Bitcoin e le tecnologie delle criptovalute
Stato dell’arte e prospettive future

Fabrizio Venettoni
Giulio Magnanini

Roma 22 gennaio 2018
Agenda

- Richiami sui principi e i meccanismi di funzionamento di Bitcoin
- Schemi di decentralizzazione alternativi. Community, politica e regolamentazione
- Ecosistema delle cripto valute e coin alternativi
- Sviluppi futuri e possibili applicazioni: un progetto concreto
What is Bitcoin

A decentralized P2P e-cash system based on cryptographic proof instead of a third party to get trust, ensuring anonymity between peers (2008, Satoshi Nakamoto)

- Money is authentic and not counterfeit
- It can only be spent once
- No one else can claim it belongs to them and not me

Transactions are like lines in a double-entry bookkeeping ledger. Each transaction contains one or more “inputs”, which are like debits against a bitcoin account. On the other side of the transaction, there are one or more “outputs,” which are like credits added to a bitcoin account. The inputs and outputs (debits and credits) do not necessarily add up to the same amount. Instead, outputs add up to slightly less than inputs and the difference represents an implied transaction fee, which is a small payment collected by the miner who includes the transaction in the ledger. A bitcoin transaction is shown as a bookkeeping ledger entry.
...are mined together in a chain of blocks

Hash chain of blocks

Merkle tree of transactions in each node
∃Nonce | SHA256(Prev Hash, MerkleTree, Nonce) ≤ Target
A mechanism to reach global decentralized consensus

Bitcoin e le tecnologie delle cripto valute: stato dell’arte e prospettive future
Double spending attack

signed by \( pk_{Alice} \)
Pay to \( pk_{Bob} : H(\cdot) \)

signed by \( pk_{Goofy} \)
Pay to \( pk_{Alice} : H(\cdot) \)

signed by \( pk_{Goofy} \)
CreateCoin [uniqueCoinID]

1 confirmation
3 confirmations

double-spend attempt

Hear about \( C_A \rightarrow B \) transaction
0 confirmations

Double-spend probability decreases exponentially with # of confirmations

Most common heuristic:
6 confirmations
In the 1st scenario, for IC2 to be satisfied, **Lieutenant 1 must obey the order to attack.** In the 2nd, Lieutenant 1 does not know who the traitor is, and he cannot tell what message the commander actually sent to Lieutenant 2. Hence, the two scenarios appear exactly the same to Lieutenant 1. If the traitor lies consistently, then there is no way for Lieutenant 1 to distinguish between these two situations, so he must obey the "attack" order in both of them. Hence, whenever Lieutenant 1 receives an "attack" order from the commander, he must obey it.

However, a similar argument shows that if Lieutenant 2 receives a "retreat" order from the commander then he must obey it, even if Lieutenant 1 tells him that the commander said "attack". Therefore, in the scenario of Figure 2, Lieutenant 2 must obey the "retreat" order while Lieutenant 1 obeys the "attack" order, thereby violating condition IC1.

**Hence, no solution exists for three generals that works in the presence of a single traitor.**

The main P2P Net consists of up to 12K nodes
**Bitcoin limitations & improvements**

*Hard coded limits*

- 10 min avg. creation time per block
- 1 Mb in a block
- 20K signature operations per block
- 100M satoshis per bitcoin
- 21M total bitcoin maximum
- Mining reward rate: 50, 25, 12.5, …
- Hash functions
- Only 1 signature algorithm (ECDSA, P256)

- Economic effect too much to change now
- Crypto primitives might break by 2040
Hard & soft forking changes

Old nodes will never catch up

Adding new features which can only limit the set of valid transactions; Need majority of nodes to enforce new rules; Old nodes will approve (even mining now-invalid blocks)
Agenda

• Richiami sui principi e i meccanismi di funzionamento di Bitcoin

• Schemi di decentralizzazione alternativi. Community, politica e regolamentazione

• Ecosistema delle cripto valute e coin alternativi

• Sviluppi futuri e possibili applicazioni: un progetto concreto
A good puzzle scheme prevent miners domination

- Contrast ASIC
- Prevent large pools
- It’s Intrinsic usefulness
- Eliminate the need for mining HW at all
Alternative puzzle schemes

- Proof of (useful) work
- Non outsourceable puzzle
- Virtual Mining
  - Stake of a coin grows over time as long as the coin is used
  - Mining with a coin destroys it
  - Mining with deposit (can reclaim a coin after time)
  - Proof of activity: any coin might win (if online)
Developers, miners or investors who has the power?

