Bitcoin

ZOLTÁN VÁRNAGY (2014)
Contents

- Introduction
- Short history
- Basic definitions, methods and security
- Countermeasures
- Conclusion
- Links... questions?
What is Bitcoin?

- "Bitcoin is an experimental, decentralized digital currency that enables instant payments to anyone, anywhere in the world." /en.bitcoin.it/

- Main properties:
  - Anonym (therefore untraceable)
  - Decentralized (does not need a trusted third party, e.g. bank)
  - Uses peer-to-peer networks and broadcast communication
  - Secure
  - Provides easy storage and transaction
History

- The idea was first published by Satoshi Nakamoto in a mailing list(!), in 2008
- In the next 3 years it was not used widely...
- The first transaction, where someone used bitcoin as money, was in May 2010!
  - Laszlo Hanyecz from Florida paid 10,000 BTC for 2 pizzas (indirectly), which was worth 25$ at that time

More history:
- The first few transactions in 2009 were made by Nakamoto him/herself
- Exchange rates published in Oct 2009: $1 = 1309.03 BTC
- Now 10,000 BTC is worth nearly 3.5 million dollars!
More history:
- At that time e.g. Wikileaks started to accept donations in bitcoins
- When the exchange rate raised to 12.000 USD/BTC, the China Central Bank banned Bitcoin in China!
- 2014. November: Truecoin
Silk Road website in 2011

Shop by category:
- Drugs(732)
- Cannabis(280)
- Ecstasy(35)
- Dissociatives(11)
- Psychedelics(94)
- Opioids(82)
- Stimulants(33)
- Other(107)
- Benzos(70)
- Lab Supplies(6)
- Digital goods(58)
- Services(48)
- Money(55)
- Weaponry(15)
- Home & Garden(14)
- Food(4)
- Electronics(5)
- Books(49)
- Drug paraphernalia(28)
- XXX(30)
- Medicines(3)
- Computer equipment(4)
- Apparel(4)
- Musical instruments(2)
- Tourism(1)

News:
- Escrow hedging update
- New feature to help protect sellers
- We are hiring! Get paid for a referral, too...
- Reclaim lost coins from MyBitcoin.com
- Seller ranking and feedback overhaul
- Change your Mt. Gox password
Bitcoin: the basics

- When we want to use bitcoins for paying, we must first download a **bitcoin client** to our computer.
Bitcoin: the basics

- For every client we get a **wallet**, where we store:
  - our **bitcoins**
  - our bitcoin **addresses**
  - keypairs for each of our bitcoin addresses (discuss later)
  - data from all transactions from/to our addresses
  - other user and version data

- For every transaction we can and should make new address and keypairs (full anonymity)
Bitcoin: the basics

- If we know the **address** of the other person’s account, we can start a **transaction**
  - Bitcoin uses TCP port 8333 for transactions
- As Bitcoin uses broadcast communication, when we start a transaction, our client sends it to **every** node in the bitcoin community
  - So **every** bitcoin client knows **every** transaction **ever made**!
  - This is necessary, because we want to make sure, nobody wants to inject old transactions into the system (**double payment**)
Bitcoin: the basics

- This picture shows how this works...

[*] Picture resource: bitcoin.org
When we exchange money at e.g. a bank, the anonymity is compromised a bit...

---

**Bitcoin: the basics**

- Okay, but where do **bitcoins** come from?
- One can get bitcoins from:
  - mining (discuss later)
  - exchanging real money (e.g. USD)
  - earlier transactions (e.g. laszlo sent us 10,000 BTC for his pizzas 😊)

- **The one and only way new bitcoins are inserted into the system is via bitcoin mining!**
  - This is the „mintage“ in the system
Remember: bitcoins are inserted in the system by bitcoin miners (they got bitcoins for making transaction blocks).
We have to prove, that our bitcoins are from a mined bitcoin amount!
# Bitcoin: under the hood

<table>
<thead>
<tr>
<th>Generation: 25 = 0.0249298 total fees</th>
<th>JKHE7twfBuuENAxxxxxocD66q-T6DkYY 25 0.0249298</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><img src="image-url" alt="Transaction Details" /></td>
</tr>
</tbody>
</table>

- **Transaction Details**
  - **Recipient:** JKHE7twfBuuENAxxxxxocD66q-T6DkYY
  - **Amount:** 25
  - **Fee:** 0.0249298

