What Should We Learn From Nakamoto's Blockchain?

Roger Wattenhofer

ETH Zurich – Distributed Computing Group


Not
Me!

Blockchain: The Biggest Story in Distributed Systems Since …

… the Internet?!?

Cryptocurrencies


GAME OF THRONES™

Blockchain


the office

FinTech developers and managers understand that the *blockchain* has the potential to disrupt the financial world. The blockchain allows the participants of a distributed system to agree on a common view of the system, to track changes in the system, in a reliable way. In the distributed systems community, agreement techniques have been known long before cryptocurrencies such as Bitcoin (where the term blockchain is borrowed) emerged. Various concepts and protocols exist, each with its own advantages and disadvantages. This book introduces the basic techniques when building fault-tolerant distributed systems, in a *scientific* way. We will present different protocols and algorithms that allow for fault-tolerant operation, and we will discuss practical systems that implement these techniques.

About the author

Roger Wattenhofer is a professor at ETH Zurich. Before joining ETH Zurich, he was at Brown University and Microsoft Research. His research interests include fault-tolerant distributed systems, efficient network algorithms, and cryptocurrencies such as Bitcoin. He has published more than 250 scientific articles.

Inverted Forest Publishing
First Edition, 2016
ISBN-13 978-1522751830
ISBN-10 1522751831

So What Is a Blockchain?

Ledger of Transactions

Bitcoin

Figure 9-3 Manual Journal Voucher.

Page 1 of 1

MANUAL JOURNAL VOUCHER

Batch 1101 | Batch Line 9

Description ACCRUED INTEREST INCOME

Reference JY3-JAN INTEREST

PREPARED BY WLR | DATE 2/2/X5

APPROVED | DATE

Total Amount 11,200.20

Effective Date 1/31/X5 | Type A

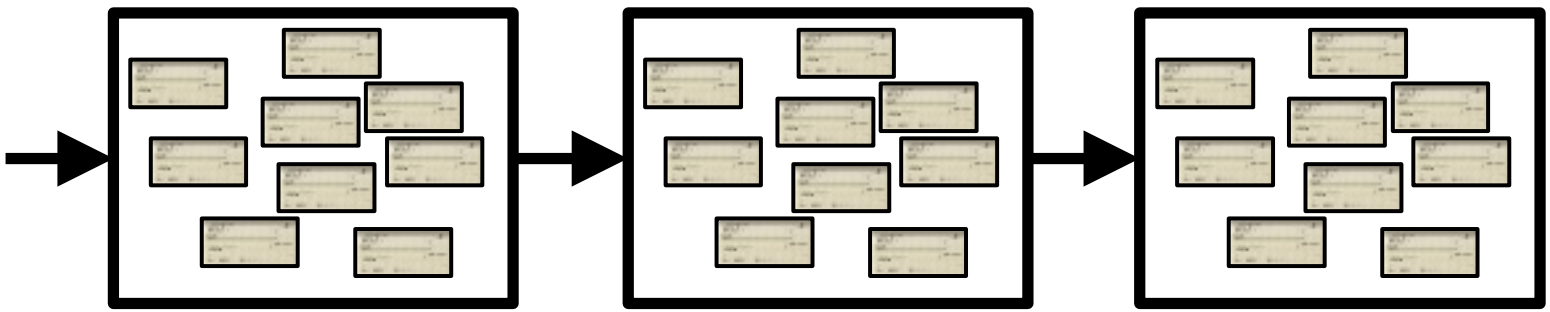
Accounting Company 10 - CORPORATE

Account Number	Description	Debit Amount	Credit Amount
1280-000	INTEREST RECEIVABLE	11,200.20	
8050-010	FIRST NATIONAL - CD		1,330.10
050-030	MUNICIPAL BONDS		6,220.80
050-010	OTHER INVESTMENTS		3,649.30

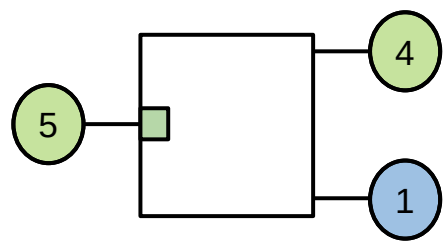
Blockchain

Distributed Systems (1982) & Cryptography (1976)

Blockchain



Transaction



Why the Hype?

