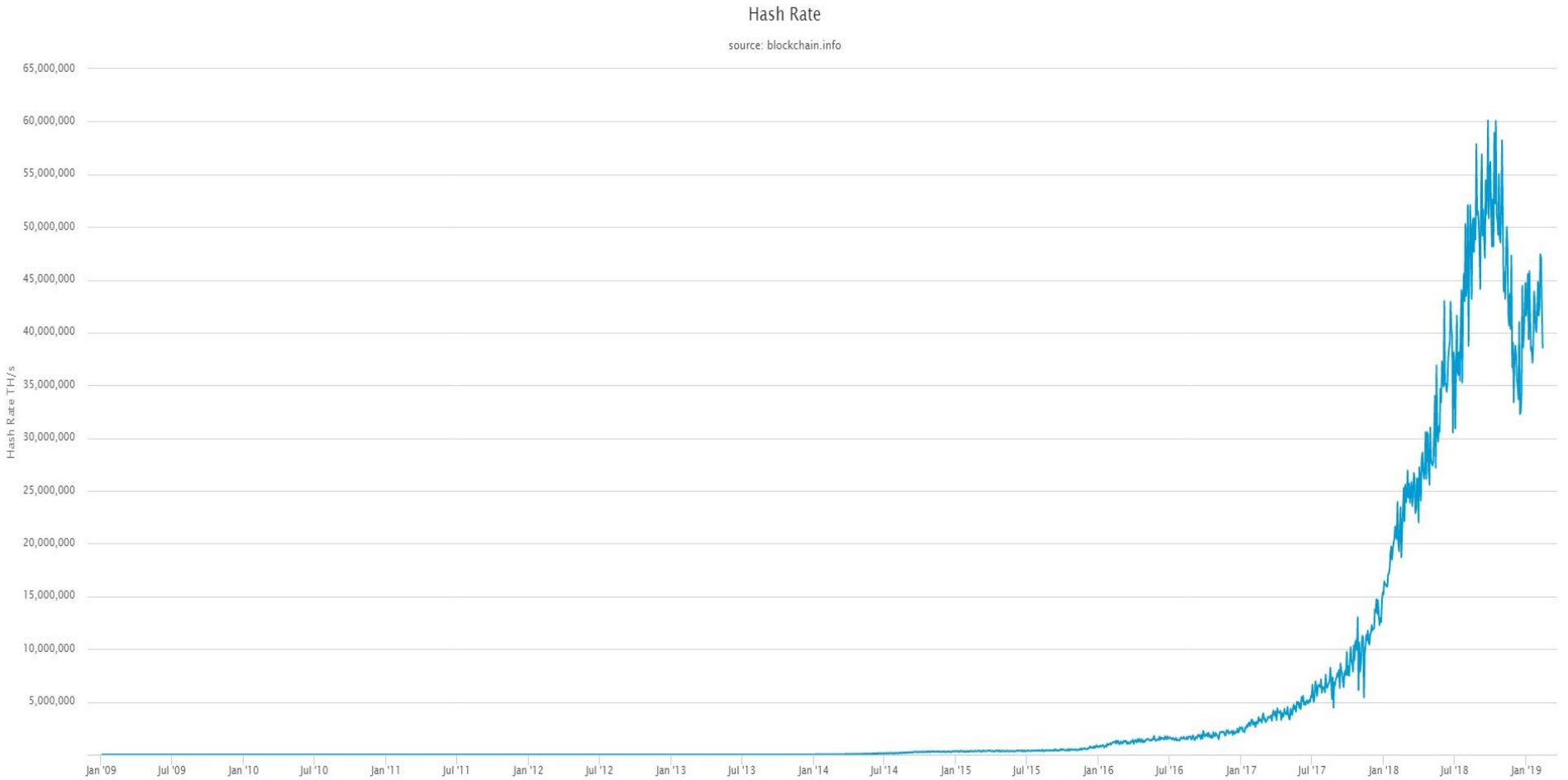
Miners' competition



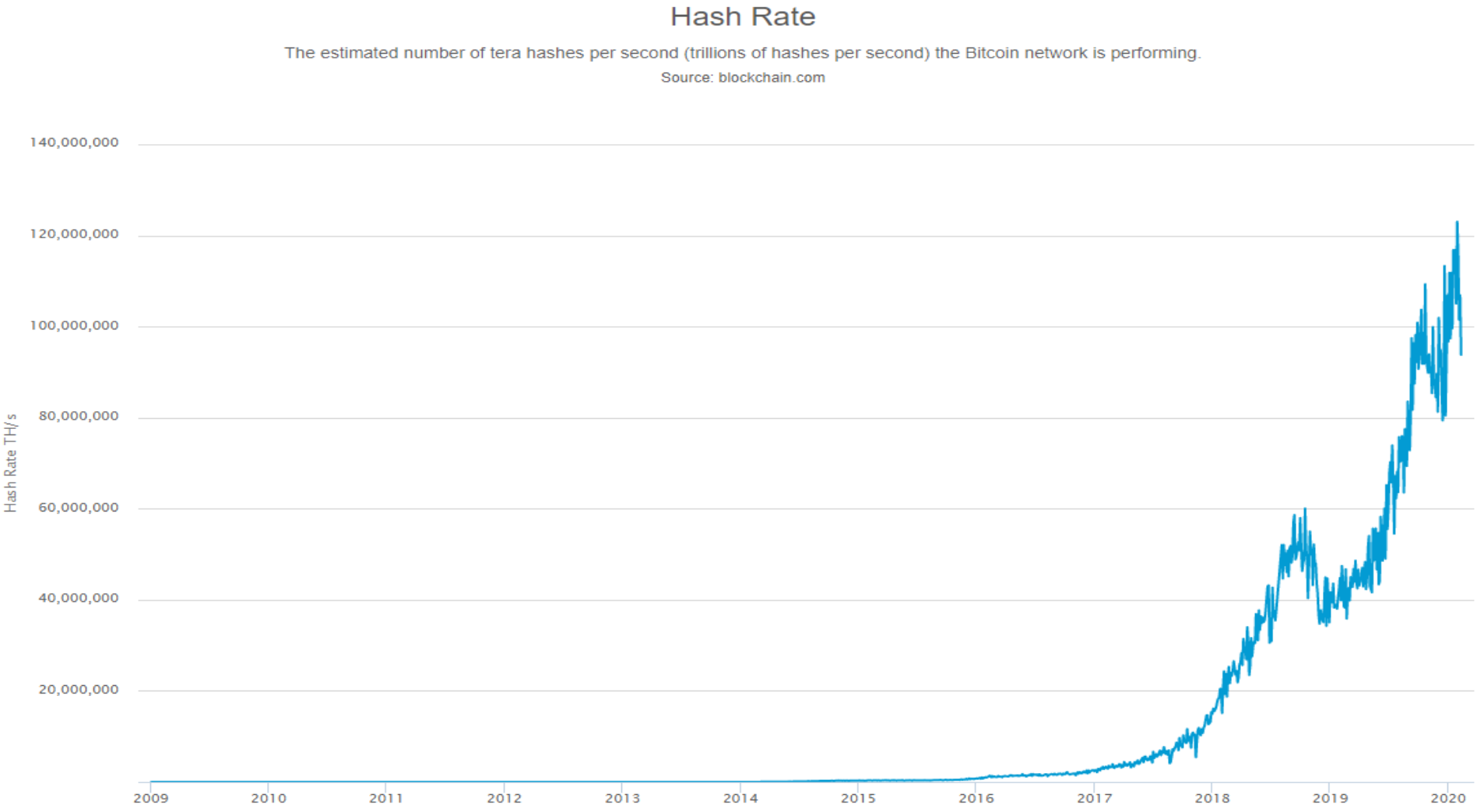
Miners' competition



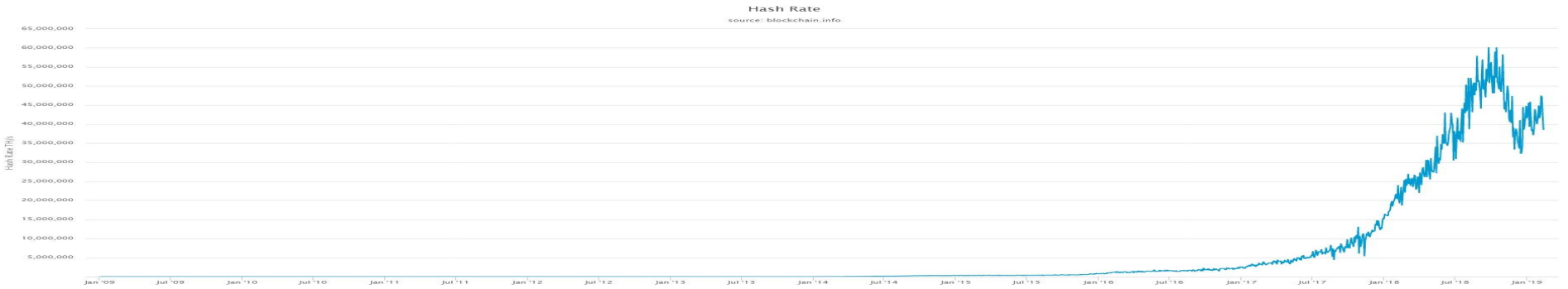
Miners' competition

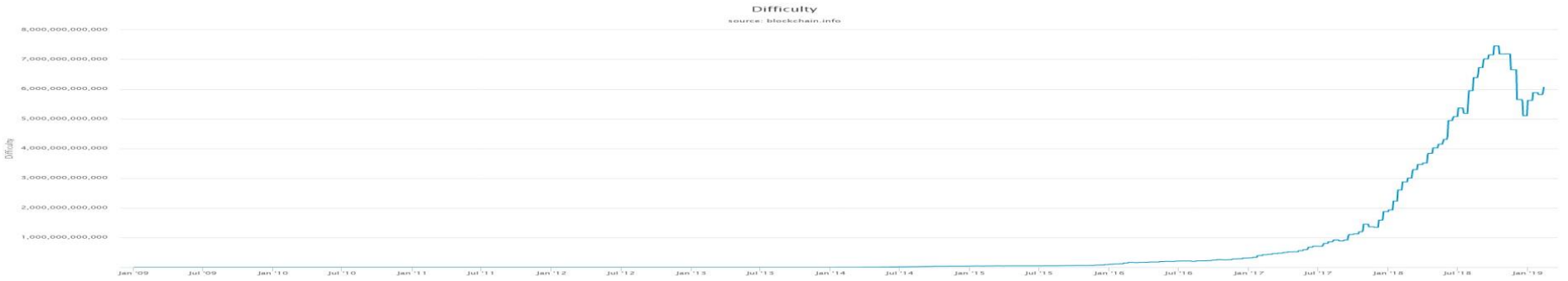


Miners' competition



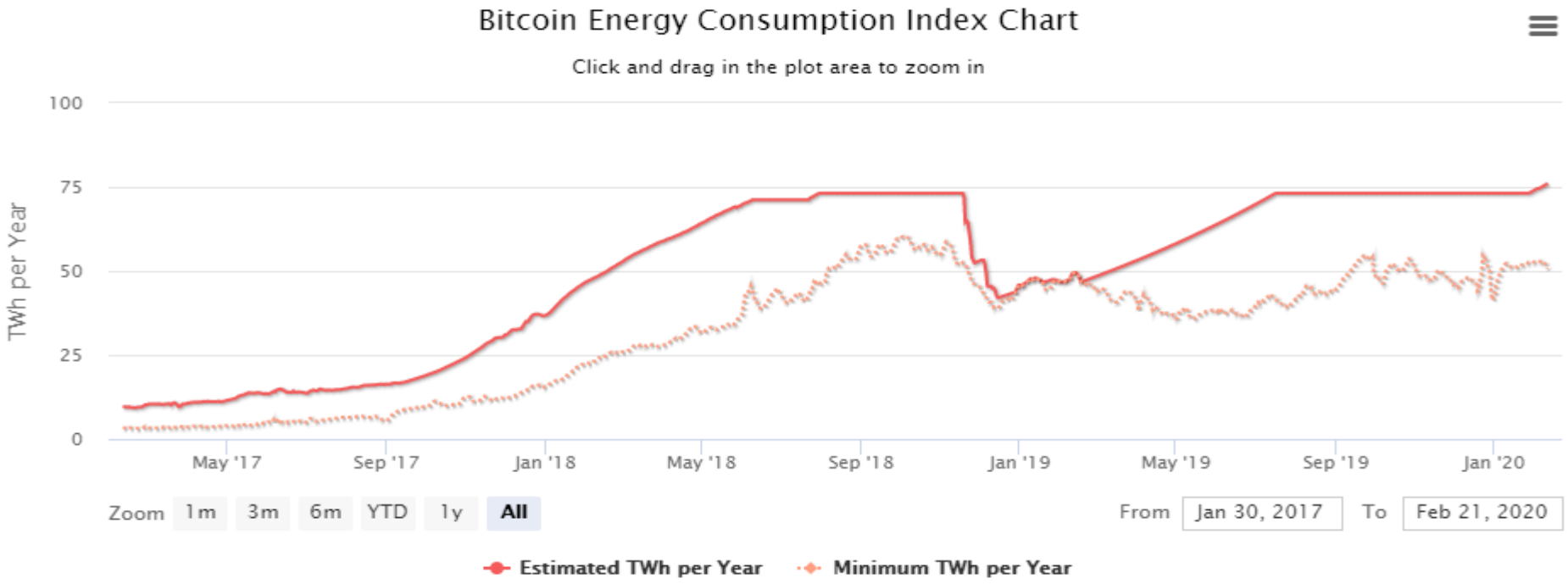
Hash rate vs. Price





