Brief Tutorial on Bitcoins

Abde Ali Kagalwalla
What is Bitcoin?

Casascuis

- Protocol to manage digital currency and process payments between users
- First proposed by “Satoshi Nakamoto”
- No central authority (Federal Reserve) or banks to manage transactions
- Decentralized, P2P system
Valuation of bitcoin

Market Price (USD)
Source: blockchain.info
Digital Signature (Image Source: Wikipedia)

**Signing**
- Data
- Hash function
- Hash: 101100110101
- Encrypt hash using signer's private key
- Signature: 111101101110
- Certificate
- Attach to data
- Digitally signed data

**Verification**
- Digitally signed data
- Decrypt using signer's public key
- Signature: 111101101110
- Data
- Hash function
- Hash: 101100110101
- ?
- Hash: 101100110101
- If the hashes are equal, the signature is valid.
Bitcoin Transactions via Digital Signature

I, Abde Ali, wish to transfer 7 bitcoins to Liangzhen

- Online transactions currently verified by a bank
  - Does Abde Ali own enough bitcoins?
  - Double spending: Abde Ali should not be able to use the same bitcoins to pay Weiche
- Can a bank be completely eliminated from the online payment transfer protocol?
  - \( \rightarrow \) Ingenuity of Bitcoin
Decentralized Transaction Verification: Block Chain

- Public ledger of transactions
- A set of transactions referred to as a ‘block’
- All verified blocks are added to the global block chain
- Liangzhen can look at the block chain and check if Abde Ali is not cheating
- Problem: What if Abde Ali tries to pay both Liangzhen and Weiche at the same time?
Prevent Double Spending: Computationally Intensive Verification

- Potential Solution: Both Liangzhen and Weiche publicly release the digital message and request all users to verify.
- Problem: Abde Ali can create millions of users that will validate both transactions.
- Bitcoin solution is to make verification computationally expensive using a proof-of-work protocol:
  - Solve a artificially challenging puzzle to verify a block chain.
  - Reward users who verify blocks with new ‘mined’ bitcoins.
  - This verification is done by bitcoin miners.
Bitcoin Mining Challenge Puzzle: Proof-of-Work

- Since hash function is ‘almost’ random, $2^K$ attempts are required to solve the challenge
- On average blocks are verified in 10 minutes
- The successful miner is rewarded with 25 newly generated bitcoins
  - Number of bitcoins generated will be halved after every 210,000 validated blocks
  - Bitcoin generation will stop once the reward less than $10^{-8}$ (Minimum unit called Satoshi)
  - Miners also receive transaction fees
## Bitcoin Mining Infrastructure

- Initially Satoshi’s open source software could be used on any CPU → No longer viable
- GPU and FPGA based mining is fairly popular
- ASIC solutions are the most viable option now

### Comparison of FPGA and ASIC Chips

<table>
<thead>
<tr>
<th></th>
<th>Spartan6-150</th>
<th>BFL Single</th>
<th>BFL miniRig</th>
<th>Avalon</th>
<th>BFL</th>
<th>ASICminer</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Type</strong></td>
<td>Xilinx FPGA</td>
<td>Altera FPGA</td>
<td>FPGA</td>
<td>ASIC</td>
<td>ASIC</td>
<td>ASIC</td>
</tr>
<tr>
<td><strong>Process</strong></td>
<td>45 nm</td>
<td>45 nm (?)</td>
<td>45 nm (?)</td>
<td>110 nm</td>
<td>65 nm</td>
<td>130 nm</td>
</tr>
<tr>
<td><strong>Hash Rate Per Chip</strong></td>
<td>210 MH/s</td>
<td>415 MH/s</td>
<td>650-750 MH/s</td>
<td>280 MH/s</td>
<td>4 GH/s</td>
<td>300 MH/s</td>
</tr>
<tr>
<td><strong>Power Draw</strong></td>
<td>15 W</td>
<td>40 W</td>
<td>35 W</td>
<td>2.8 W</td>
<td>30 W</td>
<td>2.5 W</td>
</tr>
<tr>
<td><strong>Efficiency (MH/s per W)</strong></td>
<td>14</td>
<td>10</td>
<td>20</td>
<td>100</td>
<td>133</td>
<td>120</td>
</tr>
<tr>
<td><strong>US$ / MH/s</strong></td>
<td>1 to 2.5</td>
<td>0.75</td>
<td>0.6</td>
<td>Varies</td>
<td>Varies</td>
<td>Varies</td>
</tr>
<tr>
<td><strong>Notes</strong></td>
<td>Typically 1 to 4 FPGAs Per Board</td>
<td>2 FPGAs Per Board</td>
<td>2 FPGAs Per Board, 17 to 18 Boards</td>
<td>Priced In BTC (prices increase)</td>
<td>BFL Anticipates A Slight Reduction In Power Draw</td>
<td>Priced In BTC (prices increase)</td>
</tr>
</tbody>
</table>
Comparison of Bitcoin Mining Hardware: https://bitcoinwisdom.com/bitcoin/calculator
Bitcoin Mining Pools

• Bitcoin mining is a very risky venture
  – As soon as one miner solves the puzzle, all others must restart on the next block

• Typically done in pools
  – All miners in pool share rewards for a successful mine
  – Miners who contribute more ‘partial’ solutions get greater share of reward
  – Several different miners with different protocols for joining, sharing, etc.
References

