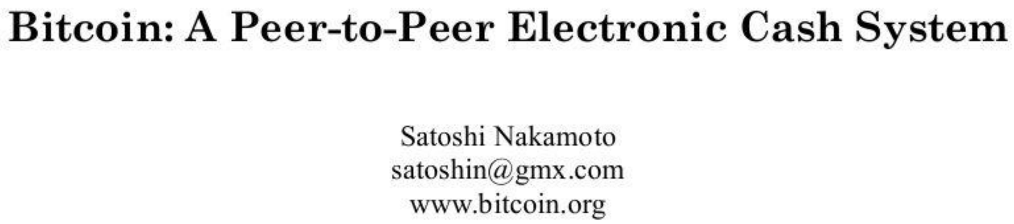
A Simple “Blockchain”

Roger Wattenhofer

A Simple Blockchain for Simple Applications



Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

“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

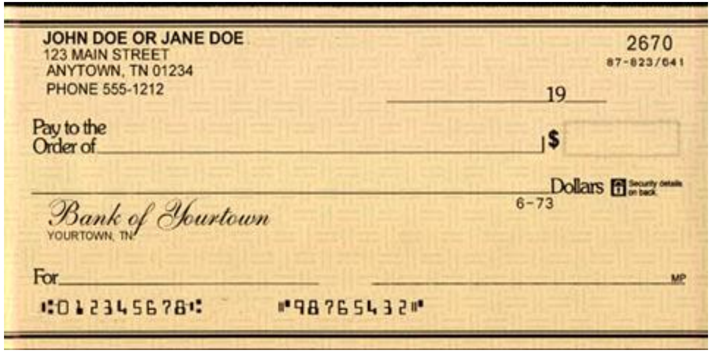
≠

single order

=

consensus

Double-Spending



JOHN DOE OR JANE DOE
123 MAIN STREET
ANYTOWN, TN 01234
PHONE 555-1212

2670
87-823/641

19

Pay to the Order of $

Dollars Security details on back.

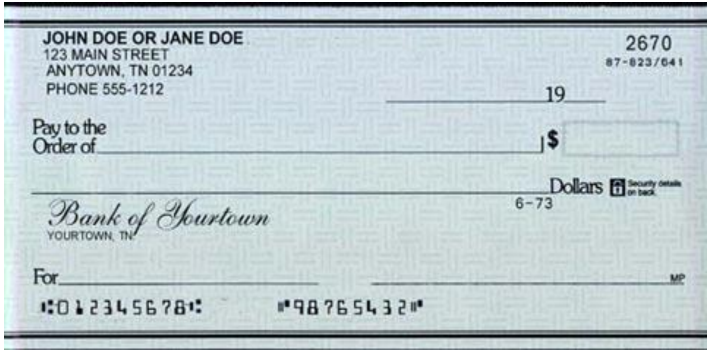
6-73

Bank of Yourtown
YOURTOWN, TN

For

MP

⑆012345678⑆ ⑈98765432⑈



JOHN DOE OR JANE DOE
123 MAIN STREET
ANYTOWN, TN 01234
PHONE 555-1212

2670
87-823/641

19

Pay to the Order of $

Dollars Security details on back.

