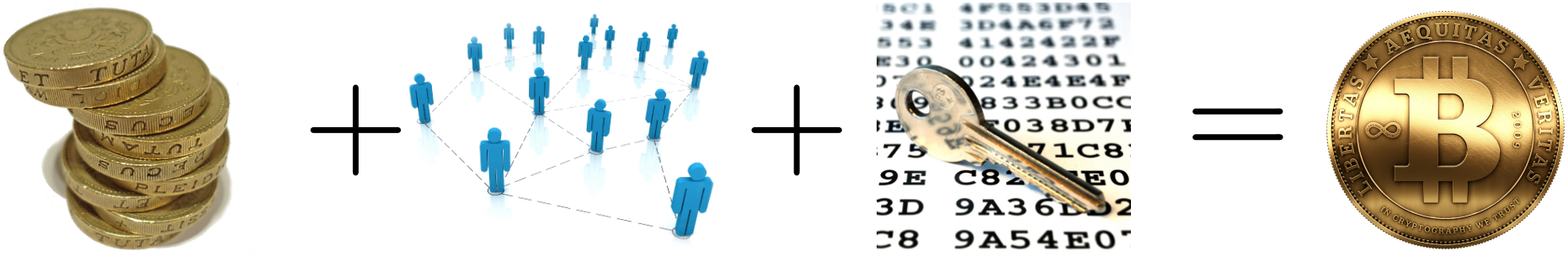
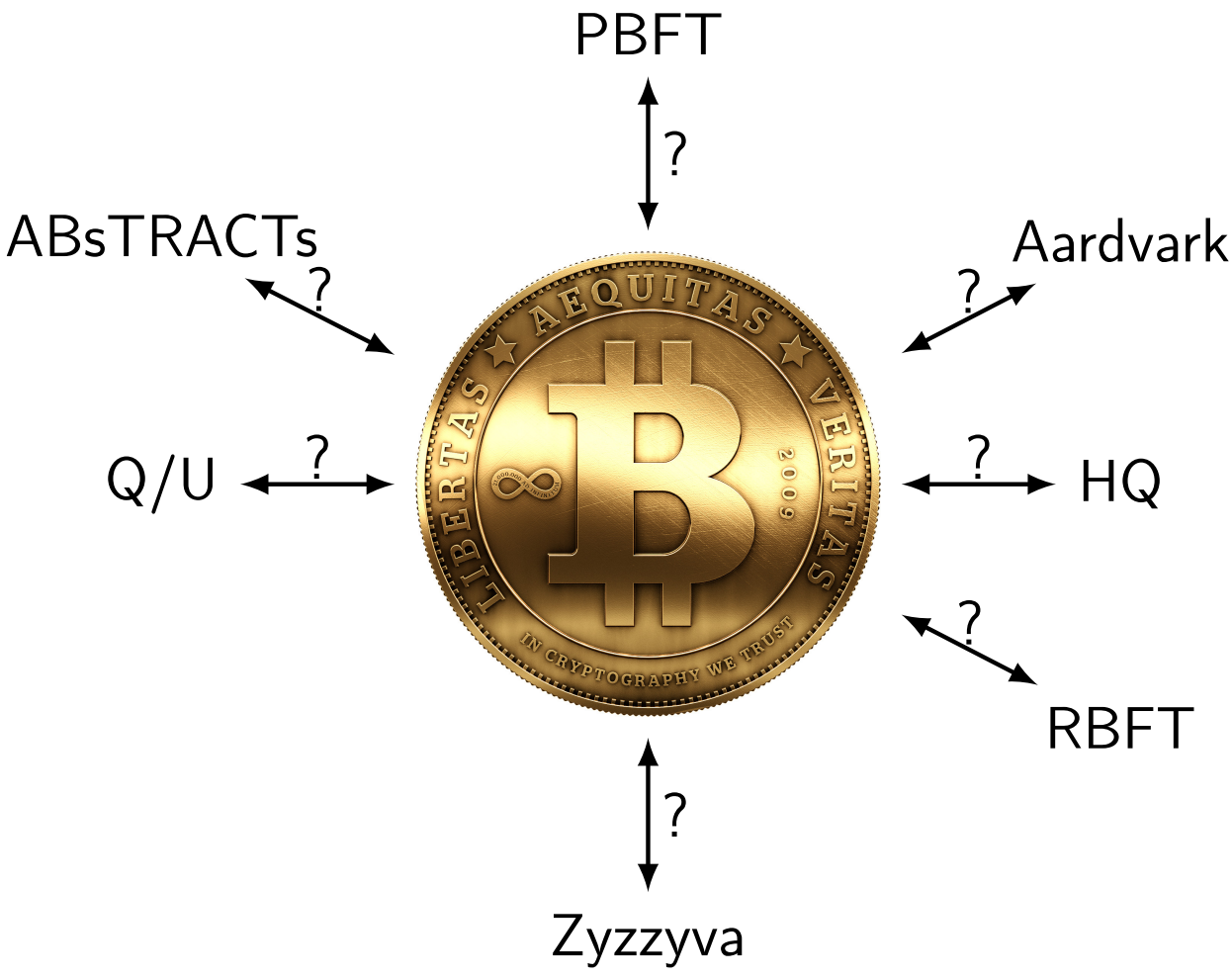
Bitcoin Meets Strong Consistency

Christian Decker
Jochen Seidel
Roger Wattenhofer

ETH Zurich – Distributed Computing Group – www.disco.ethz.ch

What is Bitcoin?



