BitCoin
“Consensus” without Paxos

Jinyang Li
What we’ve learnt so far

• So far we discussed distributed systems within data centers
  – **closed** system
    • Managed by a single administrative entity (e.g. Google)
    • Only chosen machines participate
    • Participating machines are trusted (cooperative)

• Ideal consisency (linearizability)
  – Paxos for consensus (MultiPaxos for linearizable replication)
Today: BitCoin

• Very different from all other systems we’ve discussed in this class
• BitCoin is peer-to-peer (aka open system; aka decentralized)
  – any machine can participate in the protocol
  – no single administrative entity
• BitCoin is the first practical cryptocurrency
Many cryptocurrencies exist today

<table>
<thead>
<tr>
<th>#</th>
<th>Name</th>
<th>Symbol</th>
<th>Market Cap</th>
<th>Price</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Bitcoin</td>
<td>BTC</td>
<td>$130,614,483,900</td>
<td>$7,217.80</td>
</tr>
<tr>
<td>2</td>
<td>Ethereum</td>
<td>ETH</td>
<td>$15,609,501,022</td>
<td>$143.18</td>
</tr>
<tr>
<td>3</td>
<td>XRP</td>
<td>XRP</td>
<td>$9,611,176,686</td>
<td>$0.222041</td>
</tr>
<tr>
<td>4</td>
<td>Tether</td>
<td>USDT</td>
<td>$4,149,632,878</td>
<td>$1.01</td>
</tr>
<tr>
<td>5</td>
<td>Bitcoin Cash</td>
<td>BCH</td>
<td>$3,760,231,388</td>
<td>$207.05</td>
</tr>
<tr>
<td>6</td>
<td>Litecoin</td>
<td>LTC</td>
<td>$2,799,464,202</td>
<td>$43.87</td>
</tr>
<tr>
<td>7</td>
<td>EOS</td>
<td>EOS</td>
<td>$2,433,406,956</td>
<td>$2.58</td>
</tr>
<tr>
<td>8</td>
<td>Binance Coin</td>
<td>BNB</td>
<td>$2,300,230,276</td>
<td>$14.79</td>
</tr>
<tr>
<td>9</td>
<td>Bitcoin SV</td>
<td>BSV</td>
<td>$1,712,594,306</td>
<td>$94.78</td>
</tr>
<tr>
<td>10</td>
<td>Stellar</td>
<td>XLM</td>
<td>$1,072,400,253</td>
<td>$0.053474</td>
</tr>
<tr>
<td>11</td>
<td>Tezos</td>
<td>XTZ</td>
<td>$1,045,408,692</td>
<td>$1.58</td>
</tr>
<tr>
<td>12</td>
<td>Cardano</td>
<td>ADA</td>
<td>$943,332,207</td>
<td>$0.036384</td>
</tr>
<tr>
<td>13</td>
<td>TRON</td>
<td>TRX</td>
<td>$941,480,177</td>
<td>$0.014119</td>
</tr>
<tr>
<td>14</td>
<td>Monero</td>
<td>XMR</td>
<td>$922,854,808</td>
<td>$53.19</td>
</tr>
<tr>
<td>15</td>
<td>UNUS SED LEO</td>
<td>LEO</td>
<td>$895,162,292</td>
<td>$0.895611</td>
</tr>
<tr>
<td>16</td>
<td>Chainlink</td>
<td>LINK</td>
<td>$760,929,642</td>