Let’s Dig Deeper!

Blockchain

Persistence

NIL

↓

Immutable

↓

Provable 

Fault-Tolerance

NIL

↓

Crash

↓

Byzantine 

Blockchain

Speed

Eventual 

↓

Strong

↓

Immediate

Throughput

10 tx/s 

↓

10k tx/s

↓

10m tx/s

Blockchain

Scalability

10 nodes

↓

100 nodes

↓

1000 nodes 

Energy Consumption

Proof of Work

Hashrate · Energy/Hash ≈ 1.3 GW

$13 \cdot 10^9$ GH/s 0.1 J/GH

Economic Incentives

Market / Energy Value ≈ 19 GW

$20k/BTC

12.5 BTC $0.08/kWh

6/h

Upper Bound 19 GW

Reality? Well…

Lower Bound 1,3 GW

Maybe Around 5 GW

Blockchain

Scalability

10 nodes

↓

100 nodes

↓

1000 nodes 

Energy

Country 

↓

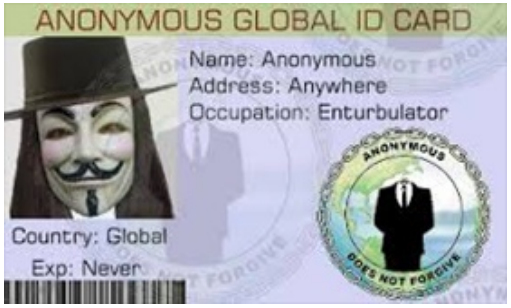
Village

↓

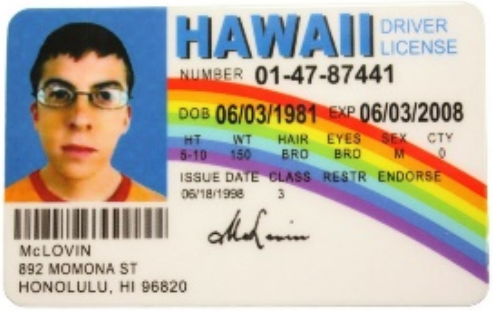
Server Room

What About Privacy?

It’s Complicated.