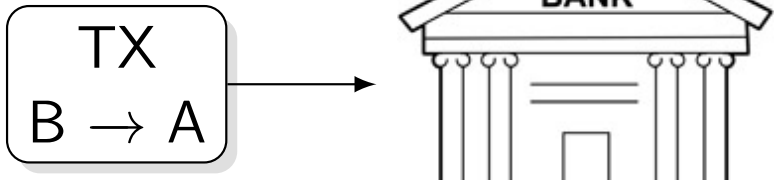

PBFT
?
ABsTRACTs
?
Aardvark
?
Q/U
?
?
HQ
?
RBFT
?
Zyzzyva
LIBERTAS
AEQUITAS
VERITAS
2009
IN CRYPTOGRAPHY WE TRUST

The Bank of Bitcoin

The Bank of Bitcoin

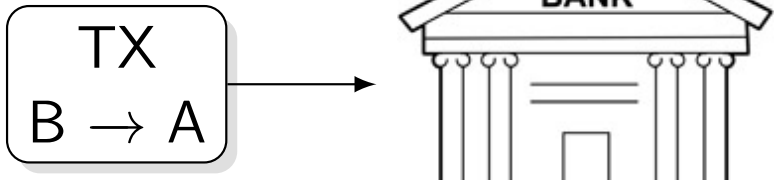
User	Balance
A	2
B	5
C	8