Rules

History

Coins are valuable
Legality around the world

Bitcoin e le tecnologie delle cripto valute: stato dell’arte e prospettive future
Untraceable digital cash facilitates some crimes…

- Kidnapping and extortion
- Tax evasion
- Sale of illegal items
- Crossing borders
- Money laundering

from BitLicence to BTC futures
Agenda

• Richiami sui principi e i meccanismi di funzionamento di Bitcoin

• Schemi di decentralizzazione alternativi. Community, politica e regolamentazione

• Ecosistema delle cripto valute e coin alternativi

• Sviluppi futuri e possibili applicazioni: un progetto concreto
<table>
<thead>
<tr>
<th>#</th>
<th>Name</th>
<th>Market Cap</th>
<th>Price</th>
<th>Volume (24h)</th>
<th>Circulating Supply</th>
<th>Change (24h)</th>
<th>Price Graph (7d)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Bitcoin</td>
<td>$197,022,131.955</td>
<td>$11,715,00</td>
<td>$10,008,800,000</td>
<td>16,817,937 BTC</td>
<td>-8.20%</td>
<td><img src="image1" alt="Graph" /></td>
</tr>
<tr>
<td>2</td>
<td>Ethereum</td>
<td>$103,060,172.111</td>
<td>$1,061,07</td>
<td>$3,376,720,000</td>
<td>97,128,533 ETH</td>
<td>-7.22%</td>
<td><img src="image2" alt="Graph" /></td>
</tr>
<tr>
<td>3</td>
<td>Ripple</td>
<td>$54,491,640.452</td>
<td>$1,41</td>
<td>$2,917,550,000</td>
<td>38,739,142,811 XRP *</td>
<td>-9.88%</td>
<td><img src="image3" alt="Graph" /></td>
</tr>
<tr>
<td>4</td>
<td>Bitcoin Cash</td>
<td>$30,402,066.513</td>
<td>$1,796,34</td>
<td>$736,866,000</td>
<td>16,924,450 BCH</td>
<td>-9.94%</td>
<td><img src="image4" alt="Graph" /></td>
</tr>
<tr>
<td>5</td>
<td>Cardano</td>
<td>$15,856,011.112</td>
<td>$0,611,562</td>
<td>$817,450,000</td>
<td>25,927,070,538 ADA *</td>
<td>-12.23%</td>
<td><img src="image5" alt="Graph" /></td>
</tr>
<tr>
<td>6</td>
<td>Litecoin</td>
<td>$10,554,469.619</td>
<td>$192,38</td>
<td>$465,688,000</td>
<td>54,861,758 LTC</td>
<td>-7.71%</td>
<td><img src="image6" alt="Graph" /></td>
</tr>
<tr>
<td>7</td>
<td>NEM</td>
<td>$9,714,779.999</td>
<td>$1,08</td>
<td>$99,918,700</td>
<td>8,999,999,999 XEM *</td>
<td>-9.66%</td>
<td><img src="image7" alt="Graph" /></td>
</tr>
<tr>
<td>8</td>
<td>NEO</td>
<td>$8,700,380.000</td>
<td>$133,85</td>
<td>$351,437,000</td>
<td>65,000,000 NEO *</td>
<td>-9.33%</td>
<td><img src="image8" alt="Graph" /></td>
</tr>
<tr>
<td>9</td>
<td>EOS</td>
<td>$8,437,804.128</td>
<td>$13,62</td>
<td>$2,906,610,000</td>
<td>619,465,691 EOS *</td>
<td>-10.14%</td>
<td><img src="image9" alt="Graph" /></td>
</tr>
<tr>
<td>10</td>
<td>Stellar</td>
<td>$8,404,799.980</td>
<td>$0,469,738</td>
<td>$161,314,000</td>
<td>17,892,527,281 XLM *</td>
<td>-10.91%</td>
<td><img src="image10" alt="Graph" /></td>
</tr>
</tbody>
</table>
Better security, more features, different parms, policies

**Early altcoins**

- **namecoin**
- **litecoin**
- **peercoin**
- **D**

**Sample platforms**

- **ETHEREUM**
- **aeternity**
- **RCHAIN COOPERATIVE**
- **STELLAR**
Agenda

• Richiami sui principi e i meccanismi di funzionamento di Bitcoin

• Schemi di decentralizzazione alternativi. Community, politica e regolamentazione

• Ecosistema delle cripto valute e coin alternativi

• Sviluppi futuri e possibili applicazioni: un progetto concreto
A software application for issuers of premium bonds to manage direct retail offers based on the Ethereum blockchain
Bibliografia


Andreas M. Antonopoulos, *Mastering Bitcoin – Programming the open blockchain*, 2017


Contatti

- fabrizio.venettoni@cdp.it
- giu.magnanini@gmail.com

Grazie...