- **Transaction IDs:**
  - 1R46s7ABdZaREQE5GTK8Qdx1bZHV9cEL: 0.2
  - JN1hN5DkJ/BUwMeU1JZeE4qjytFQpHLw5RQ: 0.03800471
  - JAcwM1luku8w1Z2X3t8C9Z3w8F8FEXr 0.16198529
  - JAcweM1luku8w1Z2X3t8C9Z3w8F8FEXr 0.16198529
  - 1J7Ncut3ZX318s7C8zQw8F8FEXr 135.84575666
  - JFvthN3KlxyLKNZx3i1GVP3j1Nkk46T8 10.94987
  - JAcwM1luku8w1Z2X3t8C9Z3w8F8FEXr 125.05768395
Bitcoin: under the hood

- Second problem: *How can the real sender and receiver of a transaction be identified?*
- The answer: ECDSA signature with a public-private keypair
- Every transaction has two additional fields:
  - the digitally signed hash of the next owner’s public key
  - the digitally signed hash of the previous transaction of the bitcoins
- Our bitcoin address is associated with this keypair’s public key
Bitcoin: under the hood

- The digital signing proves the sender (only the sender's public key can verify the signature)
- The owner's public key identifies the next owner of the BTC
Bitcoin: under the hood

- So when we spend our BTC from our earlier transactions, we:

1. Find our previous transaction, where we got the BTC
2. Find the (hash of our) public key in it
3. Find the private key for that certain public key
4. Make a signature for the transaction (and the next owner’s public key hash) with that key -> later this can be verified with a "scripting system" (won’t be discussed)
Bitcoin: the basics

- Transactions are collected into **blocks**
- Every block is made by **blockminers**
  - They also verify the transactions
  - Miners get money (BTC) for making one block (**incentive**)
  - They can also get money from **transaction fees**
  - This money will be the first transaction in the next block!
  - Anybody can be a miner, who has a miner software...
- When someone makes a block, he/she chains it after the last block, which was made before that block
  - So every block is chained together -> **blockchain**

Bitcoin: the basics

- When a new block is put at the end of the current chain, the miner broadcasts the new chain
  - So everyone knows which is the new chain...
  - When someone downloads a client, immediately the last valid chain is also downloaded by the client
What happens, when two blocks are made at the same time? -> both of them are chained at the end
But only the **longest** blockchain is accepted as „THE” blockchain!
- When there are two possible paths, the one which continues earlier will be accepted
- The other path’s blocks will be unchained

„orphan” blocks : these will be unchained soon and the transactions in it will be released (they will be included in the next few blocks)
Bitcoin: the basics

- E.g. What happens when we buy a glass of beer?

Your payment MAY get valid here...

1. Transaction 1
   Transaction 5
   Transaction 34
   Transaction S4
   Transaction 65
   Memory pool

2. Node

3. Miner
   Validates all transactions
   and creates a block

4. Block gets added to the node's Blockchain

[*] Picture resource: on.tech.eu
But why are these structures (block, blockchain) necessary?
At this point we only know, that if one amount of bitcoins are already spent (=is in an old transaction), the new transaction with these bitcoins are discarded.
When someone starts to make a new block, he/she must be sure, that
- All transactions are valid
- The blockchain is valid
Bitcoin: under the hood

- **Fourth problem:** *Okay, but it is not a big deal to calculate the hashes of the blocks of a fake blockchain...*

- **Proof-of-work**
  - When someone makes a block (and gets money for it) he/she must solve a **cryptographic problem**
  - The hash value of the block must be lower than a *pregenerated number* – in other words the hash must be like this:

  \[
  00000...00|X
  \]
I think this is the real meaning of mining: you mine bitcoins by „mining” an acceptable random nonce for a block...
Bitcoin: under the hood

- How difficult is to solve the cryptographic problem?
  - One new block should be made in every 10 minutes (for this reason, the difficulty is changed in every 2 weeks if necessary)

- Now, if laszlo wants to corrupt the last n blocks of the chain, he must solve n cryptographic problems
  - 10 min/block ratio is calculated for large mining pools!
  - But laszlo is alone, he can only make one proof-of-work in hours → during this time a lot of new blocks appear in the chain!
Bitcoin: under the hood

- So the only chance of laszlo is, if he enslaves 50% of the world...

- If this happens, he has 50% chance!

