How I could be a millionaire
or
a bit* about Bitcoin

*simplified

Vitalii Iarko
Outline

0) Modern money and Internet payments.
1) What is Bitcoin?
2) How it works?
3) Disadvantages.
Modern money.

• Fiat money
• Value guaranteed by government or law
• Not valuable itself

One needs to trust 3rd party…
(money emission and so on)
Internet payments

• Financial institutions serving as trusted third parties
• No 100% nonreversible transactions
• Transactions fee
• No anonymity

Again trusting 3rd parties…
- But I do not like to trust someone…
- What about cryptographic proof?
What is Bitcoin?

• Online payment system
• Decentralized (peer to peer)
• So called cryptocurrency (does not require trusting at all)
• …complex system of strongly interacting agents with equal opportunities!
How it works?
List of all accounts (Ledger)

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Alice</td>
<td>123 BTC</td>
<td>-5 BTC</td>
</tr>
<tr>
<td>Bob</td>
<td>0.0001 BTC</td>
<td>+5 BTC</td>
</tr>
<tr>
<td>Victor</td>
<td>0 BTC</td>
<td></td>
</tr>
<tr>
<td>...</td>
<td>...</td>
<td></td>
</tr>
</tbody>
</table>

Hey, everyone!
I’m sending 5 BTC to Bob.

Alice  
Bob  
Alice
List of all transactions (and no balances)

<table>
<thead>
<tr>
<th>Transaction ID</th>
<th>From, to</th>
<th>Amount</th>
</tr>
</thead>
<tbody>
<tr>
<td>ah32...</td>
<td>Victor to Alice</td>
<td>3 BTC</td>
</tr>
<tr>
<td>28ba...</td>
<td>Peggy to Alice</td>
<td>4 BTC</td>
</tr>
<tr>
<td>fe39...</td>
<td>Romeo to Juliet</td>
<td>0.1337 BTC</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
<td>...</td>
</tr>
</tbody>
</table>
Hey, everyone!
I got 7 bitcoins in transactions ah32... and 28ba...
Now I’m sending 5 BTC to Bob (and 2 BTC back to me).
Why can’t Mallory send Alice’s bitcoins?

Digital signature ECDSA (Elliptic Curve Digital Signature Algorithm).

Only Alice knows
Public key = some function(private key)

Inverse of some function is hard to compute
Alice does

Message (transaction)

Private key

ECDSA

signature

Others do

Real
Alice’s signature of the message or not?

Public key

ECDSA

signature

Message (transaction)
Double spending

1) Alice broadcasts that she sends 5 BTC to Bob.
2) Bob gets message and sends her goods.
3) Alice broadcasts that she sends this 5 BTC to herself.
4) Nodes that receive 3) before 1) discard 1).

>>Contradiction in the network.
unconfirmed (unordered) transactions

Block
Id: ea562...
Prev: ...
Transactions: ...

Block
Id: abe5...
Prev: ea562...
Transactions: ...

New Block
Id: eff4...
Prev: abe5 ...
Transactions: a4cb...
fd9f...
e37c...

New Block
Id: a58b...
Prev: abe5 ...
Transactions: a4cb...
e37c...

by Alice

by Bob
Math “puzzle”

To “solve” a block = find K such that

\[
F(\text{block}) < \text{threshold}
\]

SHA256 (cryptographic hash)

New Block
Id: eff4…
Prev: abe5 …
Transactions
a4cb…
fd9f…
Random
guess K:
328490123
SHA256(“Complex Systems Seminars 2015”)
b5c941cdc49d79fa9fd3f777709c506f4d2256f4dfd615a54f79027b31e7b0f7

SHA256(“Complex Systems Seminars 2014”)
27c7b1fe7862b1d22ec190c26e0dfd657a0b85883f44fdae649fb1709ba874b3

Very unpredictable
unconfirmed (unordered) transactions

This block becomes discarded and transactions are unordered again.
Again double spending

