A Simple “Blockchain”
A Simple Blockchain for Simple Applications
“The problem of course is the payee can't verify that one of the owners did not double-spend the coin.”

“We need a system for participants to agree on a single history of the order in which [transactions] were received.”
no double-spending
\( \neq \)
single order
\( = \)
consensus
Double-Spending
Blockchains Solve Double-Spending Problem
What About Network Outages?
Without Consensus

ABC: Asynchronous Blockchain without Consensus

Jakub Silvinski and Roger Wattenhofer

ETH Zurich

{jslivinski, wattenhofer}@ethz.ch
Permissioned Blockchain

Needed: 4 out of 5 signatures
Permissioned Blockchain
Permissioned Blockchain
Usual Safety Condition

Less than 1/3 Malicious
Additional Condition

Single Owner Accounts*

*organized multi-owners, not fancy open-access smart contracts
Point To All Transactions!

No Main Chain, No Total Order
Sharded Signing

X \rightarrow L \rightarrow Z
A \rightarrow V \rightarrow C

sign please

sign please
Sharded Signing

X → L

L → Z

A → V

V → C

sign please

A-F

G-K

L-P

Q-U

V-Z
Also Permissionless?

(Without Proof-of-Work)
Permissionless / Open
Multiple Participants?

- **No**: No Blockchain (use database)

  Participants Known?

  - **No**: Permissionless Blockchain
  - **Yes**: Permissioned Blockchain

    Participants Known?
    - **No**: Permissionless Blockchain
    - **Yes**: Permissioned Blockchain
1. Transferrable Signing Keys

![Diagram showing the transferrable signing keys: B→D+E, D→F, E→J.](image)
1. Transferrable Signing Keys

2. Key Delegation (Pooling)
Thank You!

Questions & Comments?

Roger Wattenhofer, ETH Zurich, www.disco.ethz.ch
Ene, mene, eins, zwei, drei, Bitcoins bringe mir herbei. Hash Hash.