Plan

Tutorial Introduction to Bitcoin
Hype vs. Reality in Bitcoin Today
Scaling Bitcoin
Ombuds (Nick Skelsey)

What is money?

Aristotle’s Politics 350 BCE
Fiat Currency

With a strong enough army, anything can be a fiat currency

Centralized Digital Currency

<table>
<thead>
<tr>
<th>Account No.</th>
<th>Owner’s Identify</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>3022493</td>
<td>Alice</td>
<td>2033.23</td>
</tr>
<tr>
<td>3022494</td>
<td>Bob</td>
<td>85733.03</td>
</tr>
<tr>
<td>3022495</td>
<td>Colleen</td>
<td>24331.77</td>
</tr>
<tr>
<td>3022496</td>
<td>Dave</td>
<td>0.01</td>
</tr>
</tbody>
</table>

Communications of the ACM
October 1985

Security without Identification: Transaction Systems to Make Big Brother Obsolete

David Chaum
Computerization is robbing individuals of the ability to monitor and control the ways information about them is used. As organizations in both the private and the public sectors routinely exchange such information, individuals have no way of knowing if the information is inaccurate, obsolete, or otherwise inappropriate. The foundation is being laid for a dossier society, in which computers could be used to infer individuals’ life-styles, habits, whereabouts, and associations from data collected in ordinary consumer transactions. Uncertainty about whether data will remain secure against abuse by those maintaining or tapping it can have a “chilling effect,” causing people to alter their observable activities. As computerization becomes more pervasive, the potential for these problems will grow dramatically.
Double Spending Challenge

Bob wants to verify:
1. Alice owns X
2. Alice hasn’t transferred X
3. The coin will be valuable for Bob

Node C
Node A
Node B
Node C

Bob wants to verify:
1. Alice owns X
2. Alice hasn’t transferred X
3. The coin will be valuable for Bob
Bob wants to verify:
1. Alice owns X
2. Alice hasn’t transferred X
3. The coin will be valuable for Bob

Blockchain

Distributed ledger maintained by network of untrusted nodes
Blocks added require proof-of-work,
Node's agree to consensus: longest (most difficult) chain

Incentives designed to encourage network nodes to:
Validate and record transactions
Spend effort on extending consensus chain

Bitcoin P2P e-cash paper

Satoshi Nakamoto

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without the burdens of going through a financial institution.
**Bitcoin Script**

**Locking Script**

OP_DATA <signature>

**Unlocking Script**

OP_DATA <public key>

OP_CHECKSIG

---

**Transaction d8730d**

**Input 1:**

v1, a1

**Output 1:**

x1, d1

**Output 2:**

x2, d2

---

**Example Transaction**

**OP_RETURN (until July 2010)**

https://github.com/bitcoin/bitcoin/blob/v0.1.5/script.cpp#L170

```c
    case OP_RETURN:
        pc = pend;
        break;
```

**Universal Unlocking Script!**

OP_DATA 1

OP_RETURN

---

**Outputs Created (2)**

- 0.01523 BTC to
  - 12jQKbY9xVhL1tMzT9lJNMvM3A6UPvW2T0912
  - 1bend

- 0.006796 BTC to
  - 1LEtQG7bV4PsfuFwRb155WvM9M2y
  - 1bend

- 0.00101111 BTC to
  - 1WmN957bKjDxvM6B3c6sQj6KZw5vM9BZy
  - 1bend

- 0.006997 BTC to
  - 1aJU69m18Za2Zfdg3x2B1cEPhL7y8ym7
  - 1bend

**Fees are optional...**
**Bitcoin Transaction**

- **Input 1:** v₁, a₁
- **Input 2:** v₂, a₂

- **Output 1:** x₁, d₁
- **Output 2:** x₂, d₂

**Transaction fees** = sum(input values) – sum(output values) (must be non-negative for valid transaction)

**How is new bitcoin created?**

**Coinbase Transaction**

- **Output 1:** x₁, d₁
- **Output 2:** x₂, d₂

**sum(output values) ≤ sum(transaction fees) + mining reward**

**mining reward** = \( \frac{50 \text{ BTC}}{2^{floor(block number / 210,000)}} \)
Bitcoin’s Proof-of-Work

Find a nonce $x$ such that:

$$\text{SHA-256}(\text{SHA-256}(r \parallel x)) < T/d$$

$r = \text{header}$ includes $H(\text{previous block})$ root of Merkle tree of transactions