The Bank of Bitcoin



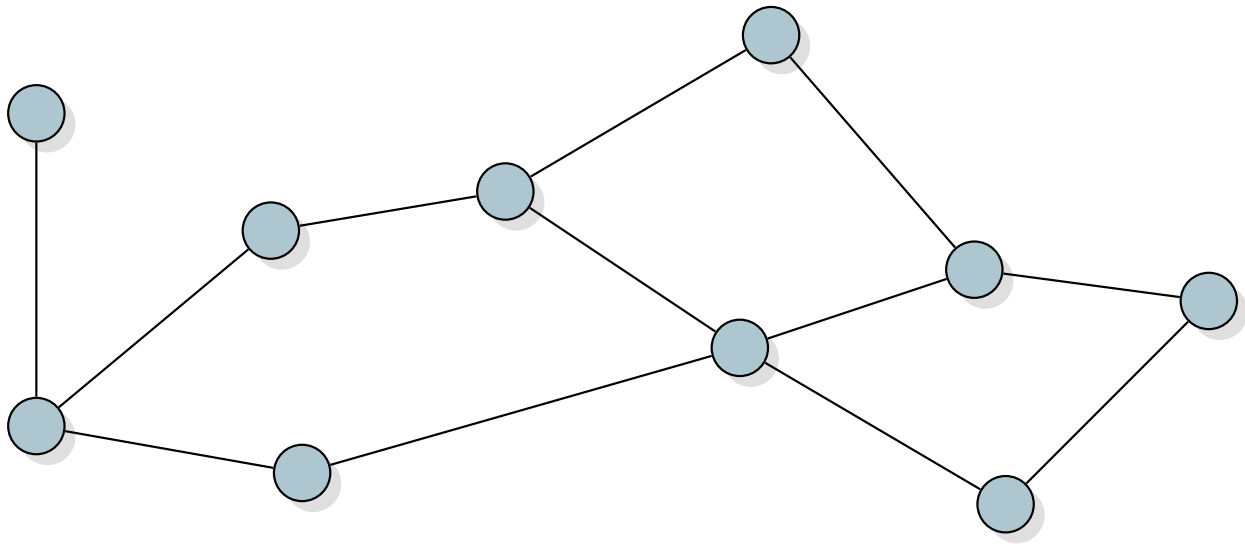
User	Balance
A	2
B	5
C	8

The Bank of Bitcoin

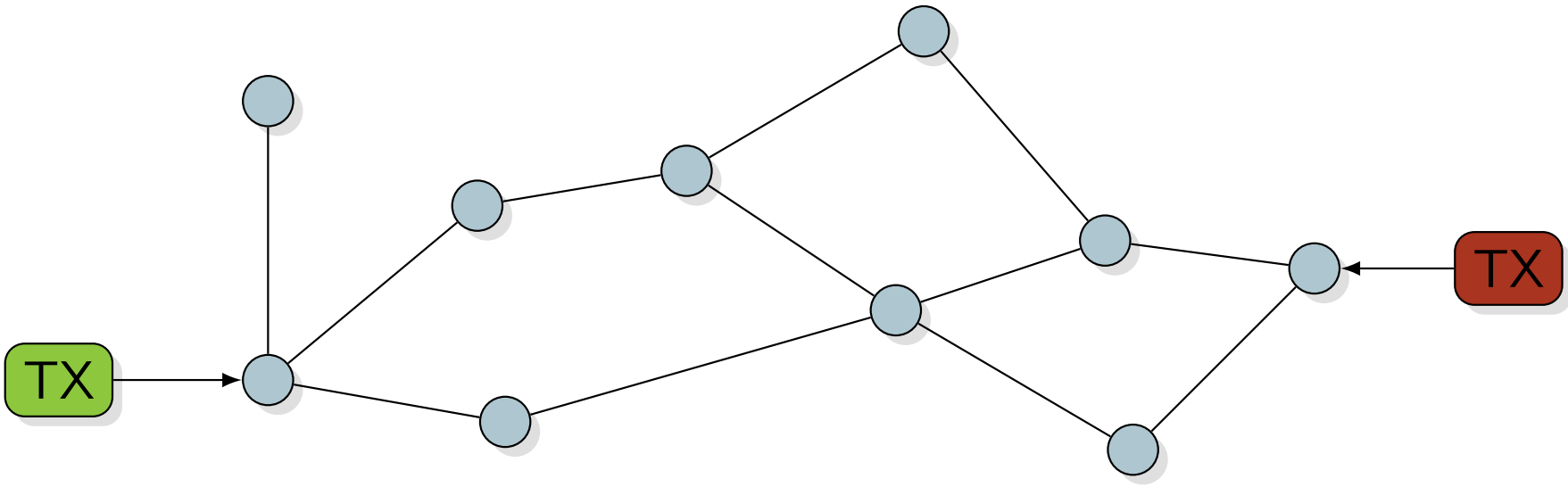


User	Balance
A	~~2~~ 4
B	~~5~~ 3
C	8

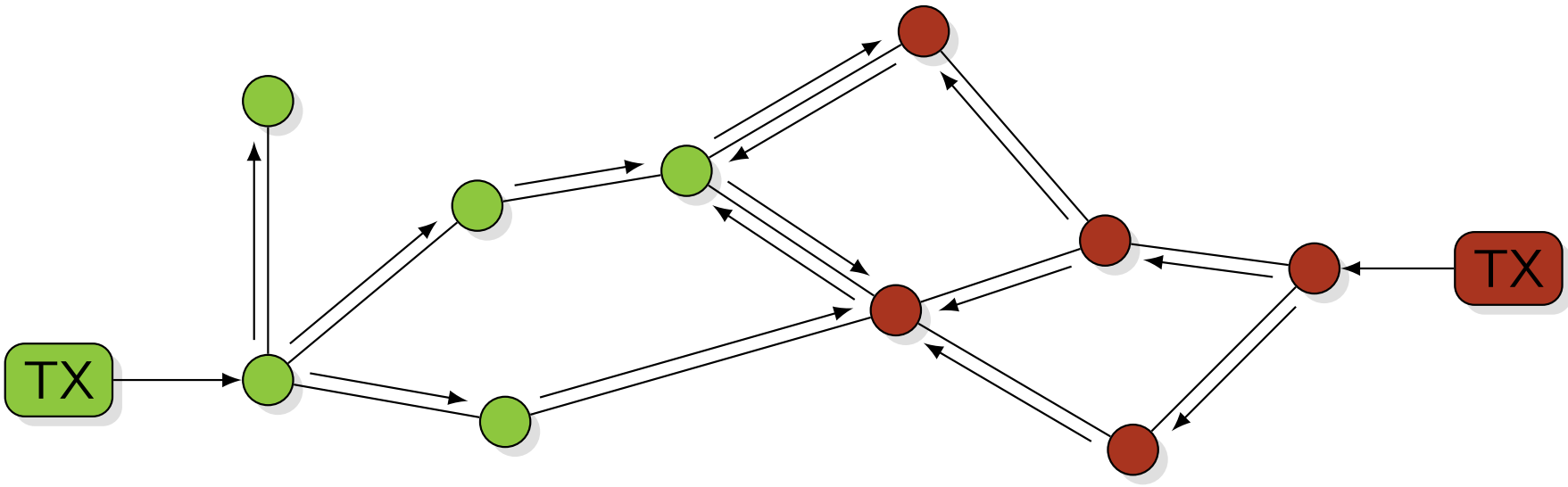
Distributing the Bank