[*] Picture ref.: http://optilux.deviantart.com/
Bitcoin: under the hood

- Now we can see why bitcoin miners get BTC for mining:
  - Not just to invest new bitcoins in the system...
  - Mining requires a lot of energy (this energy loss must be paid)
  - Fairness!

- Today there are **mining pools** with hundreds of GPU-s (and nowadays FPGA-s)
Bitcoin: what we did not discuss

- What kind of algorythm verify the transactions?
  - Scripting system

- How can be the blockchain easily managed?
  - Merkle-trees

- How can BTC be fully anonym on the web?
  - Tor networks

- What kind of messages are in the BTC network?

https://bitcoin.org/en/developer-guide#transactions
# Bitcoin: under the hood

### Inputs

<table>
<thead>
<tr>
<th>Previous output (index)</th>
<th>Amount</th>
<th>From address</th>
<th>Type</th>
<th>ScriptPubKey</th>
</tr>
</thead>
<tbody>
<tr>
<td>3841141700828...1</td>
<td>10</td>
<td>30450212009c7b273172a4d970692c1c33371c041c2b6552d7b170a270968372649003c3</td>
<td>Address</td>
<td></td>
</tr>
<tr>
<td>6f08e5739c0...0</td>
<td>5</td>
<td>30450212009c7b273172a4d970692c1c33371c041c2b6552d7b170a270968372649003c3</td>
<td>Address</td>
<td></td>
</tr>
<tr>
<td>444644e4c8bb...1</td>
<td>10</td>
<td>30450212009c7b273172a4d970692c1c33371c041c2b6552d7b170a270968372649003c3</td>
<td>Address</td>
<td></td>
</tr>
</tbody>
</table>

### Outputs

<table>
<thead>
<tr>
<th>Index</th>
<th>Redeemed at input</th>
<th>Amount</th>
<th>To address</th>
<th>Type</th>
<th>ScriptPubKey</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Not yet redeemed</td>
<td>25</td>
<td>30450212009c7b273172a4d970692c1c33371c041c2b6552d7b170a270968372649003c3</td>
<td>Address</td>
<td></td>
</tr>
</tbody>
</table>

30
Countermeasures

- Deflation
  - The most mentioned problem with bitcoin
  - In every 4 years, the mining reward is halved (now it is 25 BTC), and in ~2140 no more new bitcoins will be added!
  - Because of this, deflation is a potential end for Bitcoin

- Possible loss of our money
  - If someone loses his/her private key – the money is gone...

- Economy
  - Today hundreds of thousands of GPU-s are working on just solving cryptographic problems to earn BTC
  - In a perspective, this is a waste of energy
Deflation

Money: Bitcoin's deflation problem | The Economist

https://www.economist.com/blogs/professionals/2014/04/bitcoin

Bitcoin Doesn’t Have a Deflation Problem - Forbes


Bitcoin Doesn’t Have A Deflation Problem - Business Insider

https://www.businessinsider.com/bitcoin-doesnt-have-a-deflation-problem
References (HU)

- Bitcoin.hu – Hungarian Bitcoin Portal

- An article from player.hu

  Bitcoin – Laci másfél milliárdos sonkás-gombás pizzája
References (EN)

- The original Bitcoin paper from Nakamoto

  \textit{Bitcoin: A Peer-to-Peer Electronic Cash System}
  
  Satoshi Nakamoto
  satsoshn@gmx.com
  www.bitcoin.org

- Bitcoin wiki
References (EN)

- Bitcoin Monitor

  ![Bitcoin Monitor](image)

  Bitcoin is a peer-to-peer digital currency. This website visualizes the activities on the Bitcoin network: coins being moved around (transactions), recording and tamper-proofing the history of events (block creation) and exchanges with other currencies taking place (currency trades).

- Bitcoin Block Explorer

<table>
<thead>
<tr>
<th>Number</th>
<th>Hash</th>
<th>Time</th>
<th>Transactions</th>
<th>Total BTC</th>
<th>Size (kB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>220901</td>
<td>c6d186edf7</td>
<td>2014-11-20 21:08:12</td>
<td>761</td>
<td>2752.3253172</td>
<td>398.379</td>
</tr>
<tr>
<td>220900</td>
<td>816112865</td>
<td>2014-11-20 20:59:10</td>
<td>639</td>
<td>17374.80524646</td>
<td>348.86</td>
</tr>
</tbody>
</table>
Any questions?