6-73

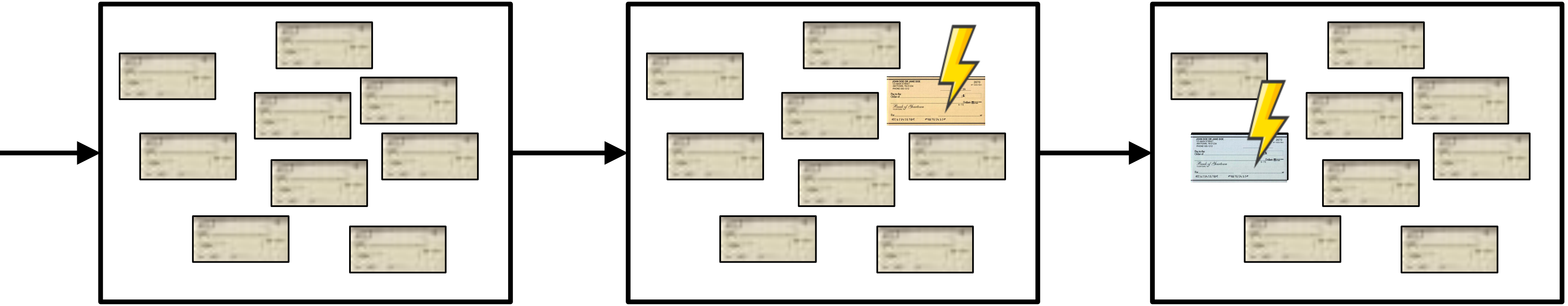
Bank of Yourtown
YOURTOWN, TN

For

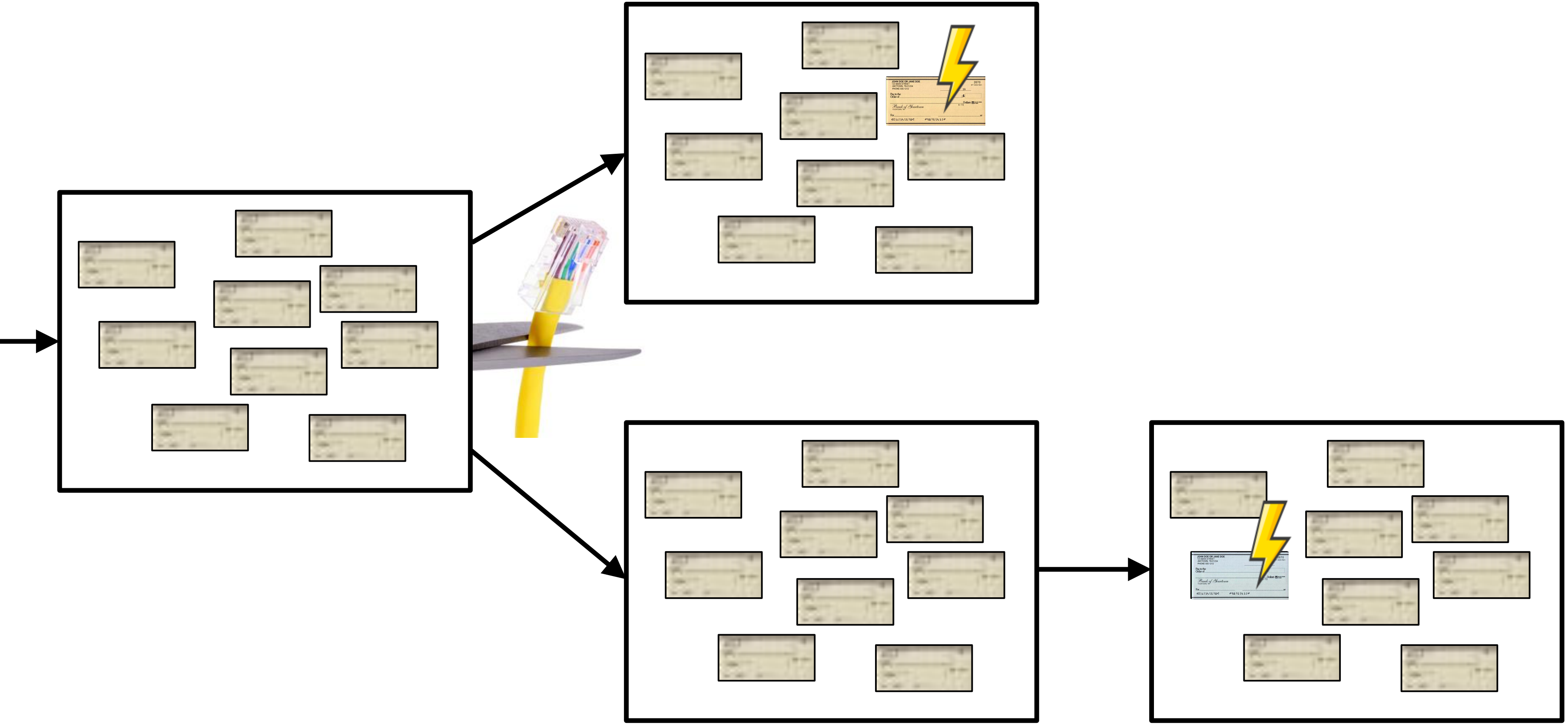
MP

⑆012345678⑆ ⑈98765432⑈

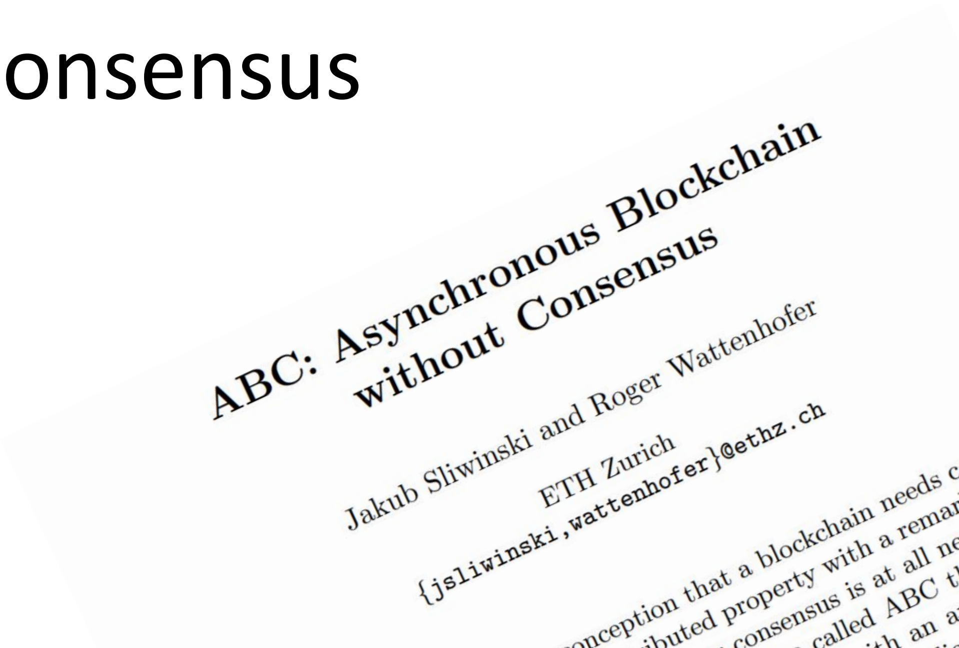
Blockchains Solve Double-Spending Problem