Actual Bitcoin Block

**Block Headers**

Block headers are sent in a headers packet in response to a getheaders message.

<table>
<thead>
<tr>
<th>Field Size</th>
<th>Description</th>
<th>Data type</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>version</td>
<td>uint32_t</td>
<td>Block version information, based upon the software version creating this block.</td>
</tr>
<tr>
<td>32</td>
<td>prev_block</td>
<td>char[32]</td>
<td>The hash value of the previous block this particular block references.</td>
</tr>
<tr>
<td>32</td>
<td>nonce</td>
<td>char[32]</td>
<td>The reference to a Merkle tree collection which is a hash of all transactions related to this block.</td>
</tr>
<tr>
<td>4</td>
<td>timestamp</td>
<td>uint32_t</td>
<td>A timestamp recording when this block was created (WII overflow in 2106).</td>
</tr>
<tr>
<td>4</td>
<td>bits</td>
<td>uint32_t</td>
<td>The calculated difficulty target being used for this block.</td>
</tr>
<tr>
<td>4</td>
<td>nonce</td>
<td>uint32_t</td>
<td>The nonce used to generate this block... to allow variations of the header and compute different hashes.</td>
</tr>
<tr>
<td>4</td>
<td>vin_count</td>
<td>uint32_t</td>
<td>Number of transaction entries, this value is always 0.</td>
</tr>
</tbody>
</table>

difficulty = 62,253,982,450
expected hashes = $2.67 \times 10^{20} \sim 2^{68}$

“number of grains of sand on earth”

https://en.bitcoin.it/wiki/Protocol_documentation#Block_Headers
Mining

32-bit XOR in CPU

32-bit XOR in ASIC

4 transistors XOR design

XOR two 32-bit values in CPU

XOR two 32-bit values in ASIC

(General-Purpose)

Computers are Useless

https://en.bitcoin.it/wiki/Mining_hardware_comparison

Be sure to research any of these vendors and machines intensely before spending any money.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>AntMiner S2 [2]</td>
<td>1,000,000</td>
<td>900</td>
<td>442</td>
<td>1100</td>
<td>2259</td>
<td>Discontinued</td>
<td>Ethernet</td>
<td>GPL infringement</td>
</tr>
<tr>
<td>AntMiner S4 [4]</td>
<td>2,000,000</td>
<td>1429</td>
<td>1429</td>
<td>1400</td>
<td>1400</td>
<td>Discontinued</td>
<td>Ethernet</td>
<td>GPL infringement</td>
</tr>
<tr>
<td>AntMiner S5 [5]</td>
<td>1,155,000</td>
<td>1957</td>
<td>3121</td>
<td>590</td>
<td>370</td>
<td>Discontinued</td>
<td>Ethernet</td>
<td>GPL infringement</td>
</tr>
<tr>
<td>AntMiner S7 [6]</td>
<td>4,860,000</td>
<td>4000</td>
<td>2666</td>
<td>1,210</td>
<td>1,823</td>
<td>No</td>
<td>Ethernet</td>
<td>GPL infringement</td>
</tr>
</tbody>
</table>
Fire at mining facility in Thailand, 14 Oct 2014

Photo credit: www.thairath.co.th
Entire bitcoin network: 1/10th Lake Anna Power Station
Reality Check