Privacy



Operator

World

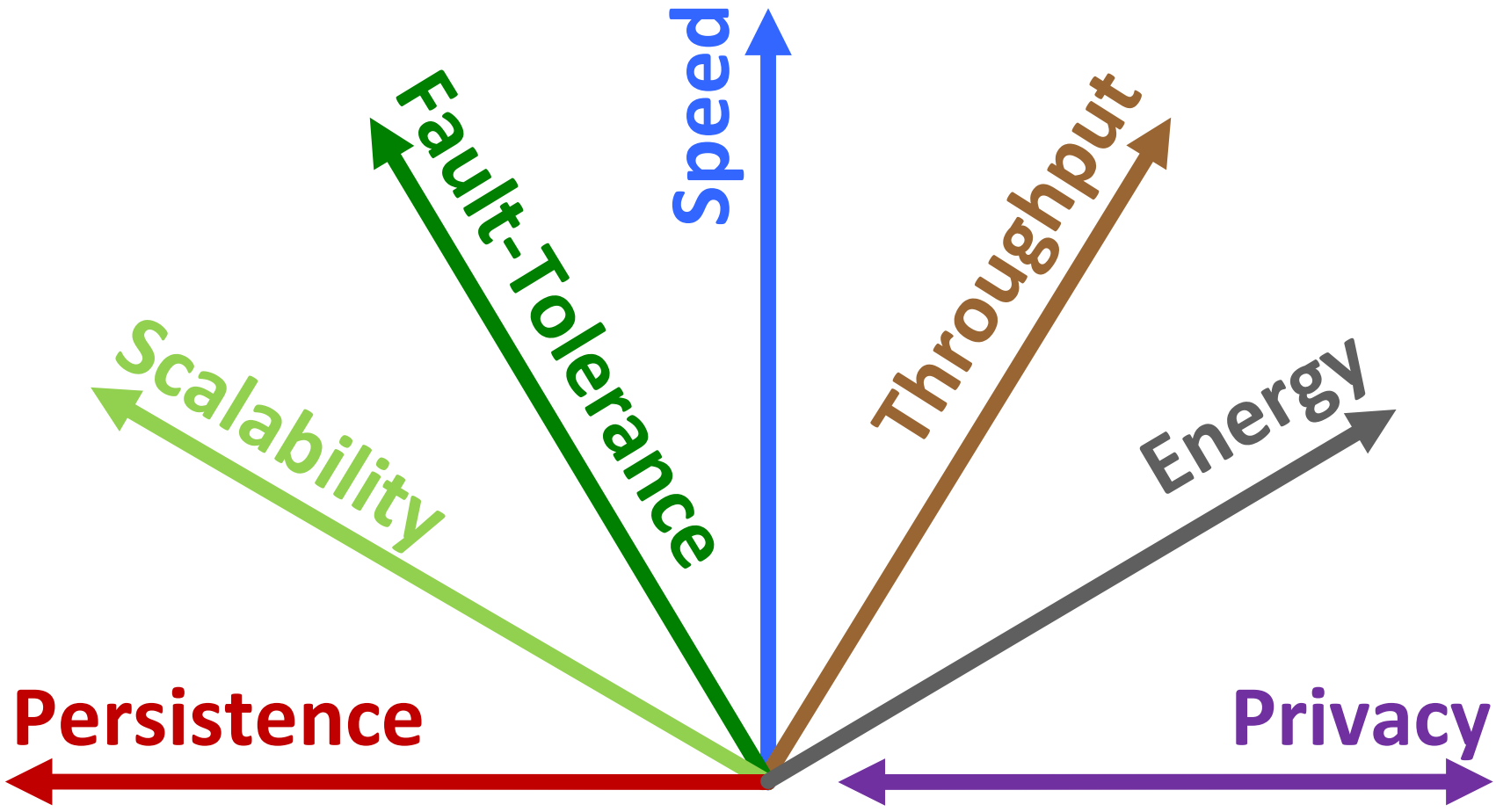
Open PoW

Hacker stahlen ETH-Doktoranden Bitcoin für 9 Millionen

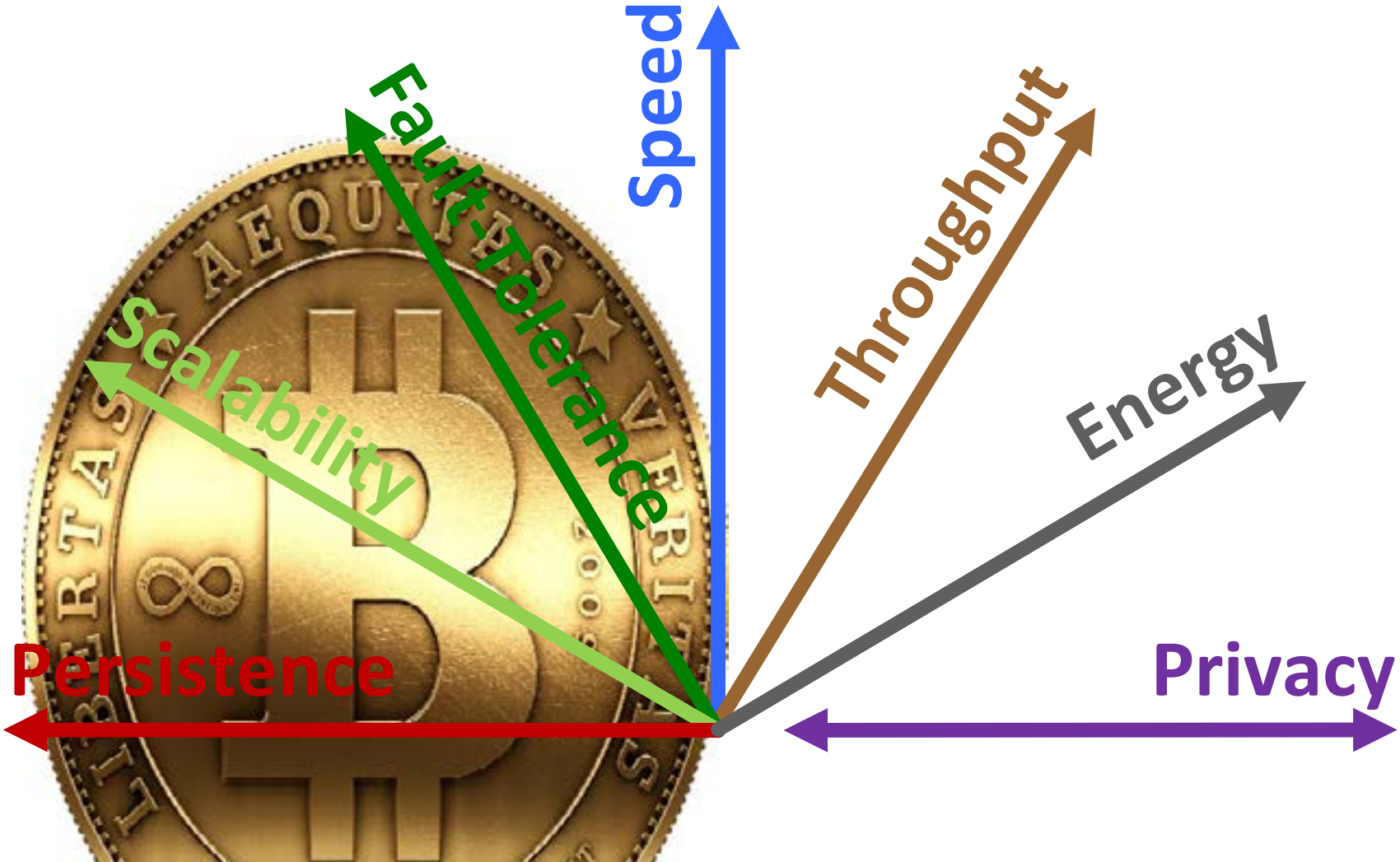
Diebstahl Hacker erbeuteten bei einem Mitarbeiter der ETH Zürich 9222 Bitcoin. Heute sind die virtuellen Münzen 9 Millionen Franken wert. Der Fall liegt nun bei der Kantonspolizei.