What About Network Outages?



Without Consensus



ABC: Asynchronous Blockchain without Consensus

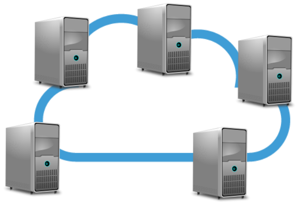
Jakub Sliwinski and Roger Wattenhofer

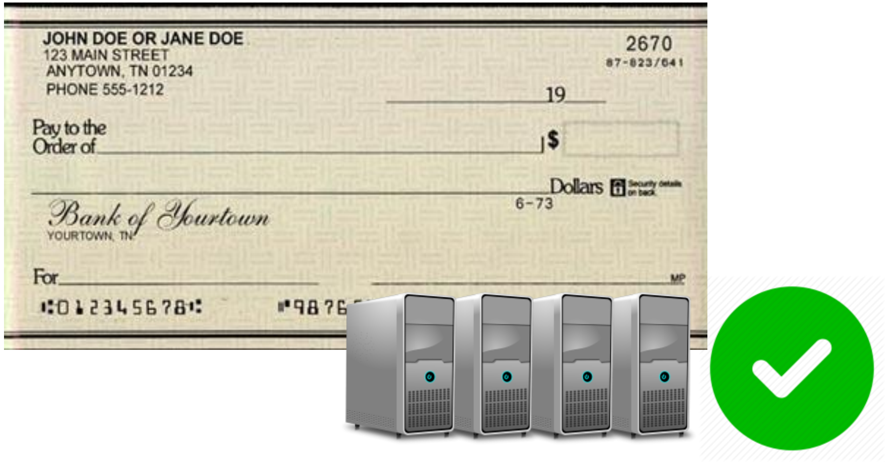
ETH Zurich

{jsliwinski,wattenhofer}@ethz.ch

conception that a blockchain needs c
ibuted property with a remar
consensus is at all ne
called ABC t
ith an a

Permissioned Blockchain





JOHN DOE OR JANE DOE
123 MAIN STREET
ANYTOWN, TN 01234
PHONE 555-1212

2670
87-823/641

19

Pay to the Order of $

Dollars Security details on back.