Bitcoin “Market Capitalization” = Number of Bitcoins × Market Price
= 14,777,800 × $314 = $4.64B

What does a $4.64B Market Cap company look like?
Can Bitcoin Scale?


```c
1 // Copyright (c) 2009-2010 Satoshi Nakamoto
2 // Copyright (c) 2009-2014 The Bitcoin Core developers
3 // Distributed under the MIT software license, see the accompanying
4 // file COPYING or http://www.opensource.org/licenses/mit-license.php.
5 #ifndef BITCOIN_CONSENSUS_CONSENSUS_H
6 #define BITCOIN_CONSENSUS_CONSENSUS_H
7 #endif
8
9 // The maximum allowed size for a serialized block, in bytes (network rule) */
10 static const unsigned int MAX_BLOCK_SIZE = 1000000;
11 // The maximum allowed number of signature check operations in a block (network rule) */
12 static const unsigned int MAX_BLOCK_SIGOPS = MAX_BLOCK_SIZE/50;
13 // Coinbase transaction outputs can only be spent after this number of new blocks (network rule) */
14 static const int COINBASE_MATURITY = 100;
```


```c
1 bool CheckBlock(const CBlock& block, CValidationState& state, bool fCheckMerkleRoot, bool fCheckEccMerkleRoot)
2 {
3     // These are checks that are independent of context.
4     if (block.IsRisky())
5         return true;
6     // Check that the header is valid (particularly P2S). This is mostly
7     // redundant with the call in AcceptBlock.
8     if (fCheckMerkleRoot && !state.CheckMerkleRoot(block))
9         return false;
10     // Check the merkle root.
11     if (fCheckEccMerkleRoot) {
12         bool mutable;
13         uint256 hashMerkleRoot2 = block.GetMerkleRoot2(mutable);
14         if (hashMerkleRoot2 != hashMerkleRoot)
15             return state.CheckMerkleRoot(block, fCheckEccMerkleRoot),
16                 MEDIUM_NONCE, "bad-block-merkle-root", true);
17         // Check for merkle tree sallability (CVC-2002-2005): repeating sequences
18         // of transactions in a block without affecting the merkle root of a block.
19         // while still invalidating it.
20         if (mutable)
21             return state.CheckMerkleRoot(block, fCheckEccMerkleRoot, true),
22                 MEDIUM_NONCE, "bad-tx-duplicate", true);
23     }
24     return true;
25 }
```
**Scale Today**

Block Size = 1MB  
Typical transaction size ~ 500 Bytes  
Maximum of ~2000 transactions per block / 10 minutes  
So, about 3-4 transactions per second

Cost to control bitcoin (assuming other miners are “rational”):  
value per block-minute = $7500/10 minutes ~ $750/minute ~ $1M/day  
to increase to $1B/day with current transaction rate:  
$3472 fee per transaction (without losing transactions)  
or 33 Billion transactions per day (with current $0.03 fee)
Cost to control bitcoin (assuming other miners are “rational”):
- Value per block-minute = $7500/10 minutes ~ $750/minute ~ $1M/day
- To increase to $1B/day with current transaction rate:
  - $3472 fee per transaction (without losing transactions)
  - 33 Billion transactions per day (with current $0.03 fee)

Transactions per Day
- VISA: 300M
- Interbank: 100M
- Cash: 20B

Transactions per Day
- VISA: 300M
- Interbank: 100M
- Cash: 20B
- Facebook Likes: 4.5B
- SMS Messages: 25B
- WhatsApp Msg: 50B

Scale Today

Block Size = 1MB
Typical transaction size ~ 500 Bytes
Maximum of ~2000 transactions per block
So, about 3-4 transactions per second

Cash is the single biggest opportunity

Transactions per Day
- VISA: ~13T
- Cash: ~6T

Transactions per Day
- VISA: ~13T
- Cash: ~6T

Nick Skelsey – Cofounder @ Soapbox Systems