What is Bitcoin?
The Bank of Bitcoin
The Bank of Bitcoin

<table>
<thead>
<tr>
<th>User</th>
<th>Balance</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>2</td>
</tr>
<tr>
<td>B</td>
<td>5</td>
</tr>
<tr>
<td>C</td>
<td>8</td>
</tr>
</tbody>
</table>
The Bank of Bitcoin

<table>
<thead>
<tr>
<th>User</th>
<th>Balance</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>2</td>
</tr>
<tr>
<td>B</td>
<td>5</td>
</tr>
<tr>
<td>C</td>
<td>8</td>
</tr>
</tbody>
</table>
The Bank of Bitcoin

TX
B → A

<table>
<thead>
<tr>
<th>User</th>
<th>Balance</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>2 4</td>
</tr>
<tr>
<td>B</td>
<td>5 3</td>
</tr>
<tr>
<td>C</td>
<td>8</td>
</tr>
</tbody>
</table>
Distributing the Bank
Distributing the Bank
Distributing the Bank
Distributing the Bank
Resolving Conflicts
How to Choose a Leader?
The Blockchain

Time

Diagram showing a blockchain with nodes connected in a chain over time.
The Blockchain
The Blockchain
Downsides

- Slow confirmation
- Requires multiple confirmations
- Large blocks
- No snapshots
- Application specific blockchain
 Downsides

- Slow confirmation
- Requires multiple confirmations
- Large blocks
- No snapshots
- Application specific blockchain

Bitcoin
From Bitcoin to Traditional Systems
How to assign identities?
PeerCensus

Blockchain

Chain Agreement

Application
PeerCensus
PeerCensus

Blockchain → Chain Agreement

Block → Commit

Chain Agreement → Application
PeerCensus

Blockchain

Chain Agreement

Application

Block
Commit
Join
Leave
PeerCensus

Blockchain

Chain Agreement

Membership

Applications

Join

Leave

Block

Commit
Advantages

- Fast confirmations
- Atomic commits
- Small, Application agnostic blockchain
- Snapshots to bootstrap new nodes
Conclusions

- Stronger consistency guarantees for Bitcoin
- Realtime confirmation
- Reusable subsystem
Thank you, questions?