6-73

Bank of Yourtown
YOURTOWN, TN

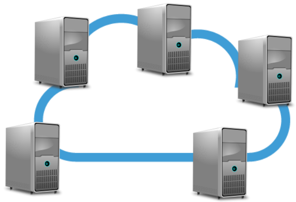
For

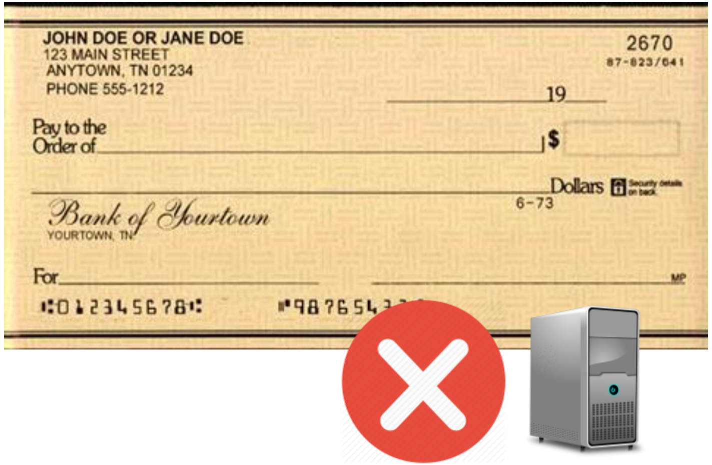
MP

⑆012345678⑆ ⑈9876

Needed: 4 out of 5 signatures

Permissioned Blockchain





JOHN DOE OR JANE DOE
123 MAIN STREET
ANYTOWN, TN 01234
PHONE 555-1212

2670
87-823/641

19

Pay to the Order of $

Dollars

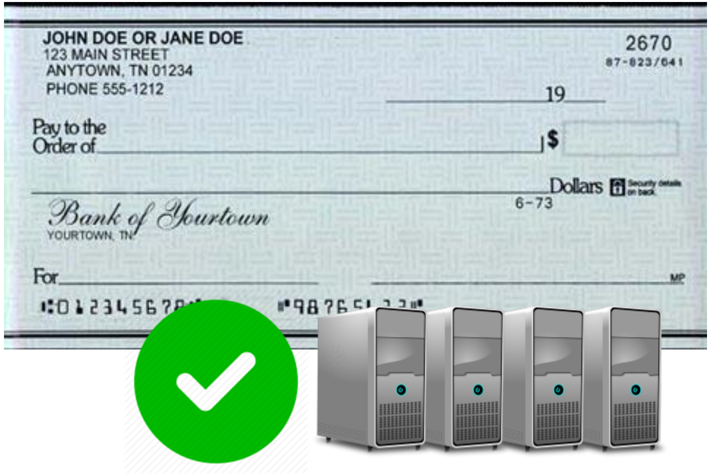
Bank of Yourtown
YOURTOWN, TN

6-73

For

MP

⑆012345678⑆ ⑈987654



JOHN DOE OR JANE DOE
123 MAIN STREET
ANYTOWN, TN 01234
PHONE 555-1212

2670
87-823/641

19

Pay to the Order of $

Dollars

Bank of Yourtown
YOURTOWN, TN

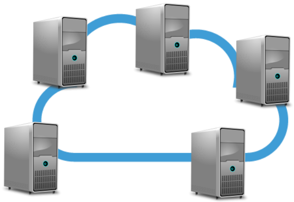
6-73

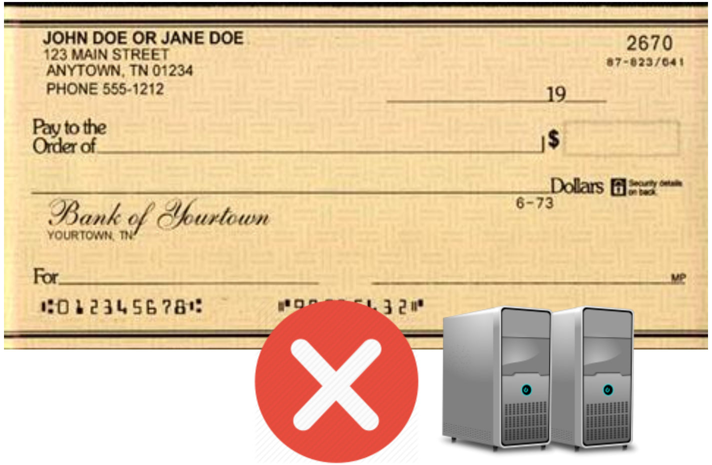
For

MP

⑆0123456 ⑈98765

Permissioned Blockchain





JOHN DOE OR JANE DOE
123 MAIN STREET
ANYTOWN, TN 01234
PHONE 555-1212

2670
87-823/641

19

Pay to the Order of $

Dollars Security details on back.

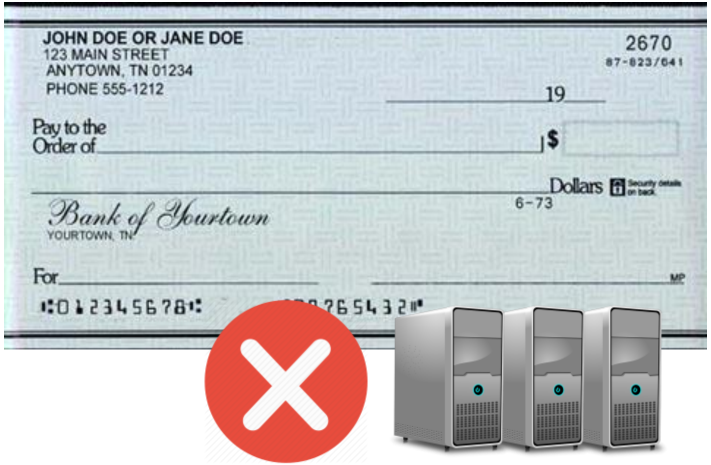
Bank of Yourtown
YOURTOWN, TN

6-73

For

MP

⑆0123456781⑆ ⑈98...5432⑈



JOHN DOE OR JANE DOE
123 MAIN STREET
ANYTOWN, TN 01234
PHONE 555-1212

2670
87-823/641

19

Pay to the Order of $

Dollars Security details on back.