VON CHRISTIAN BÜTIKOFER 06.12.2013

The Seven Blockchain Dimensions



The Seven Blockchain Dimensions

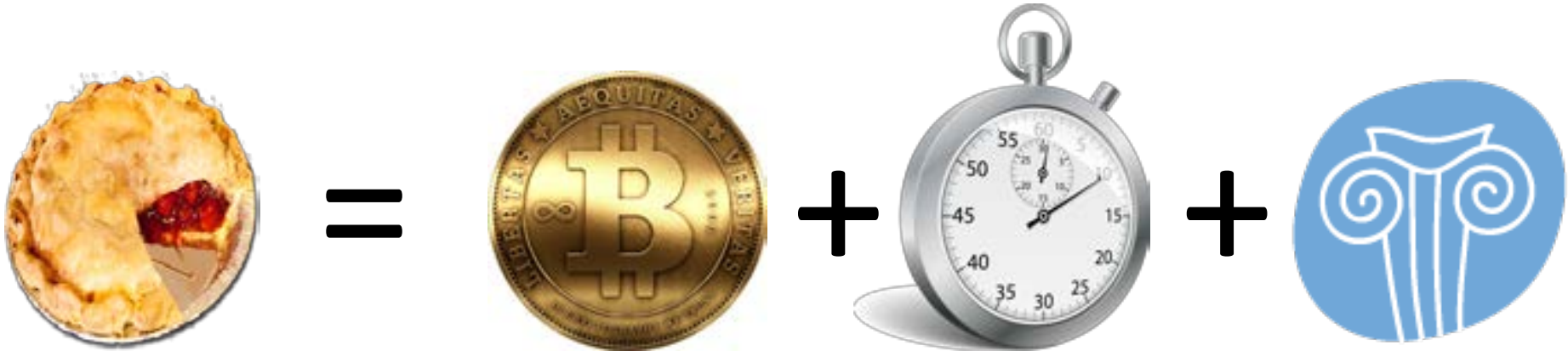


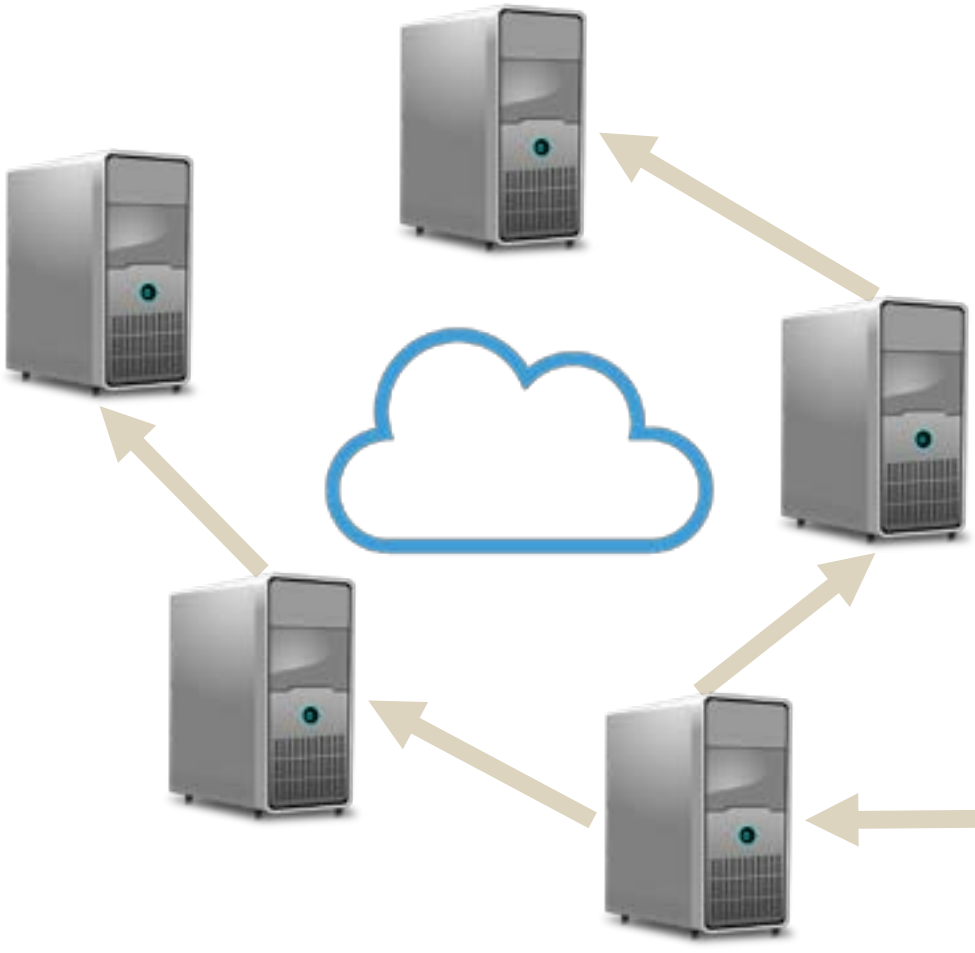
Plenty of Research Dimensions