<td>$2.17</td>
</tr>
<tr>
<td>17</td>
<td>Cosmos</td>
<td>ATOM</td>
<td>$700,771,457</td>
<td>$3.67</td>
</tr>
<tr>
<td>18</td>
<td>Huobi Token</td>
<td>HT</td>
<td>$659,345,613</td>
<td>$2.73</td>
</tr>
<tr>
<td>19</td>
<td>NEO</td>
<td>NEO</td>
<td>$601,172,356</td>
<td>$8.52</td>
</tr>
<tr>
<td>20</td>
<td>IOTA</td>
<td>MIOTA</td>
<td>$548,419,195</td>
<td>$0.197306</td>
</tr>
<tr>
<td>21</td>
<td>Maker</td>
<td>MKR</td>
<td>$487,468,289</td>
<td>$487.47</td>
</tr>
<tr>
<td>22</td>
<td>USD Coin</td>
<td>USDC</td>
<td>$476,659,583</td>
<td>$1.00</td>
</tr>
<tr>
<td>23</td>
<td>Dash</td>
<td>DASH</td>
<td>$458,772,455</td>
<td>$49.84</td>
</tr>
<tr>
<td>24</td>
<td>Ethereum Classic</td>
<td>ETC</td>
<td>$437,982,799</td>
<td>$3.78</td>
</tr>
<tr>
<td>25</td>
<td>Ontology</td>
<td>ONT</td>
<td>$377,364,902</td>
<td>$0.592083</td>
</tr>
<tr>
<td>26</td>
<td>Crypto.com Coin</td>
<td>CRO</td>
<td>$354,331,561</td>
<td>$0.028905</td>
</tr>
<tr>
<td>27</td>
<td>VeChain</td>
<td>VET</td>
<td>$340,409,619</td>
<td>$0.006139</td>
</tr>
<tr>
<td>28</td>
<td>NEM</td>
<td>XEM</td>
<td>$318,590,385</td>
<td>$0.035399</td>
</tr>
<tr>
<td>29</td>
<td>HedgeTrade</td>
<td>HEDG</td>
<td>$316,690,402</td>
<td>$1.10</td>
</tr>
<tr>
<td>30</td>
<td>Dogecoin</td>
<td>DOGE</td>
<td>$267,317,646</td>
<td>$0.002184</td>
</tr>
<tr>
<td>31</td>
<td>Zcash</td>
<td>ZEC</td>
<td>$257,270,522</td>
<td>$31.98</td>
</tr>
<tr>
<td>32</td>
<td>Basic Attention Token</td>
<td>BAT</td>
<td>$249,147,055</td>
<td>$0.176581</td>
</tr>
<tr>
<td>33</td>
<td>Paxos Standard</td>
<td>PAX</td>
<td>$235,429,426</td>
<td>$1.00</td>
</tr>
<tr>
<td>34</td>
<td>Decred</td>
<td>DCR</td>
<td>$215,145,044</td>
<td>$19.95</td>
</tr>
<tr>
<td>35</td>
<td>Synthetix Network Token</td>
<td>SNX</td>
<td>$199,061,096</td>
<td>$1.33</td>
</tr>
<tr>
<td>36</td>
<td>Qtum</td>
<td>QTUM</td>
<td>$166,751,675</td>
<td>$1.73</td>
</tr>
<tr>
<td>37</td>
<td>TrueUSD</td>
<td>TUSD</td>
<td>$160,615,128</td>
<td>$1.00</td>
</tr>
<tr>
<td>38</td>
<td>0x</td>
<td>ZRX</td>
<td>$135,904,003</td>
<td>$0.224850</td>
</tr>
<tr>
<td>39</td>
<td>Centrality</td>
<td>CENNZ</td>
<td>$131,896,923</td>
<td>$0.123332</td>
</tr>
<tr>
<td>40</td>
<td>Algorand</td>
<td>ALGO</td>
<td>$131,445,164</td>
<td>$0.283688</td>
</tr>
</tbody>
</table>
BitCoin’s (original) goal