Bank of Yourtown
YOURTOWN, TN

6-73

For

MP

⑆0123456781⑆ ...7654321⑈

Usual Safety Condition

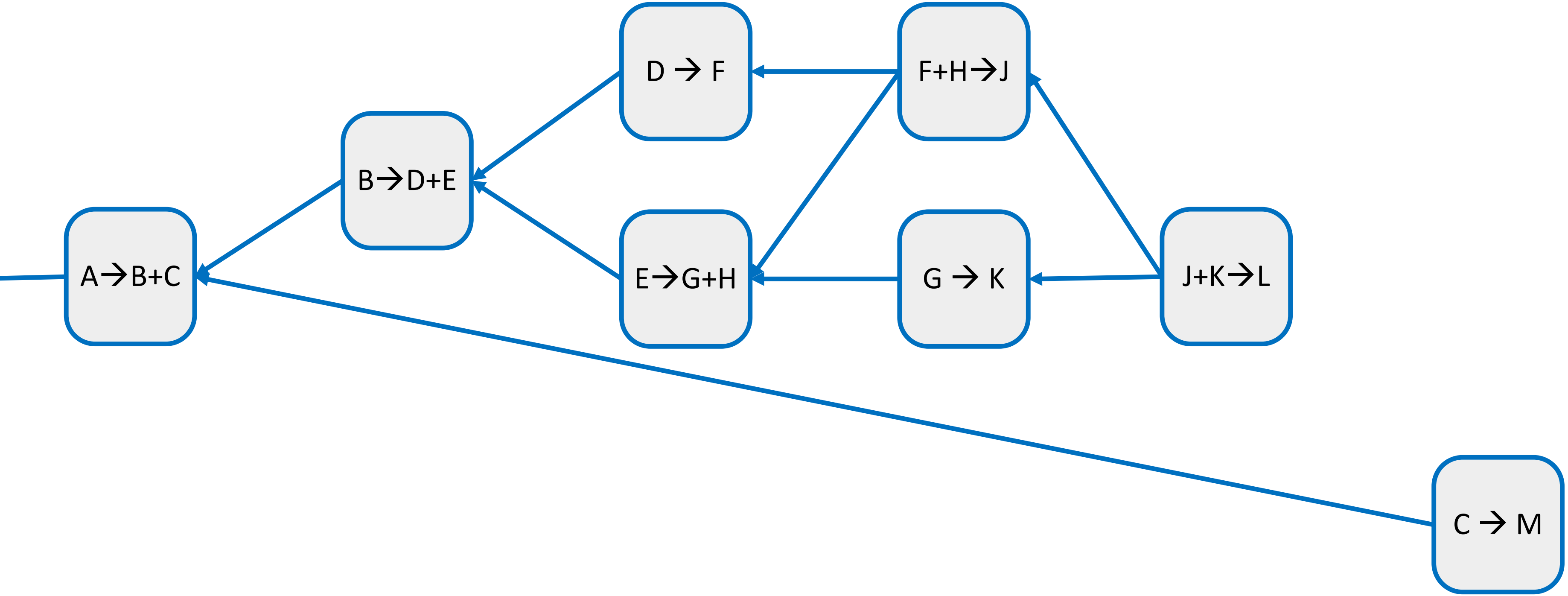
Less than 1/3 Malicious

Additional Condition

