Week 4: Network + Mining

Proj 1 due Thursday
Recap: 3 protocols

* Consensus
* Transactions
* Network
Bitcoin "nodes"

- full nodes
- lite nodes (track block headers)

miners

non-miners (entire blockchain) track
Chancellor on brink of second bailout for banks
Validate the blockchain

- Prev block pointers

General:
- Puzzle solution \( \sim H(\text{block}) < \text{target} \)
- Timestamp \(< < 2 \text{ hours future (UTC)} \)
  \( \Rightarrow \text{med (prev. 11 blocks)} \)

TX:
- All TX valid
- No money created/destroyed (except coinbase)

Chains:
- "Longest" chain (most difficult)
- Tiebreaker: first relayed
- Root is genesis block
Block Propagation Times

Yonatan Sompolinsky and Aviv Zohar: “Accelerating Bitcoin’s Transaction Processing” 2014
P2P network
  - goal: broadcast txs, blocks

P2P Net attacks:
  - Split view
  - Eclipse
  - DoS
  - front running

*Intersection* (ISP)
  (Tor exit node)
Bitcoin miners

- Run a full node
- Listen for new tx
- Assemble a merkle tree of tx
- Solve puzzle (find valid nonce)
- Profit! ($50K)

P2P Network

Node

Merkle root

Block

Hardware

Software

32 bytes

Centralized per 2^32 hosts
target / difficulty

update every 2016 blocks (2 weeks)

new target: \( \left( \frac{\text{time}^{\frac{1}{16,000}}}{\text{old target}} \right)^{20,160} \)

target 0x0000...00m 000000
Proof-of-burn (probably unspeakable)

ScriptPubKey:

\[
\begin{cases}
\text{FALSE} \\
\text{<40 bytes of data>} \\
\text{OP-RETURN} + 40 \text{ bytes of data}
\end{cases}
\]

Not provably unspendable

P2PKH -> random data 0x000... 00 0x deadbeef

🤔
<table>
<thead>
<tr>
<th>Year</th>
<th>Platform</th>
<th>Speed</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt; 2010</td>
<td>CPU</td>
<td>$2^0$, $2^{24}$ H/s</td>
</tr>
<tr>
<td>2010, 2011</td>
<td>GPU</td>
<td>$2^{27}$ H/s</td>
</tr>
<tr>
<td>2011, 2012</td>
<td>FPGA</td>
<td>$2^{30}$ H/s</td>
</tr>
<tr>
<td>2012+</td>
<td>ASIC</td>
<td>$2^{44}$ H/s</td>
</tr>
</tbody>
</table>
Brand New Bitmain Antminer S9 bitcoin miner Mining BTC 11.85TH Super-Efficient

Item condition: "Brand New Still in the Box As Received From Bitmain"

Price: US $1,799.95

Shipping: FREE Standard Shipping

Delivery: Estimated between Fri. Oct. 7 and Mon. Oct. 17

Payments: PayPal, Visa, Mastercard, American Express, Discover

Seller information
quickclick1194 (789)
100% Positive feedback

Follow this seller
Visit store: flybymemories
See other items
Ant miner S9:

1-year outcomes

0 blocks: 92.0%
1 block: 7.5
2 blocks+: 0.5%

Mining pool: share profit/risk w/ other miners that you don't trust
Next time:
  • Mining pools
  • Mining strategies | game theory