<table>
<thead>
<tr>
<th>Pros/cons of cash</th>
<th>Pros/cons of credit cards</th>
</tr>
</thead>
<tbody>
<tr>
<td>✓ Portable</td>
<td>✓ works online</td>
</tr>
<tr>
<td>✓ no need for trusted 3rd party</td>
<td>✓ X can repudiate</td>
</tr>
<tr>
<td>✓ anonymous</td>
<td>✓ requires trusted 3rd party</td>
</tr>
<tr>
<td>X Does not work online</td>
<td>X tracks one’s purchases</td>
</tr>
<tr>
<td>X hard to monitor/tax</td>
<td>X can prohibit some transactions</td>
</tr>
<tr>
<td>X need government to print them</td>
<td>X easy to monitor/tax/control</td>
</tr>
</tbody>
</table>

BitCoin: e-cash without a central trusted party
What’s hard socially/economically

• Why does e-cash have value?
• How to pay for infrastructure?
• What should be the monetary policy?
• What about laws? (taxes, money laundering, drugs, terrorists)
What’s hard technically?

• Forgery
• Theft
• Double spending
Cryptography background

• Public key crypto
  – Each key comes in a pair \( K, K^{-1} \)
  – \( e \leftarrow \text{Encrypt(data, } K \text{ )}, \text{ data } \leftarrow \text{Decrypt(e, } K^{-1} \text{ )} \)
  – \{data\}_{K^{-1}} \leftarrow \text{Sign(data, } K^{-1} \text{ )}, \text{ verify}(\text{signature, } K) \)

• Cryptographic hash function (e.g. SHA-256)
  – \( h_x \leftarrow \text{Hash(x)} \)
  – Property:
    • deterministic: same input \( \rightarrow \) same output
    • collision resistant: given h, it’s highly unlikely \( 2^{-256} \) to find \( x' \) such that \( \text{hash}(x') = h = \text{hash}(x) \)
Key idea #1: Cryptocurrency

- Ownership of currency
  - = possession of some private key

- Transfer of currency
  - = signing “ownership” away to another party

- A “coin” is a transaction record

- T1: A transfers a coin to B

- T2: B transfers the coin to C

- How to ensure T2 is spending the same coin of T1? (i.e. how to link T2 to T1)
Key idea #1: Cryptocurrency

• Problem: How to link transaction records?
• Strawman: serial number
  – If T1, T2 contain the same serial#, then they refer to the same coin.
  – Problem: did T1 come before T2? or vice versa?
• Idea: a secure chain of transaction records

T2: \{hash(T_1), B_{pub} \rightarrow C_{pub}\}_B

{\bullet, A_{pub} \rightarrow B_{pub}}_{A^{-1}} \quad \{\bullet, B_{pub} \rightarrow C_{pub}\}_{B^{-1}}
User-B

I’d like to buy a pizza

\[ \{\bullet, A \rightarrow B\}_{A^{-1}} \rightarrow \{\bullet, B \rightarrow C\}_{B^{-1}} \]

User-C

Your transaction is valid!
What’s hard technically?

- Forgery
- Theft
- Double spending

Pizza please

\[\{\bullet, A \rightarrow B\}_{A^{-1}} \quad \{\bullet, B \rightarrow C\}_{B^{-1}}\]

noddle please

\[\{\bullet, A \rightarrow B\}_{A^{-1}} \quad \{\bullet, B \rightarrow D\}_{B^{-1}}\]
How to defend against double-spending?

• Strawman: use a central trusted party (CP)
• Users submit all transactions to the CP
• CP verifies that no doublespending
  – User-B signs T2 and gives it to User-C. User-C asks CP to verify T2 before giving pizza to User-B.
  – Later User-B signs T3 to give the same coin to User-D. What happens?

✗ No longer peer-to-peer
Idea #2: Maintain a global log (ledger)

• All peers keep track of all transactions in a global log (“public ledger”).
  – Why log? (Why not a set?)
• Each transaction is replicated to all peers
• Forked log $\rightarrow$ double spending
• Problem: how to guarantee a non-forked log?
  – Can we run Raft/MultiPaxos among all peers?
Why not use Paxos/Raft to maintain the global ledger?

• Paxos does not scale to 10,000 nodes
• Paxos is not secure against malicious nodes
  – There’s a version of Paxos (PBFT, Castro&Liskov) that is secure if <1/3 nodes are malicious
• Vulnerable to Sybil attack
  – adversary joins the network with many identities so he controls >1/3 of all nodes
Idea #3: proof-of-work

- A peer can extend the log only after *provably* having done a lot of work.
The BlockChain

Each block has many transaction records

Prev hash needed to establish order and non-repudiation

Proof of work
The BlockChain: proof-of-work

• To extend the chain, peer needs to find nonce, s.t.:
  \[ \text{hash(block, nonce)} = \]

• There’s no better solution than brute-force
  – hash(block, 0) = ?
  – hash(block, 1) = ?
  – hash(block, 2) = ?
  – ....

• Running time? Difficulty= \(2^d\)
How to recover from “fork”s

• Two peers might “simultaneously” find different legitimate next blocks → forks in the chain
• Resolved by taking the longest chain as the main blockchain
• Unlike Paxos, blockchain does not guarantee consensus
  – It’s okay to temporarily disagree as long as eventual agreement is reached in reasonable time.
Dealing with transient forks

• A valid block may be on a main branch or a fork...

• A transaction is confirmed only after its block is followed by 5 valid successor blocks.
How difficult should proof-of-work be?