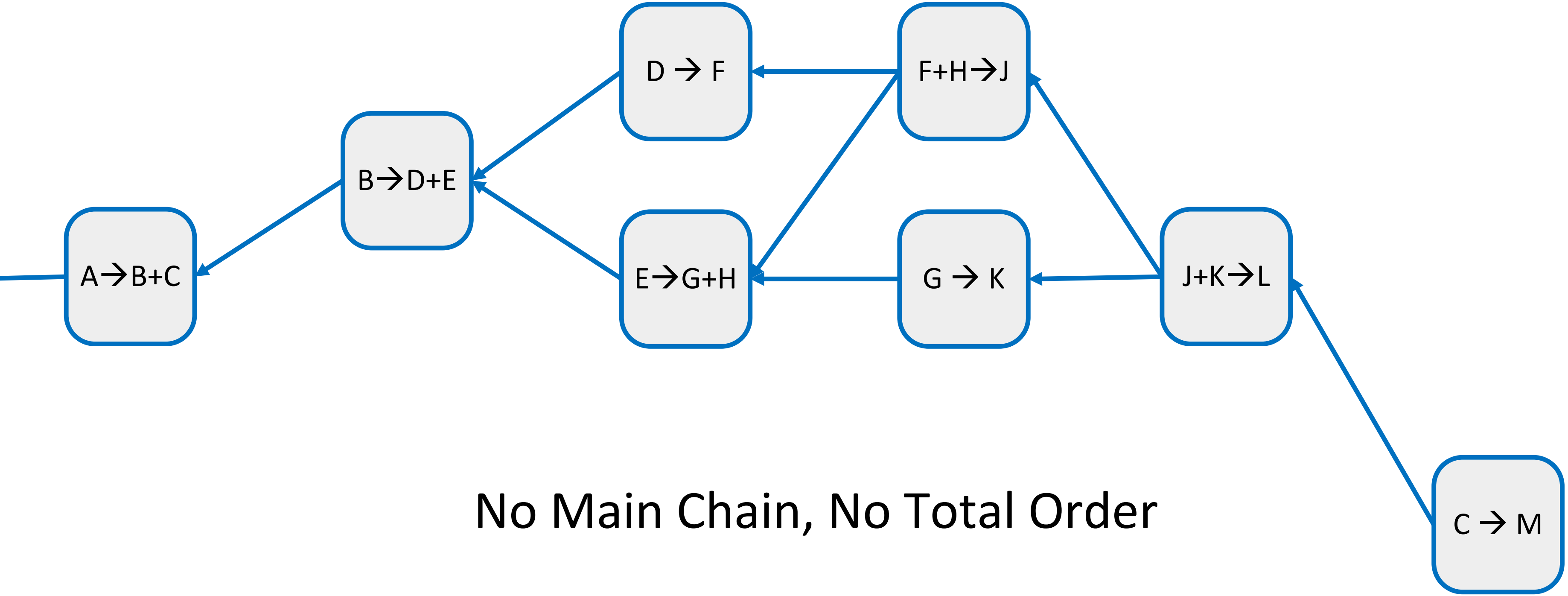
Single Owner Accounts*

*organized multi-owners, not fancy open-access smart contracts

Point to Money Source

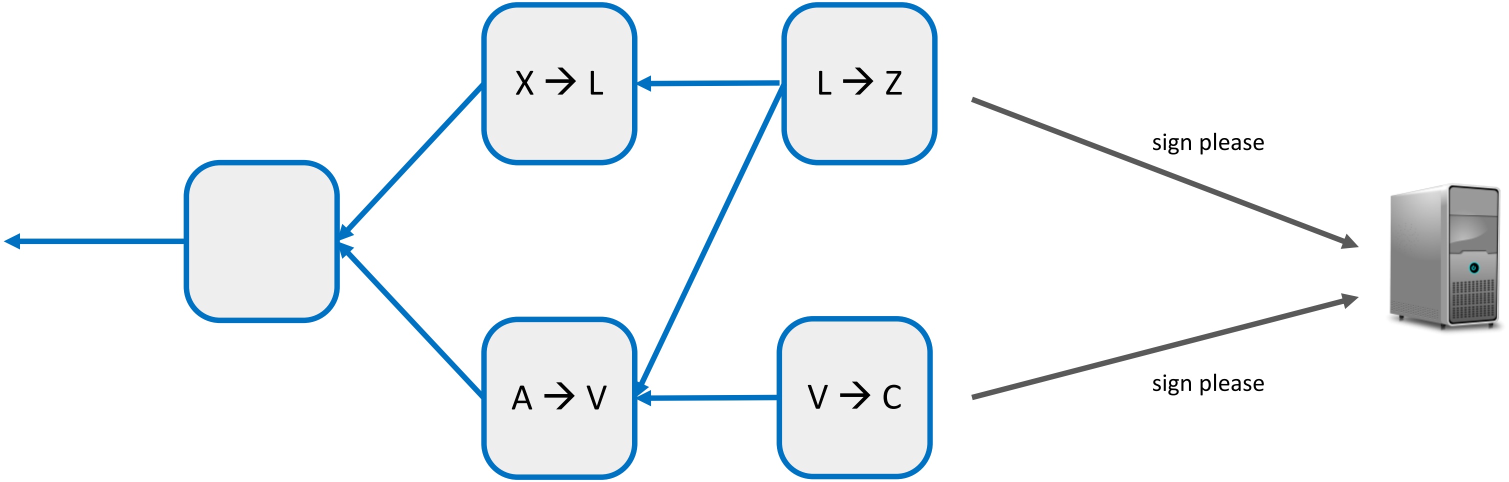


Point To All Transactions!