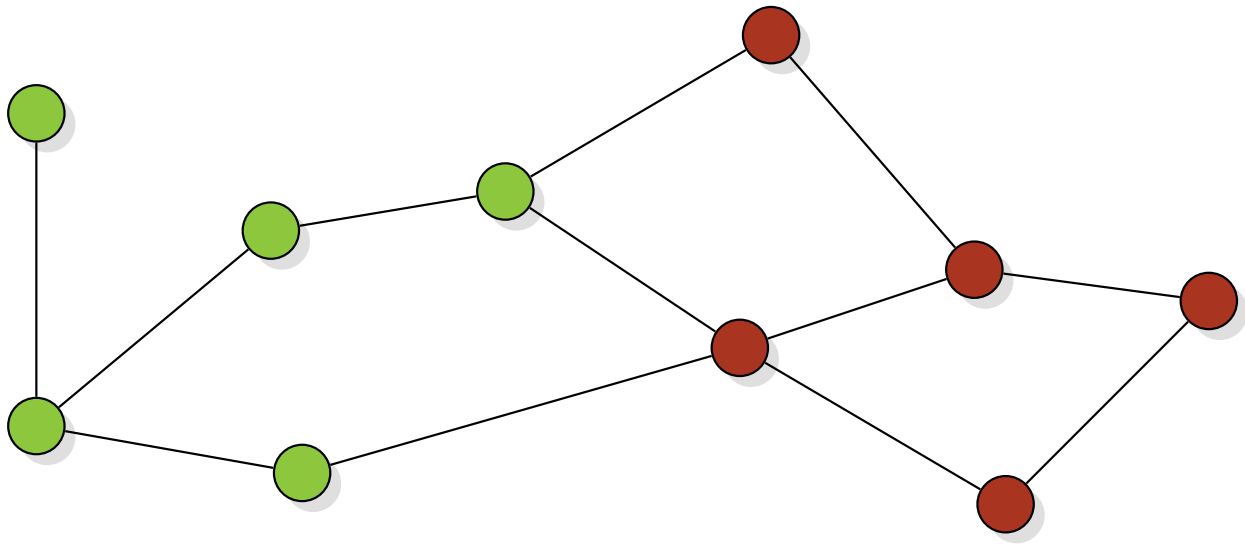
Distributing the Bank



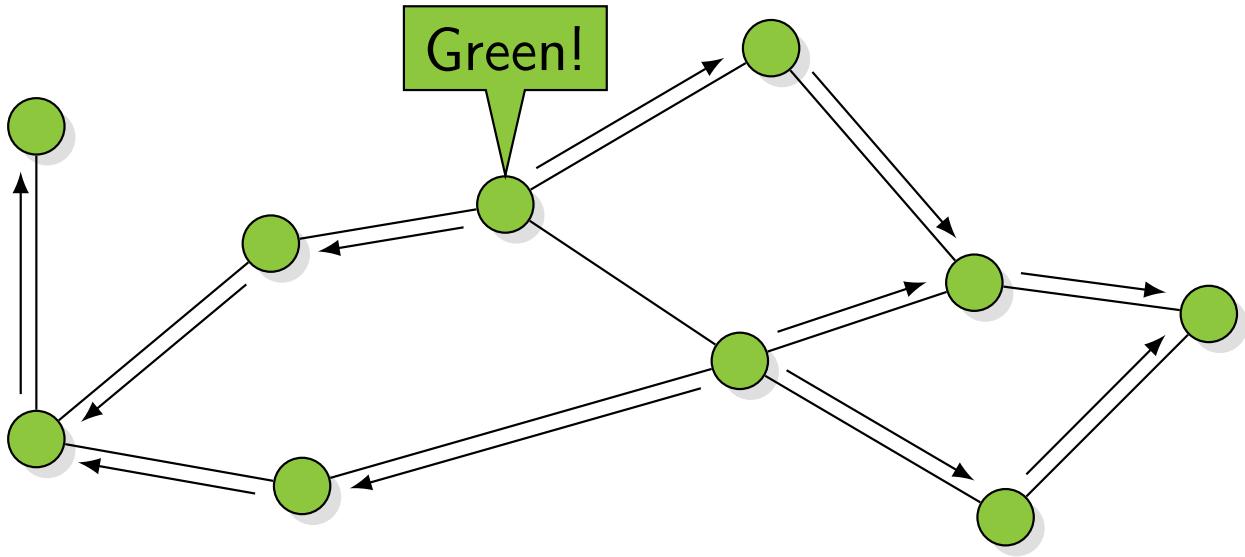
Distributing the Bank



Distributing the Bank

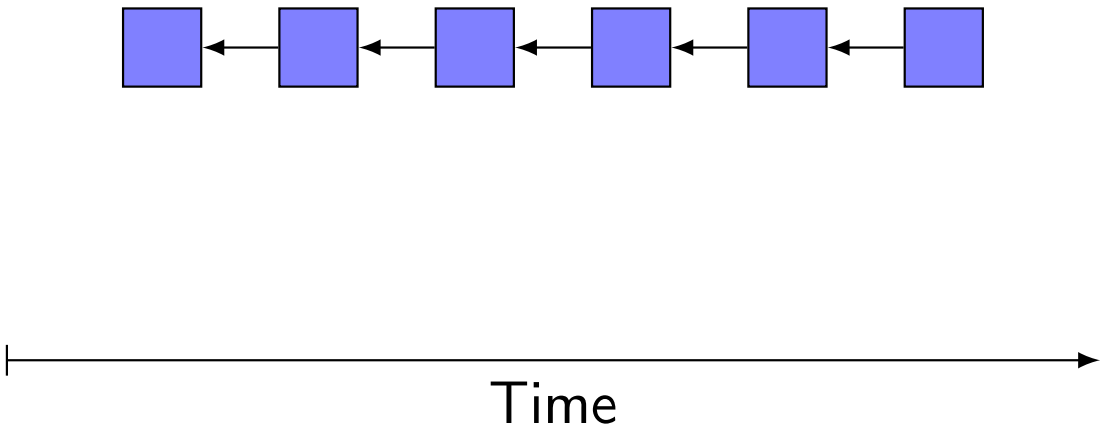


Resolving Conflicts

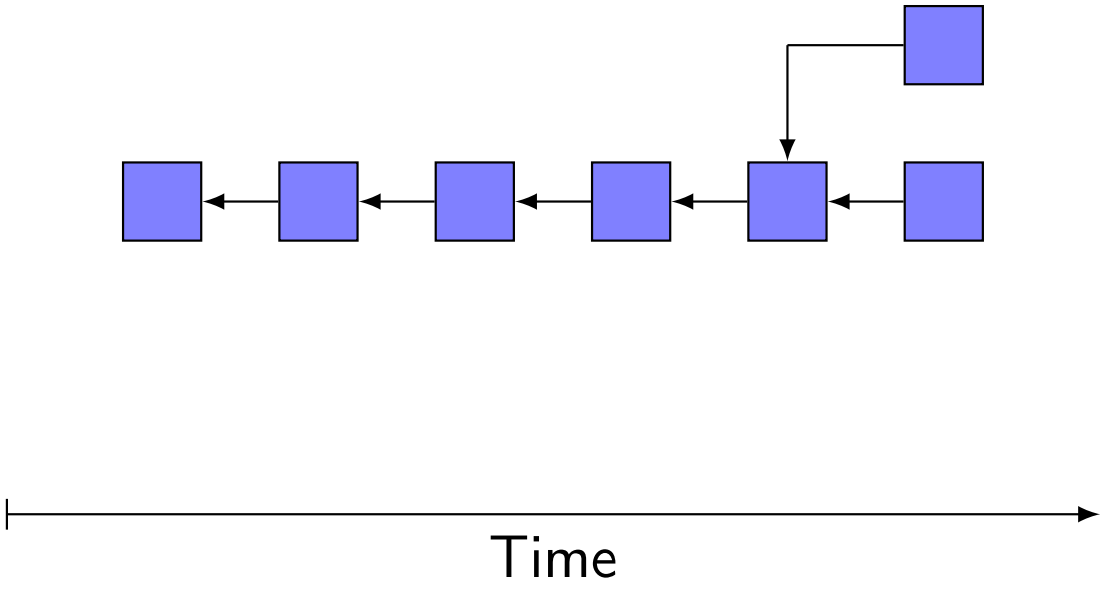


How to Choose a Leader?

