How Bitcoin Actually Works

Jan Møller
Co-founder, CTO
Chainalysis
How Does Bitcoin Actually Work?

• This talk is not about the political or economical impact of Bitcoin.

• This talk is not about how to buy, sell, spend, or secure your bitcoins.

• This talk is about how Bitcoin actually works. ...you know... nerdy stuff!
How it Started

• White paper published November 2008 by Satoshi Nakamoto

  “Bitcoin: A Peer-to-Peer Electronic Cash System”

  “I've been working on a new electronic cash system that’s fully peer-to-peer, with no trusted third party.”

• Working implementation published 3 months later as an open source project.
A Brief [FUN] History

• First Bitcoin Transaction January 2009
• 2 Pizzas 10.000 BTC May 2010
• 1 BTC Suprasses USD 1 February 2011
• 1 Cessna Aircraft 10.000 BTC June 2011
• 1 BTC Surpasses USD 100 April 2013
• 1 BTC Surpasses USD 200 April 2013
• 1 BTC Surpasses USD 1000 November 2013
• 1 BTC Down to USD 245 June 2015

Today 1 bitcoin is about USD 750
What is Bitcoin?

• Bitcoin is the name of a p2p protocol
  Allows a network of computers to govern all the rules of Bitcoin

• Bitcoin is a unit of account
  Like Euro, Australian Dollar, or WoW gold coins

• Bitcoin is a payment System
  You can send value between accounts in the Bitcoin network
Properties of Common Digital Payment Systems

• No Counterfeiting
  YOU can't increase money supply at will

• No Double Spending
  YOU can't spend the same value more than once

• Transaction irreversibility
  YOU can't undo a transaction
Properties of Bitcoin

• No Counterfeiting
  \textbf{NOBODY} can increase money supply at will

• Transaction irreversibility
  \textbf{NOBODY} can undo a transaction

• No Double Spending
  \textbf{NOBODY} can spend the same value more than once
Bitcoin Solves Two Things

• Eliminates trust in a central authority
  You trust the rules of a protocol enforced by mathematics and cryptography

• Distribution of funds
  How to distribute value when you create a new currency?
Distribution of Funds

- Every 10 minutes since inception a “random” node in the Bitcoin network receives a reward.

- The reward started at 50 bitcoins, and halves every 4 years
The Blockchain

• The big invention that makes Bitcoin work

• The blockchain is a database containing historical records of all the transactions that ever occurred in the network.

• Every full node in the network has a copy that they keep up to date and verify.

• Some nodes extend the block chain, they are called miners.
Think of it as a big accounting book. Every block is a page in the book.

Anyone can try to add a page to the book to get a reward ... but it is computationally hard to do so.

Problem: We want a new block to appear every 10 minutes on average.
Introducing SHA-256

- Cryptographically secure one-way hash function.
- Takes any input and produces a 32 byte output.
- Flipping one bit in the input gives a different randomly distributed output.

\[
\text{Sha256(“YOW”) = 990d7204316fe2907f55cb22d7b66fe9} \\
\text{    e1f7e26dca2b61041cc3d3eec303d6a7} \\
\text{Sha256(“WOY”) = cab9db6bcb5b96f48fb3e5f11cc43008} \\
\text{    a9eee6b168127ee7422f7218877751ff}
\]
How to create a new block?

**Block Header**
- Version
- Previous Block Hash
- Merkle Root
- Time Stamp
- Bits
- Nonce

**Payload**
- Transactions

80 byte header
Block Hash = Sha256( Sha256(Header) )
But there is a catch...

Variable size
Block hash must be below the target difficulty

1. Create header
2. Make nonce random
3. Calculate block hash
4. Is it below the target?
5. 😊 we are done
6. 😞 goto 2

Block# 440000 ~ 2,000,000,000 GH/s

00000000000000000000038cc0f7bcdbb451ad34a458e2d535764f835fdeb896f29b
The Difficulty Adapts
Block Propagation
Forks are Normal (1)
Forks are Normal (2)

The longest chain wins!
Distribution of Funds Summary

- Funds are distributed by solving blocks
- Difficulty adapts over time
- The longest chain wins
Bitcoin Public/Private Keys

- A Bitcoin uses Elliptic Curve cryptography
- A private key is 32 random bytes
- A public key is computed from a private key
- There is no encryption in Bitcoin, only signing
Bitcoin Addresses

• A Bitcoin address is a bit like a bank account. 1Kk18SN6WRPTEXbXBm3dZSzEw7NdbChyc9

• Calculated from a public key
  RIPEMD-160( Sha256( public key ) )

• Nobody knows who owns which addresses

• Value is moved between addresses using transactions.
Transactions (simplified)

- A Bitcoin transaction sends value from one set of addresses to another

<table>
<thead>
<tr>
<th>Inputs</th>
<th>Outputs</th>
</tr>
</thead>
<tbody>
<tr>
<td>5 BTC</td>
<td>10 BTC</td>
</tr>
<tr>
<td>3 BTC</td>
<td>2 BTC</td>
</tr>
<tr>
<td>4 BTC</td>
<td></td>
</tr>
</tbody>
</table>