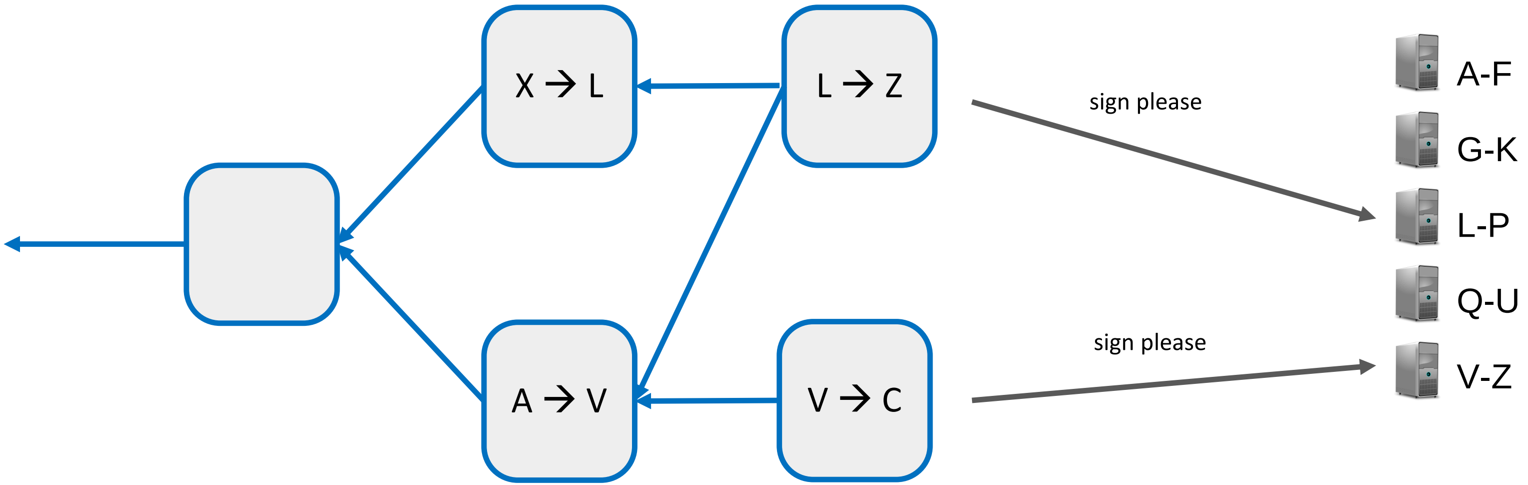


No Main Chain, No Total Order

Sharded Signing



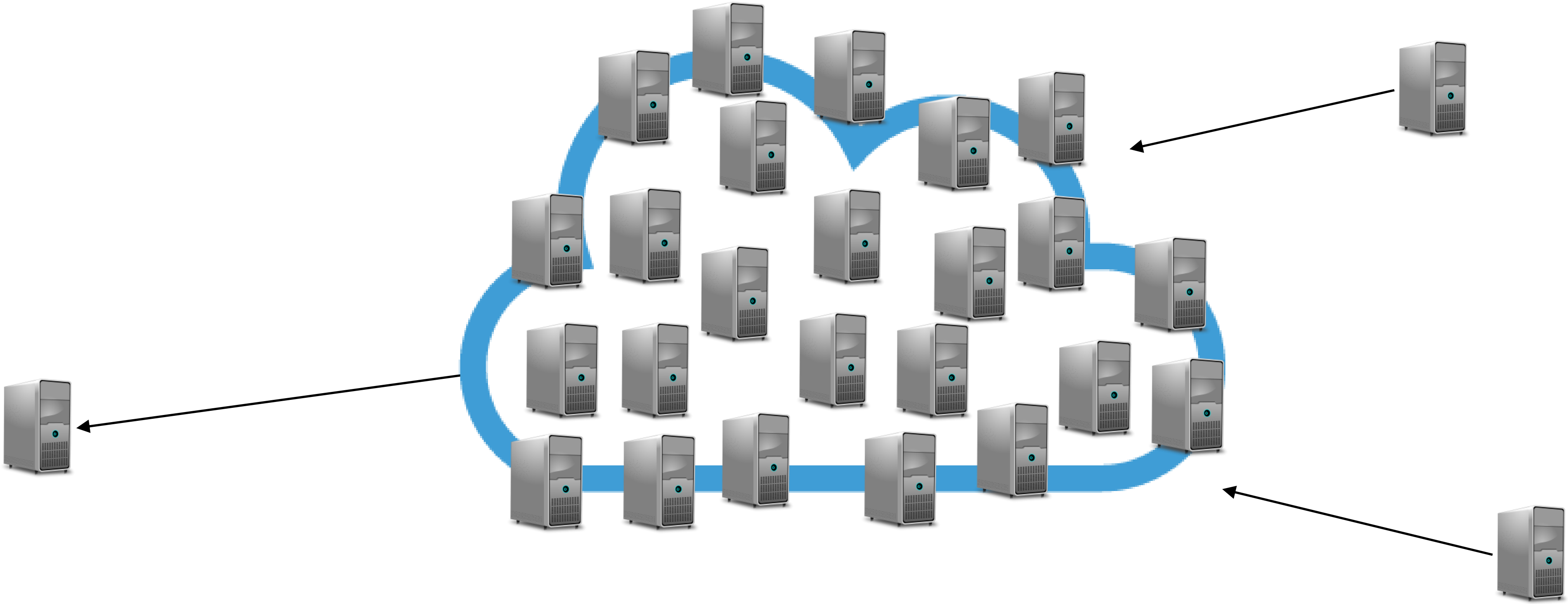
Sharded Signing

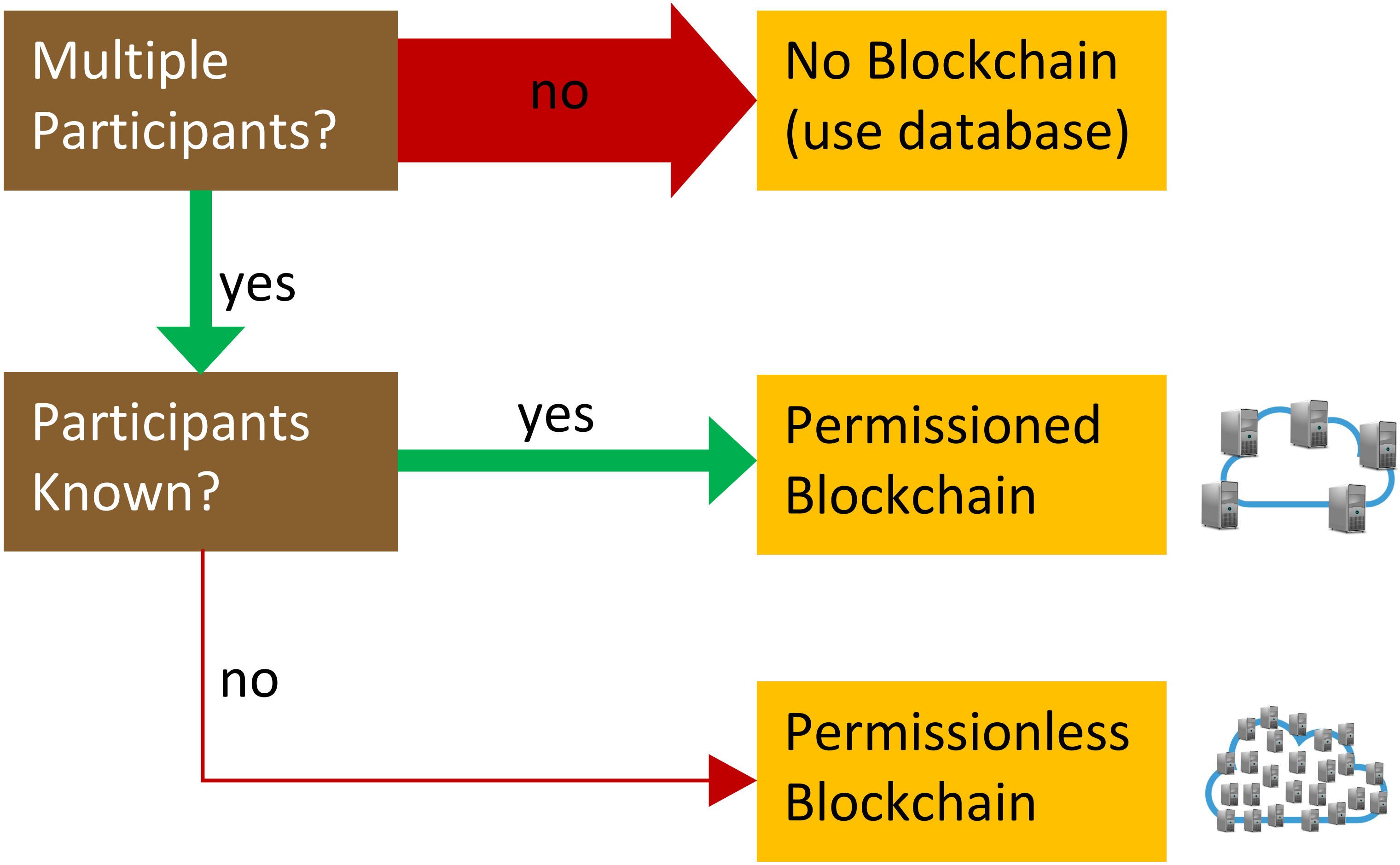


Also Permissionless?

(Without Proof-of-Work)

Permissionless / Open





Multiple Participants?

no

No Blockchain (use database)

yes

Participants Known?

