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 consistency (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 (open system)
  – any machine can participate in the protocol
  – no single administrative entity
• BitCoin is the first practical cryptocurrency
<table>
<thead>
<tr>
<th>#</th>
<th>Name</th>
<th>Symbol</th>
<th>Market Cap</th>
<th>Price</th>
<th>Circulating Supply</th>
<th>Volume (24h)</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Bitcoin</td>
<td>BTC</td>
<td>$278,983,504,999</td>
<td>$166,666.20</td>
<td>16,739,287</td>
<td>$13,445,500,000</td>
<td>0.0</td>
</tr>
<tr>
<td>2</td>
<td>Ethereum</td>
<td>ETH</td>
<td>$669,998,162,741</td>
<td>$695.56</td>
<td>96,329,933</td>
<td>$4,773,510,000</td>
<td>0.3</td>
</tr>
<tr>
<td>3</td>
<td>Bitcoin Cash</td>
<td>BCH</td>
<td>$26,854,615,804</td>
<td>$1659.39</td>
<td>16,853,899</td>
<td>$1,250,520,000</td>
<td>-0.3</td>
</tr>
<tr>
<td>4</td>
<td>Ripple</td>
<td>XRP</td>
<td>$18,743,047,322</td>
<td>$0.483888</td>
<td>38,738,194,347</td>
<td>$3,173,380,000</td>
<td>-0.9</td>
</tr>
<tr>
<td>5</td>
<td>Litecoin</td>
<td>LTC</td>
<td>$16,733,251,630</td>
<td>$307.67</td>
<td>54,290,039</td>
<td>$3,650,300,000</td>
<td>0.6</td>
</tr>
<tr>
<td>6</td>
<td>IOTA</td>
<td>IOTa</td>
<td>$11,275,887,271</td>
<td>$4.06</td>
<td>2,779,530,283</td>
<td>$400,709,000</td>
<td>2.5</td>
</tr>
<tr>
<td>7</td>
<td>Dash</td>
<td>DASH</td>
<td>$6,833,126,208</td>
<td>$861.54</td>
<td>7,751,393</td>
<td>$283,621,000</td>
<td>-0.8</td>
</tr>
<tr>
<td>8</td>
<td>Monero</td>
<td>XMR</td>
<td>$4,892,466,049</td>
<td>$310.36</td>
<td>15,474,106</td>
<td>$251,619,000</td>
<td>-0.0</td>
</tr>
<tr>
<td>9</td>
<td>New</td>
<td>XEM</td>
<td>$4,730,579,999</td>
<td>$0.525620</td>
<td>8,389,999,999</td>
<td>$630,820,400</td>
<td>-0.9</td>
</tr>
<tr>
<td>10</td>
<td>Bitcoin Gold</td>
<td>BTG</td>
<td>$4,808,721,932</td>
<td>$275.00</td>
<td>16,704,509</td>
<td>$244,900,000</td>
<td>0.2</td>
</tr>
<tr>
<td>11</td>
<td>Cardano</td>
<td>ADA</td>
<td>$3,573,009,591</td>
<td>$0.137810</td>
<td>25,227,070,538</td>
<td>$67,520,000</td>
<td>0.0</td>
</tr>
<tr>
<td>12</td>
<td>EOS</td>
<td>EOS</td>
<td>$3,483,252,840</td>
<td>$6.49</td>
<td>548,798,500</td>
<td>$67,155,000</td>
<td>2.0</td>
</tr>
<tr>
<td>13</td>
<td>Neo</td>
<td>NEO</td>
<td>$2,967,016,000</td>
<td>$45.65</td>
<td>85,000,000</td>
<td>$300,436,000</td>
<td>1.3</td>
</tr>
<tr>
<td>14</td>
<td>Ethereum Classic</td>
<td>ETC</td>
<td>$2,865,101,245</td>
<td>$30.18</td>
<td>94,377,117</td>
<td>$714,568,000</td>
<td>0.1</td>
</tr>
<tr>
<td>15</td>
<td>Stellar</td>
<td>XLM</td>
<td>$2,888,984,604</td>
<td>$0.158627</td>
<td>17,851,942,304</td>
<td>$117,260,000</td>
<td>-1.7</td>
</tr>
<tr>
<td>16</td>
<td>BitConnect</td>
<td>BCC</td>
<td>$1,775,402,653</td>
<td>$371.46</td>
<td>4,782,225</td>
<td>$297,660,000</td>
<td>-0.2</td>
</tr>
<tr>
<td>17</td>
<td>Poppous</td>
<td>PPT</td>
<td>$1,527,262,283</td>
<td>$27.02</td>
<td>41,232,249</td>
<td>$3,967,490</td>
<td>-2.8</td>
</tr>
<tr>
<td>18</td>
<td>Waves</td>
<td>WAVES</td>
<td>$1,373,952,000</td>
<td>$13.74</td>
<td>100,000,000</td>
<td>$81,626,000</td>
<td>-2.1</td>
</tr>
<tr>
<td>19</td>
<td>Qubit</td>
<td>QTVN</td>
<td>$1,312,655,888</td>
<td>$17.81</td>
<td>73,696,326</td>
<td>$575,564,000</td>
<td>0.2</td>
</tr>
<tr>
<td>20</td>
<td>Zcash</td>
<td>ZEC</td>
<td>$1,140,811,222</td>
<td>$403.35</td>
<td>2,823,369</td>
<td>$257,857,000</td>
<td>1.5</td>
</tr>
<tr>
<td>21</td>
<td>OnixGO</td>
<td>OVG</td>
<td>$1,114,233,235</td>
<td>$10.92</td>
<td>122,424,552</td>
<td>$113,697,000</td>
<td>1.0</td>
</tr>
<tr>
<td>22</td>
<td>Lisk</td>
<td>LSK</td>
<td>$1,085,024,202</td>
<td>$9.45</td>
<td>115,902,440</td>
<td>$53,657,110</td>
<td>-1.0</td>
</tr>
<tr>
<td>23</td>
<td>TRON</td>
<td>TRX</td>
<td>$1,017,643,289</td>
<td>$0.015482</td>
<td>55,748,126,175</td>
<td>$147,933,000</td>
<td>9.6</td>
</tr>
<tr>
<td>24</td>
<td>Ardor</td>
<td>ARDR</td>
<td>$992,924,624</td>
<td>$0.993888</td>
<td>998,999,999</td>
<td>$23,441,100</td>
<td>0.1</td>
</tr>
<tr>
<td>25</td>
<td>Stratis</td>
<td>STRAT</td>
<td>$431,212,619</td>
<td>$0.84</td>
<td>98,659,200</td>
<td>$30,182,000</td>
<td>-0.2</td>
</tr>
<tr>
<td>26</td>
<td>Tether</td>
<td>USDT</td>
<td>$915,110,007</td>
<td>$1.03</td>
<td>898,017,349</td>
<td>$2,253,580,000</td>
<td>-1.3</td>
</tr>
</tbody>
</table>
BitCoin’s (original) goal

