Lecture 6:

Community, politics, forks

HW 2: due Thursday

Proj 2: due Oct 19

churning BTC

Bitcoin → Now → other cryptocurrencies
3 layers of consensus

1) Consensus on state/ledger/blockchain
   - could be one-time consensus
   - in practice, want to make changes

2) Consensus on rules (genesis block)

3) Consensus on that coins have value
   (contrast with “Fiat” currencies vs. “Tinkerbell effect”)
BBFL

BDFL: "Benevolent Dictator for Life"

Problem: Satoshi gone since 2013
Changing the rules

- Easy to change (doesn't require consensus)
  - P2P network
  - L7 replace by fee
  - script whitelist
  - anti-DOS
Hard to change:
- transaction layer
- consensus layer

Hard fork
two sets of rules: \( A, B \)

\[ A/B \subseteq A/B \]
March 2013 fork

v 0.7 rejected blocks ≥ 500 KB
v 0.8 accepted blocks < 1 MB

传统 < 1 KB ... < 501 KB 0.8

传统 < 0.7
Soft fork

B recognizes all A blocks
A has > 50% power

Diagram:

```
A ← [A] ← X
↑
A ← [A] ← B ← B
```

```
Soft fork

- P2SH looks like OP_HASH160 <S> OP_TRUE
- Check lock time verify
- SEGWIT
Hard fork ideas

- Block size
- Fix MULTISIG bug
- Change block frequency
- GREP Crypto upgrades (Schnorr sigs / BLS sigs)
- Change the reward structure
- Charge # of BTC
- Consensus mechanism
- Skip 1.3+
- UTXO set commitment
Block size debate

1 MB → 1.7 KB/s → 3.7 tps

Paypal: 100 tps
VISA: >10k tps

- raise block size / increase block frequency
- increase costs of validation / storage
- increase centralization
Limited divisibility

$\approx 2^{25}$ BTC

$\approx 2^{27}$ satoshis / BTC

$2^{52}$ units of currency

$2^{33}$ humans

$500 \times$ units / human
Cross-chain replay prevention

\[ A \Rightarrow A', \quad A' \Rightarrow A, \quad A \Rightarrow A'' \]

Bitcoin Cash

Bitcoin (Classic)

What you need to replicate:

- Code (fork)
- Genesis block
- Miners
- Users / consumers (new features, new story)
# Cryptocurrency Market Capitalizations

<table>
<thead>
<tr>
<th>#</th>
<th>Name</th>
<th>Market Cap</th>
<th>Price</th>
<th>Circulating Supply</th>
<th>Volume (24h)</th>
<th>% Change (24h)</th>
<th>Price Graph (7d)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Bitcoin</td>
<td>$88,578,175,026</td>
<td>$5329.81</td>
<td>16,619,387 BTC</td>
<td>$2,566,940,000</td>
<td>10.02%</td>
<td><img src="https://example.com" alt="Graph" /></td>
</tr>
<tr>
<td>2</td>
<td>Ethereum</td>
<td>$29,105,198,326</td>
<td>$306.13</td>
<td>95,074,947 ETH</td>
<td>$486,137,000</td>
<td>1.05%</td>
<td><img src="https://example.com" alt="Graph" /></td>
</tr>
<tr>
<td>3</td>
<td>Ripple</td>
<td>$9,825,397,512</td>
<td>$0.25451</td>
<td>38,600,451,446 XRP</td>
<td>$227,384,000</td>
<td>-3.23%</td>
<td><img src="https://example.com" alt="Graph" /></td>
</tr>
<tr>
<td>4</td>
<td>Bitcoin Cash</td>
<td>$5,194,370,256</td>
<td>$311.31</td>
<td>16,685,363 BCH</td>
<td>$245,503,000</td>
<td>-0.79%</td>
<td><img src="https://example.com" alt="Graph" /></td>
</tr>
<tr>
<td>5</td>
<td>Litecoin</td>
<td>$3,048,902,840</td>
<td>$57.16</td>
<td>53,343,157 LTC</td>
<td>$270,749,000</td>
<td>12.25%</td>
<td><img src="https://example.com" alt="Graph" /></td>
</tr>
<tr>
<td>6</td>
<td>Dash</td>
<td>$2,231,625,962</td>
<td>$292.97</td>
<td>7,617,355 DASH</td>
<td>$40,718,100</td>
<td>-2.33%</td>
<td><img src="https://example.com" alt="Graph" /></td>
</tr>
<tr>
<td>7</td>
<td>NEM</td>
<td>$1,864,863,000</td>
<td>$0.207207</td>
<td>8,999,999,999 XEM</td>
<td>$4,360,710</td>
<td>-3.90%</td>
<td><img src="https://example.com" alt="Graph" /></td>
</tr>
<tr>
<td>8</td>
<td>NEO</td>
<td>$1,416,780,000</td>
<td>$28.34</td>
<td>50,000,000 NEO</td>
<td>$53,375,600</td>
<td>-5.25%</td>
<td><img src="https://example.com" alt="Graph" /></td>
</tr>
</tbody>
</table>
Initial allocation

- Just start mining
- "Pre-mine" $\rightarrow$ investors
- Fork
- Proof-of-burn $\rightarrow$ one-way peg
- Two-way peg (requires changing Bitcoin) $\rightarrow$ H("Joe.com" | $KA$)
Atomic cross-chain exchange

Alice has 1 BTC
Bob has 2 DGC

...can do this atomically without TTP
Minining for Altcoins

1) just start mining using SHA-256²
   Risk: infeasible (e.g. CoiledCoin)

2) use a new mining puzzle
   e.g. Litecoin uses scrypt
3) Overlay currency (e.g. MasterCoin) write tx to Bitcoin using OR RETURN need to verify all tx (no SPV)

4) Merge mining
Merge mining

BTC

KM

Altcoin

KM