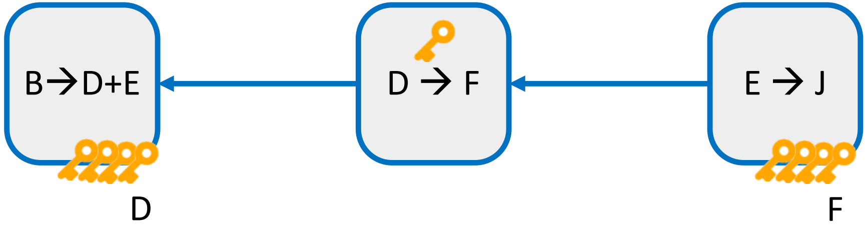
yes

Permissioned Blockchain

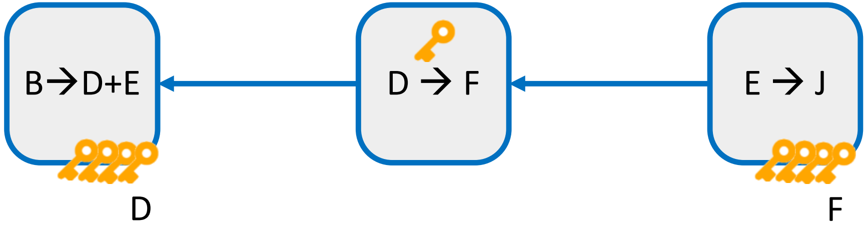
no

Permissionless Blockchain

1. Transferrable Signing Keys



1. Transferrable Signing Keys



2. Key Delegation (Pooling)

Thank You!

Questions & Comments?

Roger Wattenhofer, ETH Zurich, www.disco.ethz.ch

@grauhut

BiBi BlockChain