The Future of Bitcoin and Cryptocurrencies

MODERATOR: Bart Preneel
Professor
KU Leuven and iMinds
@CosicBe

PANELISTS:
Joseph Bonneau
Researcher
Stanford University and EFF
@josephbonneau

Greg Maxwell
CTO
Blockstream
@Blockstream

Adi Shamir
Professor
The Weizmann Institute
Bitcoin (°2008)

- Digital currency with distributed generation and verification

- Transactions
  - irreversible
  - inexpensive
  - over anonymous peer-to-peer network
  - broadcast within seconds and verified within 10 to 60 minutes by inclusion in hash chain
  - double spending prevention using a public decentralized ledger (block chain)

- Pseudonymous (believed by many to be anonymous)
Bitcoin Transaction

Transaction A
- In: 50 BTC
- Out: 8 BTC
- Out: 42 BTC

Transaction B
- In: 10 BTC
- Out: 15 BTC
- Out: 6 BTC

Transaction C
- In: 10 BTC
- Out: 7 BTC
- Out: 6 BTC
Increment counter in block header until block hash has many leading zeroes
## Block #359391

<table>
<thead>
<tr>
<th>Summary</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Number Of Transactions</td>
<td>534</td>
</tr>
<tr>
<td>Output Total</td>
<td>5,027.57450746 BTC</td>
</tr>
<tr>
<td>Estimated Transaction Volume</td>
<td>1,557.11401964 BTC</td>
</tr>
<tr>
<td>Transaction Fees</td>
<td>0.02377486 BTC</td>
</tr>
<tr>
<td>Height</td>
<td>359391 (Main Chain)</td>
</tr>
<tr>
<td>Timestamp</td>
<td>2015-06-04 14:37:52</td>
</tr>
<tr>
<td>Difficulty</td>
<td>47,589,591,153.83</td>
</tr>
<tr>
<td>Bits</td>
<td>404167307</td>
</tr>
<tr>
<td>Size</td>
<td>368.59796875 KB</td>
</tr>
<tr>
<td>Version</td>
<td>3</td>
</tr>
<tr>
<td>Nonce</td>
<td>1031353973</td>
</tr>
<tr>
<td>Block Reward</td>
<td>25 BTC</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Hashes</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Hash</td>
<td>0000000000000000000000126c7a8fd3833654f17f95d7d09d88a45872807bee4b25</td>
</tr>
<tr>
<td>Previous Block</td>
<td>0000000000000000000000136efac03881239f0e42f8ce6ba375e07f8be4776d94685</td>
</tr>
<tr>
<td>Merkle Root</td>
<td>e6d3f8630fb4590c41676f4a6f4d230e12f1ea04a42347d2ab6bca21c68</td>
</tr>
</tbody>
</table>
Mining Difficulty Level (https://blockchain.info/stats)

- Target: mining 1 block should take roughly 10 minutes
- Update level every 2016 blocks
Mining Hash Rate of Bitcoin Network

$10^{18} \text{ Hash/sec} = 2^{59.8} \text{ /sec} \text{ or } 2^{7.2} \text{ /day}$
The block chain normally is one long chain

Distributed nature of the network can lead to forks:

- Longest chain will become the main chain
- Transactions in orphan blocks are rebroadcast
- Transaction is typically accepted after it is included in 6 blocks (60 minutes)
Miners Revenue USD (https://blockchain.info STATS)
Market price in USD (https://blockchain.info/stats)

2011 bubble
Market Capitalization (https://blockchain.info/stats)

2011 bubble