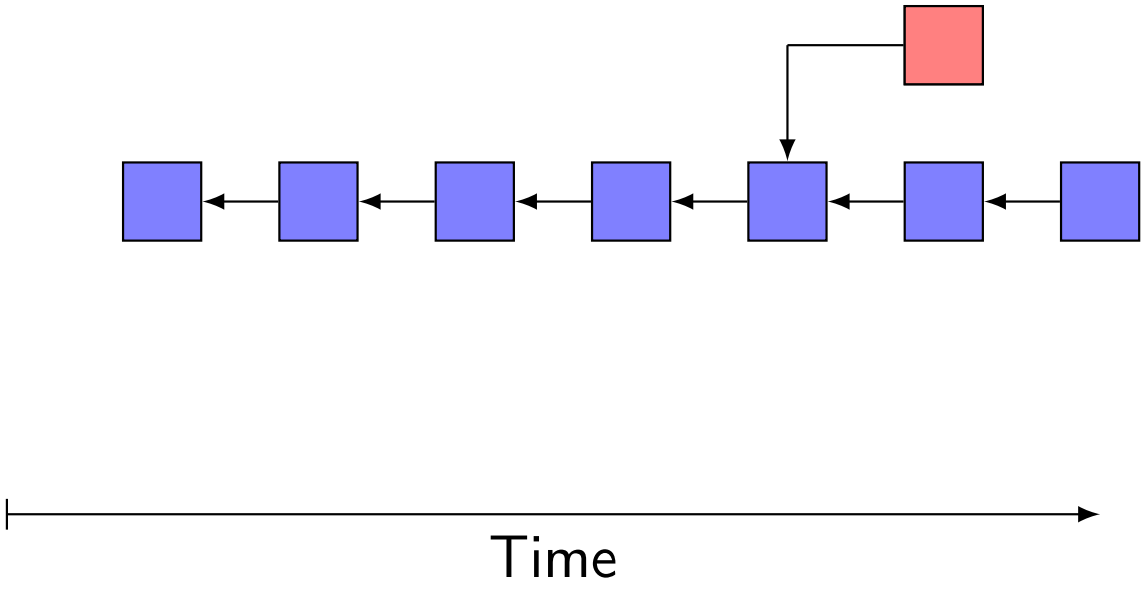
The Blockchain



The Blockchain

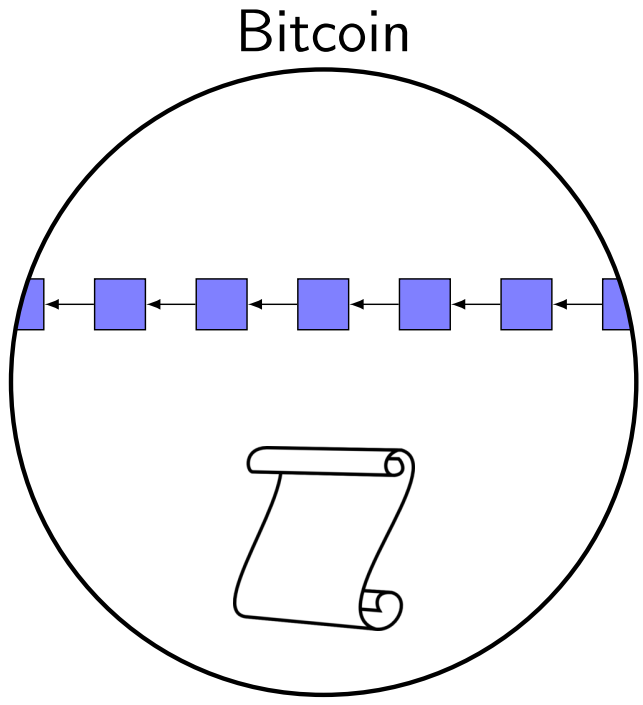


The Blockchain



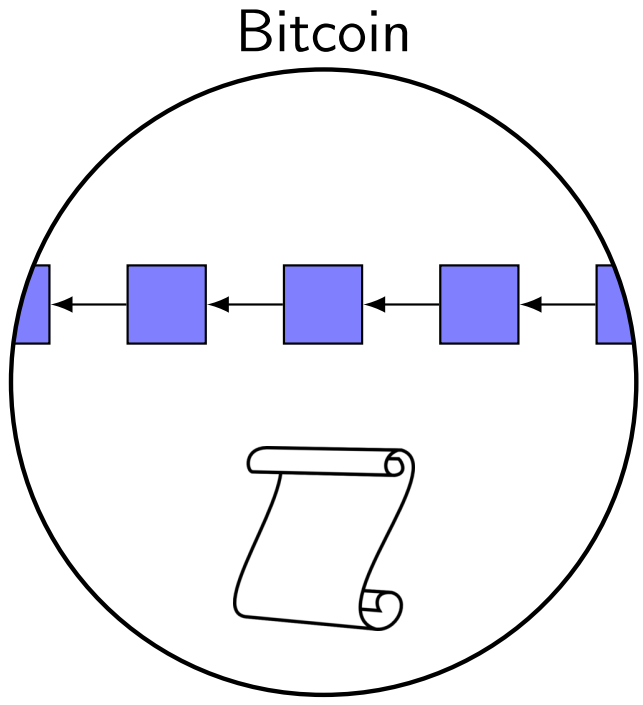
Downsides

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

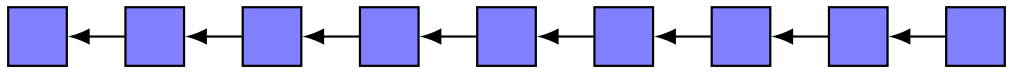


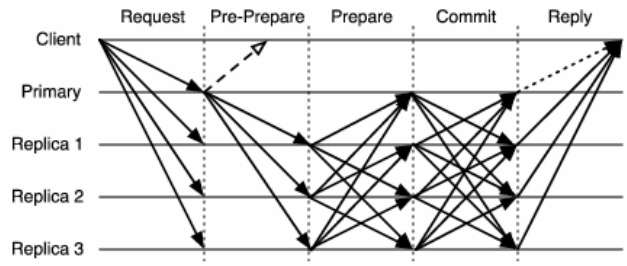
Downsides

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

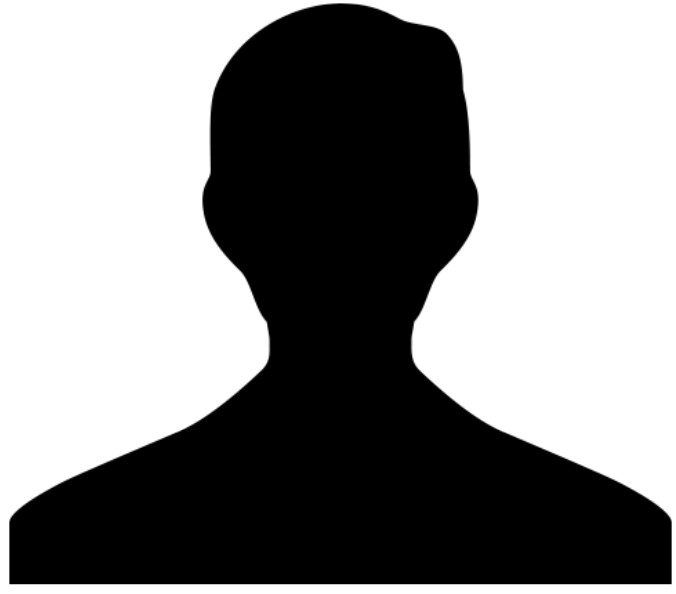


From Bitcoin to Traditional Systems





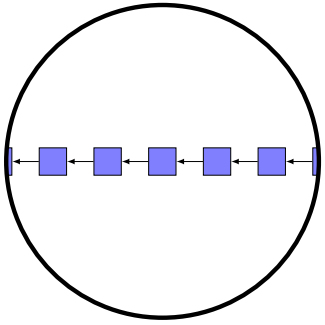
? ? ?



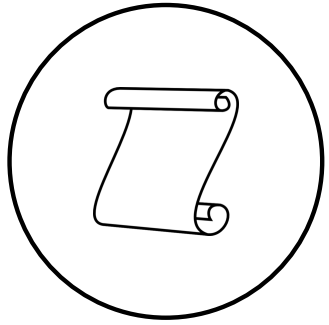
How to assign identities?