Pros/cons of cash

✓ Portable
✓ no need for trusted 3rd party
✓ anonymous
✓ cannot repudiate after payment
✗ Does not work online
✗ hard to monitor/tax
✗ need government to print them

Pros/cons of credit cards

✓ works online
✓ cannot repudiate
✗ requires trusted 3rd party
✗ tracks one’s purchases
✗ can prohibit some transactions
✗ easy to monitor/tax/control

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 \( K, K^{-1} \)
  - \( e \leftarrow \text{Encrypt(data, } K \text{ )}, \text{ data } \leftarrow \text{Decrypt(e, } K^{-1} \text{ )} \)
  - \( \{\text{data}\}_{K^{-1}} \leftarrow \text{Sign(data, } K^{-1} \text{ )}, \text{ verify}(\text{signature, } K) \)

- **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 only \( 2^{(-256)} \) likely to find \( x \) such that \( \text{hash(x)} = h \)
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: \(\{\text{hash}(T_1), B_{pub} \rightarrow C_{pub}\}_B\)
I’d like to buy a pizza

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

Your transaction is valid!
What’s hard technically?

✓ • Forgery
✓ • Theft
✗ • Double spending

Pizza please

{\bullet, A \rightarrow B}^A_{A^{-1}} \rightarrow \{\bullet, B \rightarrow C\}^B_{B^{-1}}

noddle please

{\bullet, A \rightarrow B}^A_{A^{-1}} \rightarrow \{\bullet, B \rightarrow D\}^B_{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
- Problem: how to ensure all peer keeps the same log?
  - Can we run Raft/MultiPaxos among all peers?
Why not use Paxos/Raft to maintain the global ledger?

• 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

• Membership churn
  – nodes join and leave constantly \(\rightarrow\) Paxos cannot reach agreement if >1/2 participants are down

• Vulnerable to Sybil attack
  – adversary enrolls many of his own nodes so he controls >1/2 of all nodes

• Once log diverged, no way to repair
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.:

  • $\text{hash(block, nonce)} = \text{?}$

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

• 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?
  – too much churn on what’s 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 \( n \)?
• For every 2016 blocks found, each peer sets the difficulty for the next (2016) blocks to be:
  - 2 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)
  - \((1\text{MB}/150\text{B})/600\text{sec} = 11\) transactions/sec
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 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

\{*, B \rightarrow C\}_{B^{-1}}

\{*, D \rightarrow E\}_{D^{-1}}

validate next block has no doublespenders, coins exist etc.
Shall I become a BitCoin miner now?

Intel core i7: 24MHashes/sec
top-of-theline GPU: 1GHashes/sec
ASIC: 1000 GHashes/sec
Can Bitcoin scale well?

• Size of ledger grows over time
  – currently at 140GB
• 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
• ✗ Transactions take a long time to confirm.
• ✗ With the soaring price, transaction fee is high ($20)
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