Transaction Hash = Sha256(Sha256(Transaction Data))
Creating a Transaction (1/7)
Creating a Transaction (2/7)
Creating a Transaction (4/7)

Inputs | Outputs
--- | ---
|  | 1 BTC
|  | 5 BTC

Inputs | Outputs
--- | ---
|  | 7 BTC
|  | 3 BTC

Inputs | Outputs
--- | ---
|  | 4 BTC
|  | 2 BTC

Transaction

Inputs | Outputs
--- | ---
|  | 10 BTC
|  | 2 BTC
Creating a Transaction (4/7)

<table>
<thead>
<tr>
<th>Inputs</th>
<th>Outputs</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1 BTC</td>
</tr>
<tr>
<td></td>
<td>5 BTC</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Inputs</th>
<th>Outputs</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>7 BTC</td>
</tr>
<tr>
<td></td>
<td>3 BTC</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Inputs</th>
<th>Outputs</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>4 BTC</td>
</tr>
<tr>
<td></td>
<td>2 BTC</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Transaction Fee = 0.0001 BTC
### Creating a Transaction (5/7)

<table>
<thead>
<tr>
<th>Inputs</th>
<th>Outputs</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1 BTC</td>
</tr>
<tr>
<td></td>
<td>5 BTC</td>
</tr>
<tr>
<td></td>
<td>7 BTC</td>
</tr>
<tr>
<td></td>
<td>3 BTC</td>
</tr>
<tr>
<td></td>
<td>4 BTC</td>
</tr>
<tr>
<td></td>
<td>2 BTC</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Inputs</th>
<th>Outputs</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>10 BTC</td>
</tr>
<tr>
<td></td>
<td>1.9999 BTC</td>
</tr>
</tbody>
</table>

Transaction Fee = 0.0001 BTC
Creating a Transaction (6/7)

Inputs | Outputs
--- | ---
1 BTC  |  
5 BTC  |  

Inputs | Outputs
--- | ---
7 BTC  |  
3 BTC  |  

Inputs | Outputs
--- | ---
4 BTC  |  
2 BTC  |  

Transaction

Inputs | Outputs
--- | ---
Locked  | 10 BTC
Locked  | 1.9999 BTC

Transaction Fee = 0.0001 BTC
Creating a Transaction (7/7)

Bitcoin Network

<table>
<thead>
<tr>
<th>Inputs</th>
<th>Outputs</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 BTC</td>
<td></td>
</tr>
<tr>
<td>5 BTC</td>
<td></td>
</tr>
<tr>
<td>7 BTC</td>
<td></td>
</tr>
<tr>
<td>3 BTC</td>
<td></td>
</tr>
<tr>
<td>4 BTC</td>
<td></td>
</tr>
<tr>
<td>2 BTC</td>
<td></td>
</tr>
</tbody>
</table>

Transaction

<table>
<thead>
<tr>
<th>Inputs</th>
<th>Outputs</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>10 BTC</td>
</tr>
<tr>
<td></td>
<td>1.9999 BTC</td>
</tr>
</tbody>
</table>

Transaction creation (7/7)
Transaction Relaying

- Receive transaction from peer

- Verification (simplified):
  - Verify that the signatures are sound
  - Verify that the inputs are unspent
  - Verify that the sum of outputs $\leq$ sum of inputs

- Relay transaction to other peers
Block 0

Genesis Block

Block 1

... 

Block N

Block N+1

Version
Previous Block Hash
Merkle Root
Time Stamp
Bits
Nonce

Transactions
Transactions in Forks (1)

Block N-2 → Block N-1 → Block N'

... → My Transaction

Block N'' → My Transaction

Block N'' → My Transaction
Transactions in Forks (2.1)
The longest chain wins!
No Counterfeiting

“NOBODY” can increase money supply at will

You are competing with the biggest distributed computer the world has seen.
If you can beat it, it just gets harder.
Properties of Bitcoin (2/3)

Transaction irreversibility
“NOBODY” can undo a transaction

Requires a 51% attack

Original Transaction

Reversed Transaction
Properties of Bitcoin (3/3)

No Double Spending

**NOBODY** can spend the same value more than once

Block N-2  Block N-1  Block N

Two transactions spending the same outputs
Blockchain Tech is New

Trustless decentralized ordering of events

• Decentralized DNS with Namecoin
  – A decentralized open source information registration and transfer system.

• Decentralized Stock Exchange
  – Coloredcoins.org is one of several solutions that allow you to issue and track digital assets on top of the Bitcoin blockchain.

We can do stuff that wasn’t possible before
Want to Know More?

Mastering Bitcoin
UNLOCKING DIGITAL CRYPTOCURRENCIES
Andreas M. Antonopoulos
Questions?

Jan Møller
Co-founder, CTO
Chainalysis