PeerCensus

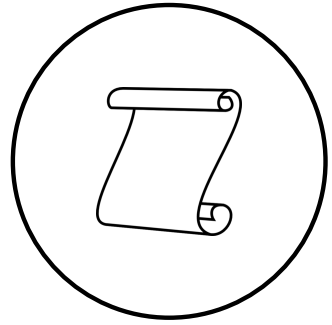
Blockchain



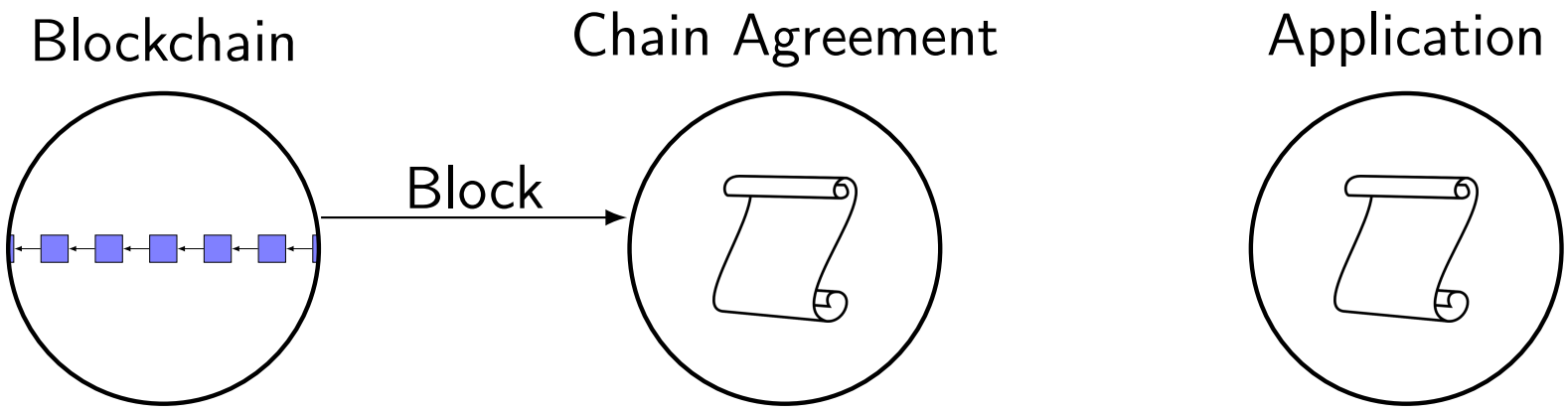
Chain Agreement



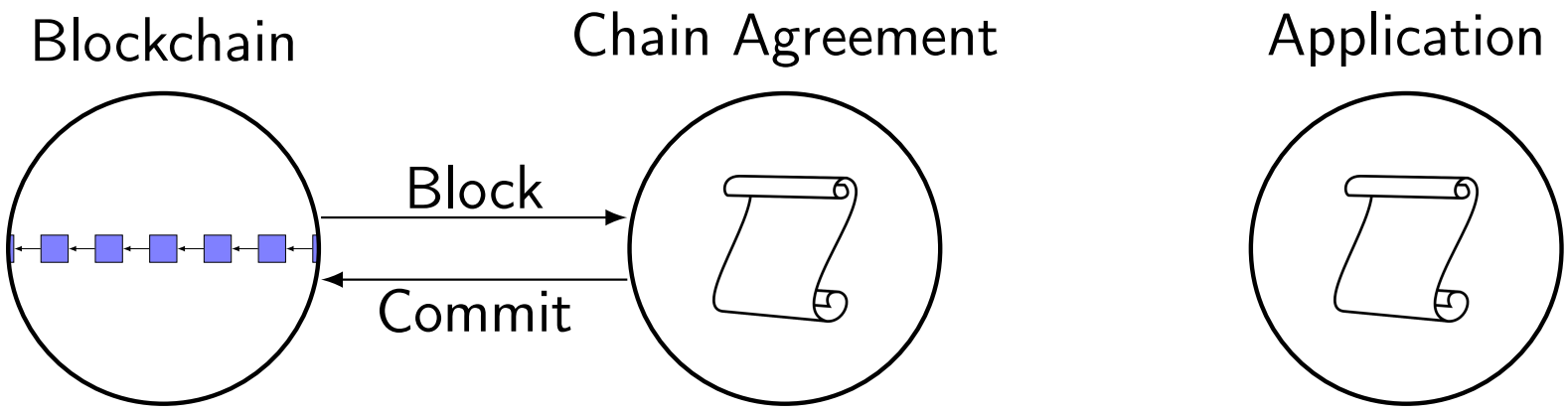
Application



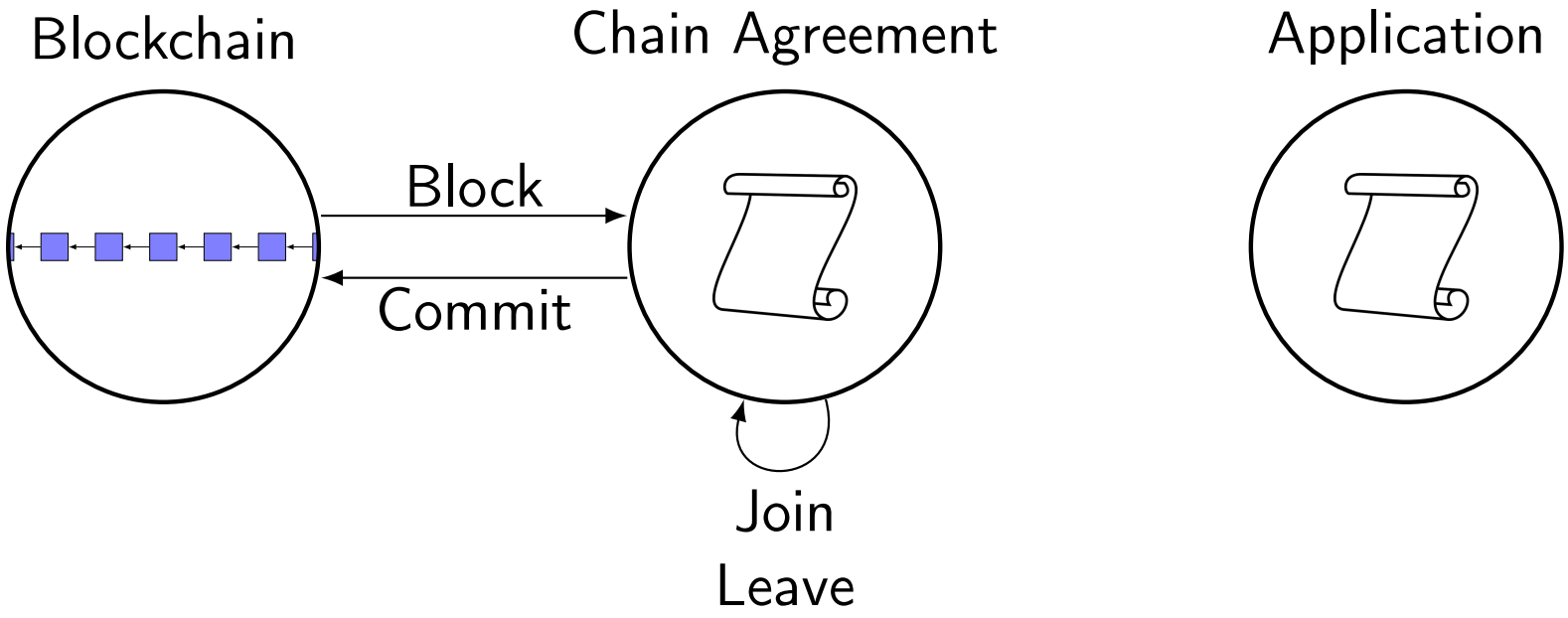