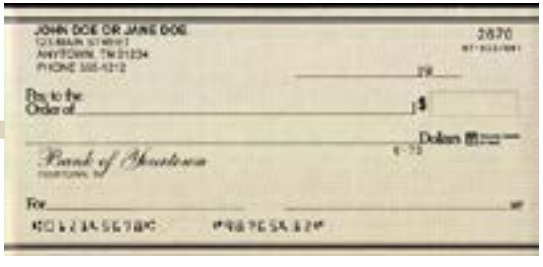
piChain

piChain: When a Blockchain Meets Paxos

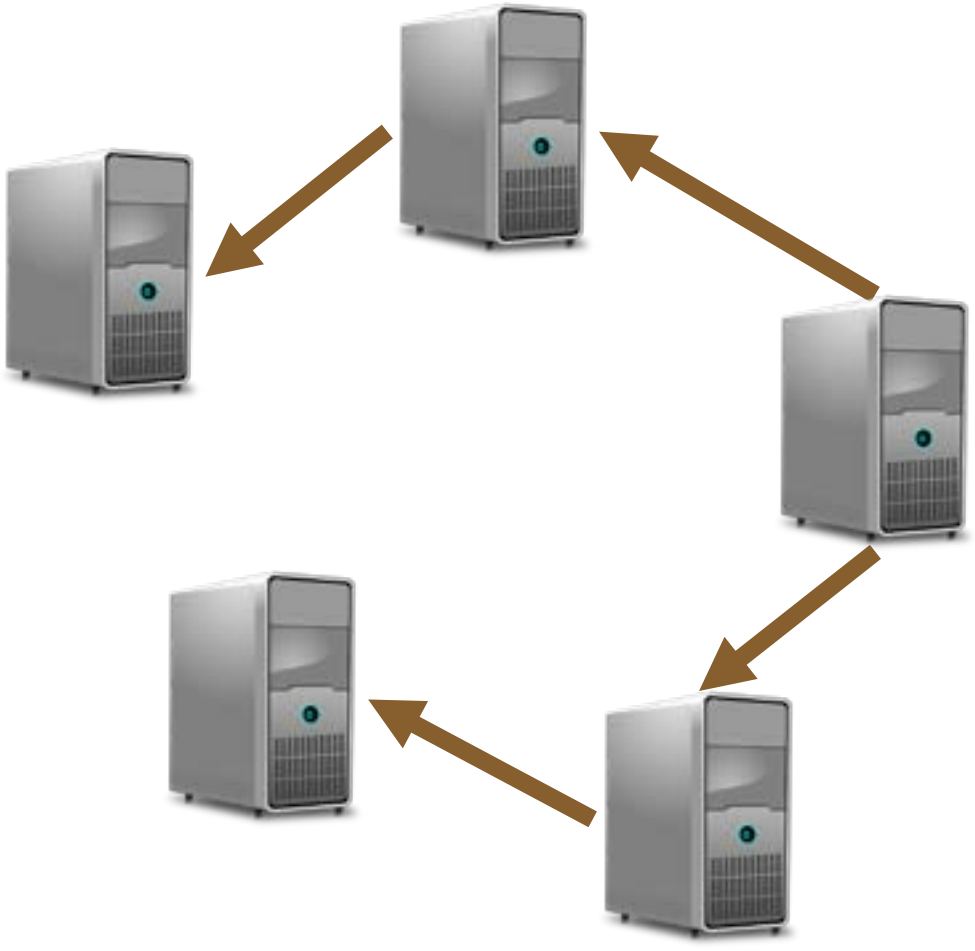
piChain: When a Blockchain Meets Paxos



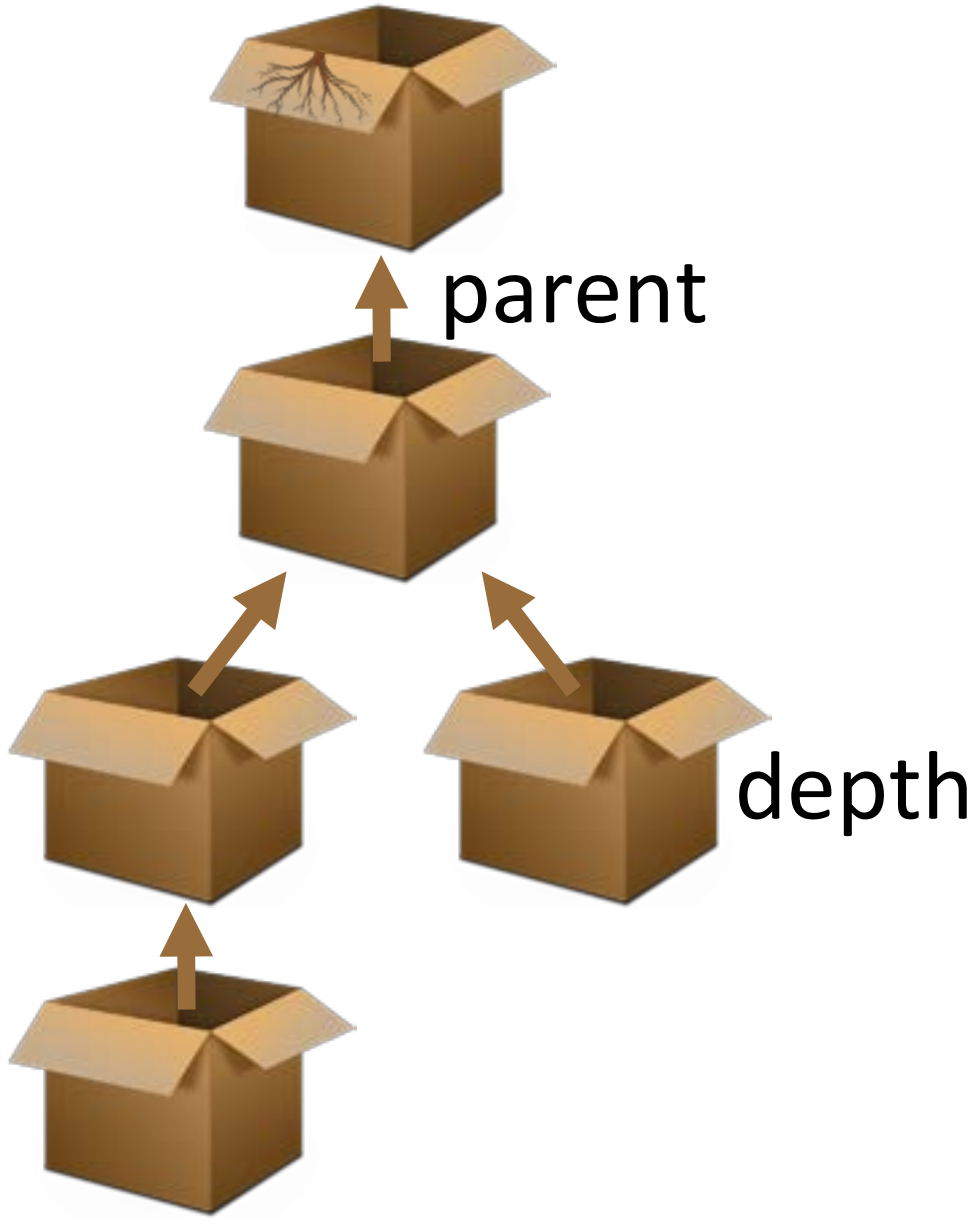