• What if set to be too hard?
  – limited transaction rate
  – longer transaction latency
• What if set to be too easy?
  – Higher chances of forking the main chain→ lots of wasted blocks.
• BitCoin: difficulty is set so that it takes entire network 10 minutes to find the next block
  – ~5 blocks wasted per day
  – How long to confirm a transaction?
How hard should proof-of-work be?

• How do peers agree on difficulty for block #n?
  – More peers \(\rightarrow\) harder for each peer

• For every 2016 blocks found, each peer sets the difficulty for the next (2016) blocks to be:
  – \(2 \text{ weeks} / T\)
    
    Time taken to find the prior 2016 blocks, according to their timestamps

• BitCoin’s transaction rate? (1MB block size, avg. transaction size 150B)
  – \((1\text{MB}/150\text{B})/600\text{sec} = 11 \text{ transactions/sec}\)
Bitcoin’s difficulty over years
Bitcoin’s incentives

• Why do people want to help with chain extension?

• Each new block contains a reward $X$ coins, hence extending blockchain is called “mining”
  – this is how money gets minted
  – $X$ halves every 210,000 blocks (~ 4 years), eventually stops after ~21 million coins
    – Currently $x=12.5$

• Miners charge users a transaction fee to include their transaction in the next block
The overall process
Shall I become a BitCoin miner now?

<table>
<thead>
<tr>
<th>Hash Rate TH/s</th>
<th>Jan '17</th>
<th>Mar '17</th>
<th>May '17</th>
<th>Jul '17</th>
<th>Sep '17</th>
<th>Nov '17</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intel core i7</td>
<td>24MHashes/sec</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>top-of-theline GPU</td>
<td>1GHashes/sec</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ASIC</td>
<td>1000 GHashes/sec</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Can Bitcoin scale well?

- Size of ledger grows over time
  - currently at 253GB
- Cost of signature checks substantial
- Need to go back to very old blocks to check validity of coins
Has BitCoin succeeded?

• In replacing cash/credit cards?
• Downsides of Bitcoin vs. cash
  – no true anonymity (ledger is public information)
• Downside of Bitcoin vs. credit cards
  – no disputes
  – no loss/recovery
• X Transactions take a long time to confirm.
• X With the soaring price, transaction fee is high ($20 in early 2018)
Alternative Cryptocurrencies

• BitCoin’s main problems:
  – Slow transaction rate
  – Wasteful (many CPU cycles wasted to mine blocks)
  – The chain of coin transfers is public

Stella, Algorand

zCash
Algorand’s approach at a high level

• Overall idea: Use Byzantine Agreement to agree on a ledger
  – BA avoids forking under certain assumptions
    • > 2/3 users are honest

• Challenges:
  – (Security) How to be resilient against Sybils?
    • Controlling >1/3 users is easy if an adversary can create arbitrarily many pseudonyms
  – (Scalability) How to make BA scale?
  – (Availability) How to defend against targeted attacks?
Algorand uses proof-of-stake

- Money as “weights”
- PKs associated with weights = relative fraction of money
  - Weights = # of votes a node can cast in BA
- Proof-of-stake is resilient to Sybil attacks
  - Attacker has to split wealth between pseudonyms
  - Total weights do not change by adding more pseudonyms
Algorand scales BA by sampling

• In traditional BA, every node broadcasts → does not scale

• Algorand samples a random committee using weights
  – Sampling computation uses private key, produces a non-interactive proof
  – Selected users originate messages; others gossip
Scale BA by sampling

• How large should the committee be?
  – Need $n \geq 3f+1$ participants to deal with $f$ bad users
  – Traditional BA wait for $2f+1$ votes on the same value
  – But selection is random!
    • No fixed $n/f$

Vote threshold is $2f+1$

Intersection must contain $\geq f+1$ nodes for safety
Scale BA by sampling

- Algorand’s threshold for votes

Probability of a committee contains >1/3 bad members for some step of the protocol
Want to learn more about cryptocurrency?

Take Prof Joseph Bonneau’s cryptocurrency class next Fall.
Final Exam Logistics

• Open book, no laptop/ipads
• Cover topics from the entire semester
• Length and format are similar to midterm
• Practice materials:
  – Preparation questions
  – Last year’s final will be posted on Piazza