PeerCensus



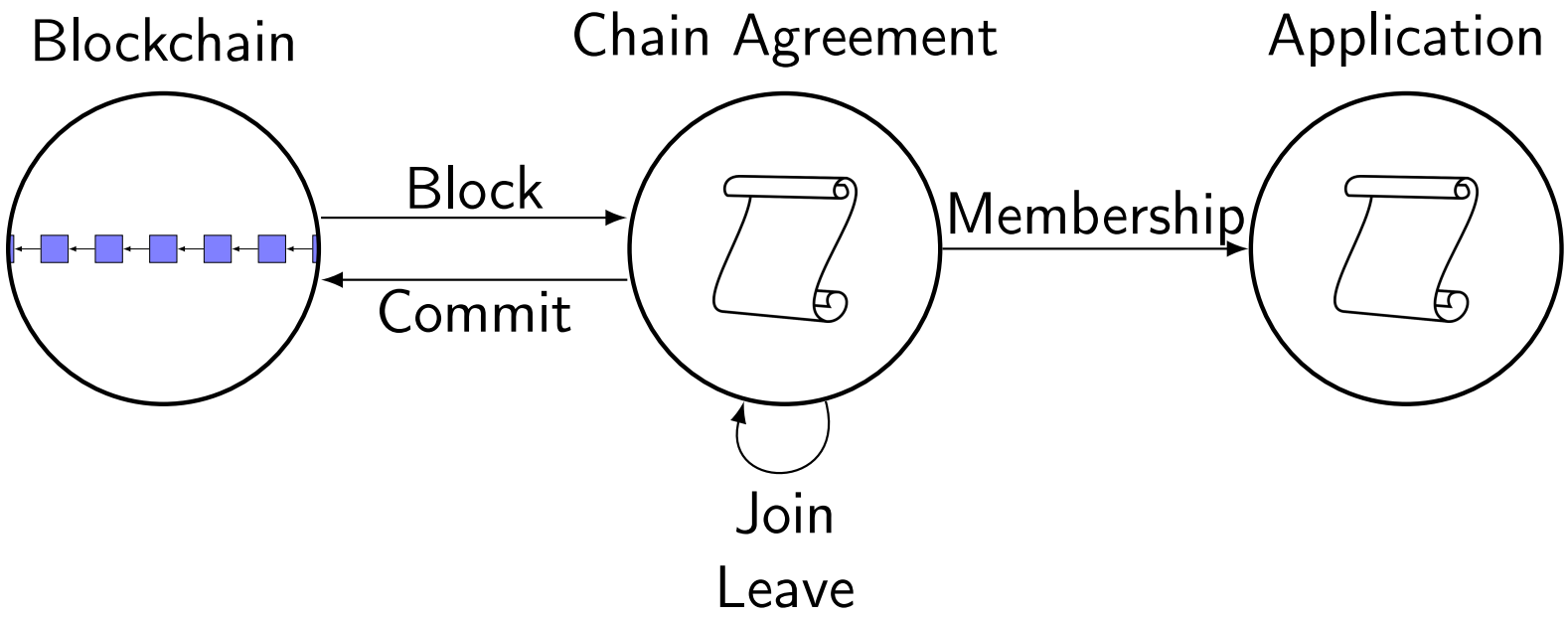
PeerCensus



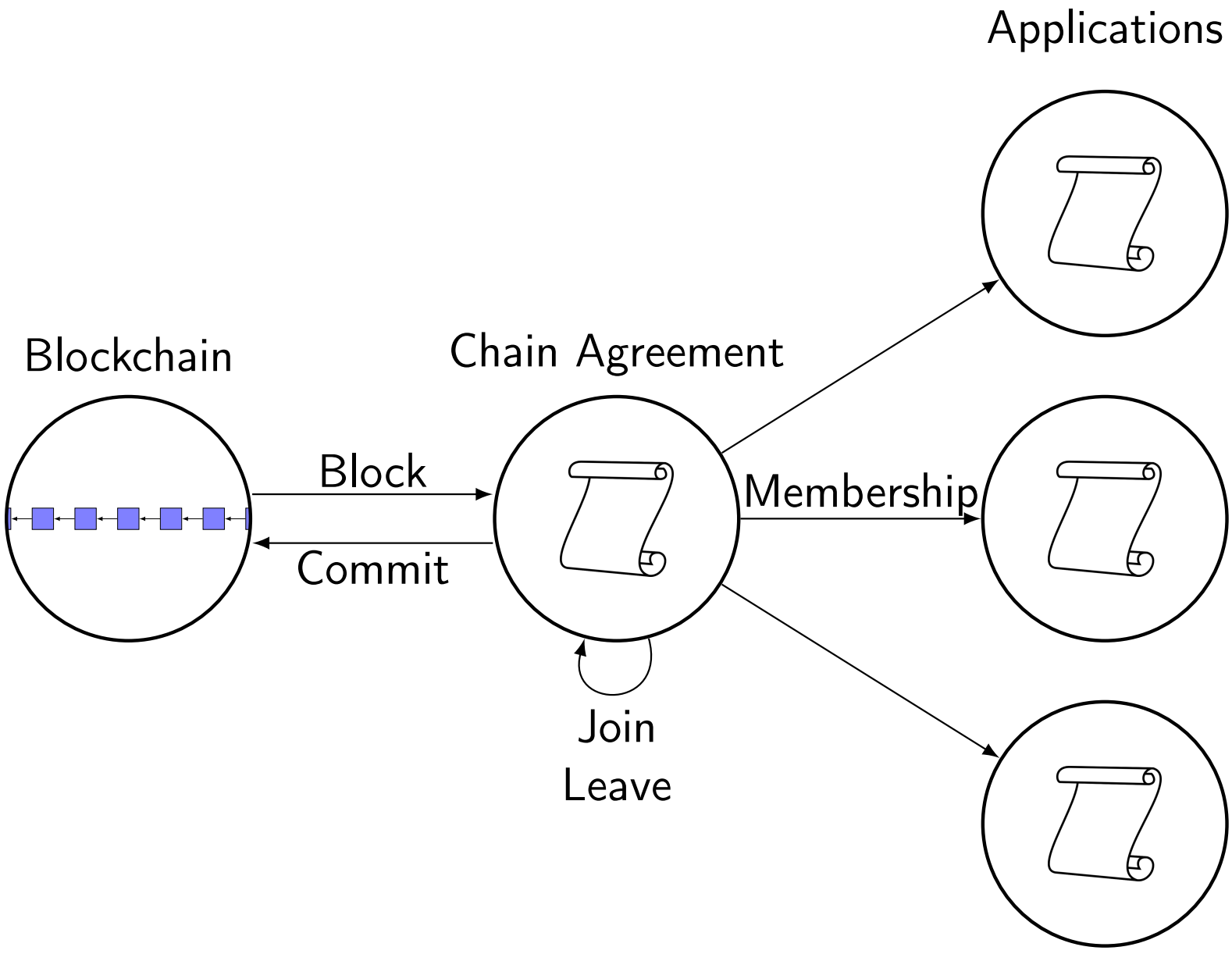
PeerCensus


Blockchain
Chain Agreement
Application
Block
Commit
Join
Leave

PeerCensus


Blockchain
Chain Agreement
Application
Block
Commit
Membership
Join
Leave

PeerCensus


Applications
Blockchain
Chain Agreement
Block
Commit
Membership
Join
Leave

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?