Block 1

Block 2

Block 3

Block 4

Block 2a

Block 3a

Block 4a

Block 5a

with Alice to Alice 5 BTC ↓

Alice’s chain!

with Alice to Bob 5 BTC

Bob sends goods

time
New Block
Id:  eff4…
Prev:  abe5 …
Transactions
a4cb…
fd9f…
Random
guess:
328490123

Block id = SHA256(block without id)
But with random guess
versus

~3 \times 10^{17} \text{ hashes/second}

More secure

\begin{align*}
\text{Block} & \quad \text{Block} & \quad \text{Block} & \quad \text{Block} & \quad \text{Block} & \quad \text{Block}
\end{align*}

less secure

\text{time}
Hash rate (1 GH/s = 10^9 H/s)

F(block) < threshold
How bitcoins are generated?

Mine them! Solved block = X bitcoins!

X <- X / 2 every 210000 blocks (four years)

Now X = 25 BTC

Already mined = 14 * 10^6 BTC

Overall  = 21 * 10^6 BTC

Last will be mined in 2140
What if all bitcoins are mined?

Fees!

Transaction may have optional fee

Miners can prefer transaction with fees

Solved block gives fees from transactions in it.
Anonymity?

- All accounts and transactions are known.
- But which account is yours?
- New account for each transaction.
Disadvantages.

- Wrong address? Very likely BTC will be lost forever (\(2^{160}\) addresses overall).
- Nobody guarantees anything (worse than fiat?).
- Waiting for transaction “confirmation”.
- Fees.
- Energy wasting.
Quick recap

Alice  broadcasts (caricature):

Current id #17d3…,  
previous transactions #fe12…, #cd62…  
to bbbbbb… 5 BTC, fee 0.01 BTC,  
remaining 1.99 BTC to aaaaaa…

5 BTC

Alice  Bob

Public key: aaaaaa…  
Public key: bbbbbb…  
transaction with  
Alice as receiver:  
3 BTC, id #fe12…  
4 BTC, id #cd62…
Miners side

unconfirmed (unordered) transactions

Miner A

New Block A
Link to last block
a4cb...; 17d3...;

F(New Block A, K = 123)=135151>1000
F(New Block A, K = 124)=686976>1000
....
F(New Block A, K = 531)=789959>1000

Miner B

New Block B
Link to last block
17d3...; fd9f...;

F(New Block B, K = 6732)=351412>1000
F(New Block B, K = 6733)=576489>1000
....
F(New Block B, K = 9859)=997<1000
Miner B solves puzzle (~10 minutes)

Then Miner B broadcasts (caricature):

I (public key …) propose next block with transactions 17d3…; a4cb… and puzzle solution is K = 9859.

All participants (including Alice and Bob):
Get Miner B’s message, check the solution, update the history.
According to the rules Miner B’s gets 25 BTC and all fees from 17d3…; fd9f…; (including 0.01 BTC from Alice). This block in history is a proof.
Bob

- Knows that one block is quite risky confirmation – may be discarded by longer brunch.
- Therefore, he waits $K$ more blocks ($\sim K \times 10$ minutes) and sends goods.
- Success!
You said “a millionaire”

Exchange rate USD per 1 BTC

- 20 USD/BTC
- 1150 USD/BTC

Network hashrate

~ here I first read about BTC
On 22nd May 2010
Laszlo Hanyecz
bought
a pizza
for 10000 BTC
(25 USD at that time).
Sources:
0) Nakamoto, Satoshi (24 May 2009).
   "Bitcoin: A Peer-to-Peer Electronic Cash System"
1) bitcoin.org
2) How Bitcoin Works Under the Hood (youtube)

Simpler view:
The Essence of How Bitcoin Works (Non-Technical) (youtube)
How Bitcoin Works in 5 Minutes (Technical) (youtube)

Interesting:
Life Inside a Secret Chinese Bitcoin Mine (youtube)
(1.5 kkUSD per month)