Miners' daily revenue

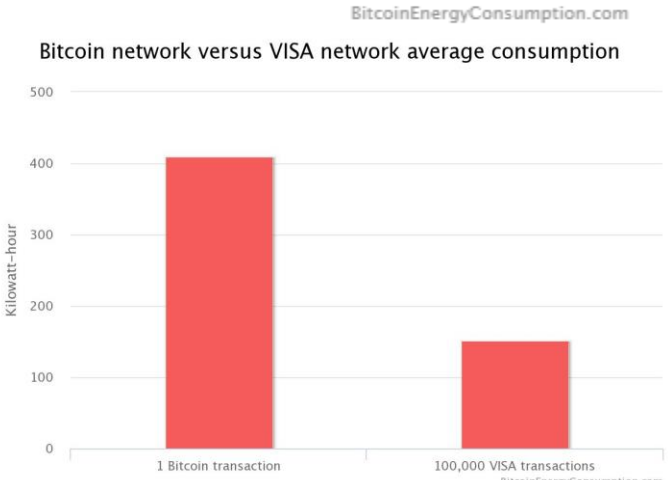
Energy Consumption



Hungary (2018): 45 TWh

as a percentage of the world's electricity consumption: 0.34%

https://digiconomist.net/bitcoin-energy-consumption



Other problems

A Survey on Security and Privacy Issues of Bitcoin (2017)

Mining

https://www.weusecoins.com/en/mining-guide/

Ki az a Satoshi Nakamoto

https://en.wikipedia.org/wiki/Satoshi_Nakamoto

Elfogadóhelyek

Pornó, drog, fegyver:
https://darknetmarkets.org/

Magyarországon:
https://coincolors.co/bitcoin-elfogadohelyek/

Life on Bitcoin:
https://www.kickstarter.com/projects/bitcoinlife/life-on-bitcoin-a-documentary-film

Balhék

Mt. Gox eltűnése:
http://www.coindesk.com/mt-gox-bitcoin-exchange-review/
https://www.mtgox.com/
http://en.wikipedia.org/wiki/Mt._Gox

BTC-e bezárása:
https://en.wikipedia.org/wiki/BTC-e

https://thechain.media/10-cryptocurrency-scandals-you-need-to-know-about