Transaction



Block


parent
depth

slow

medium

quick

New Transaction: Reaction Time

wait

wait

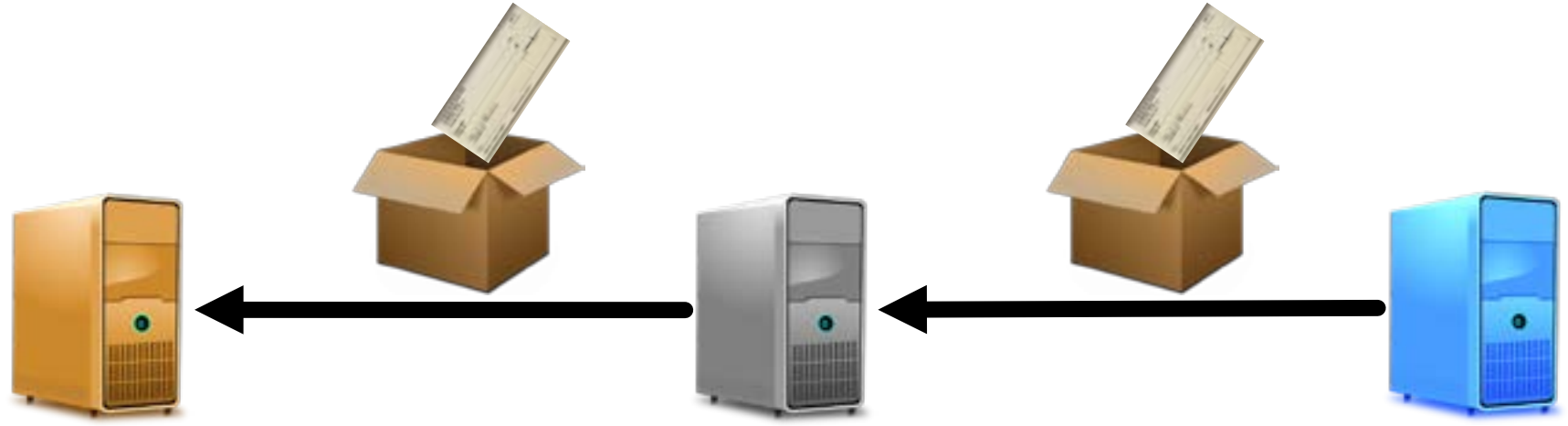
quick

medium

slow

time

State Transitions

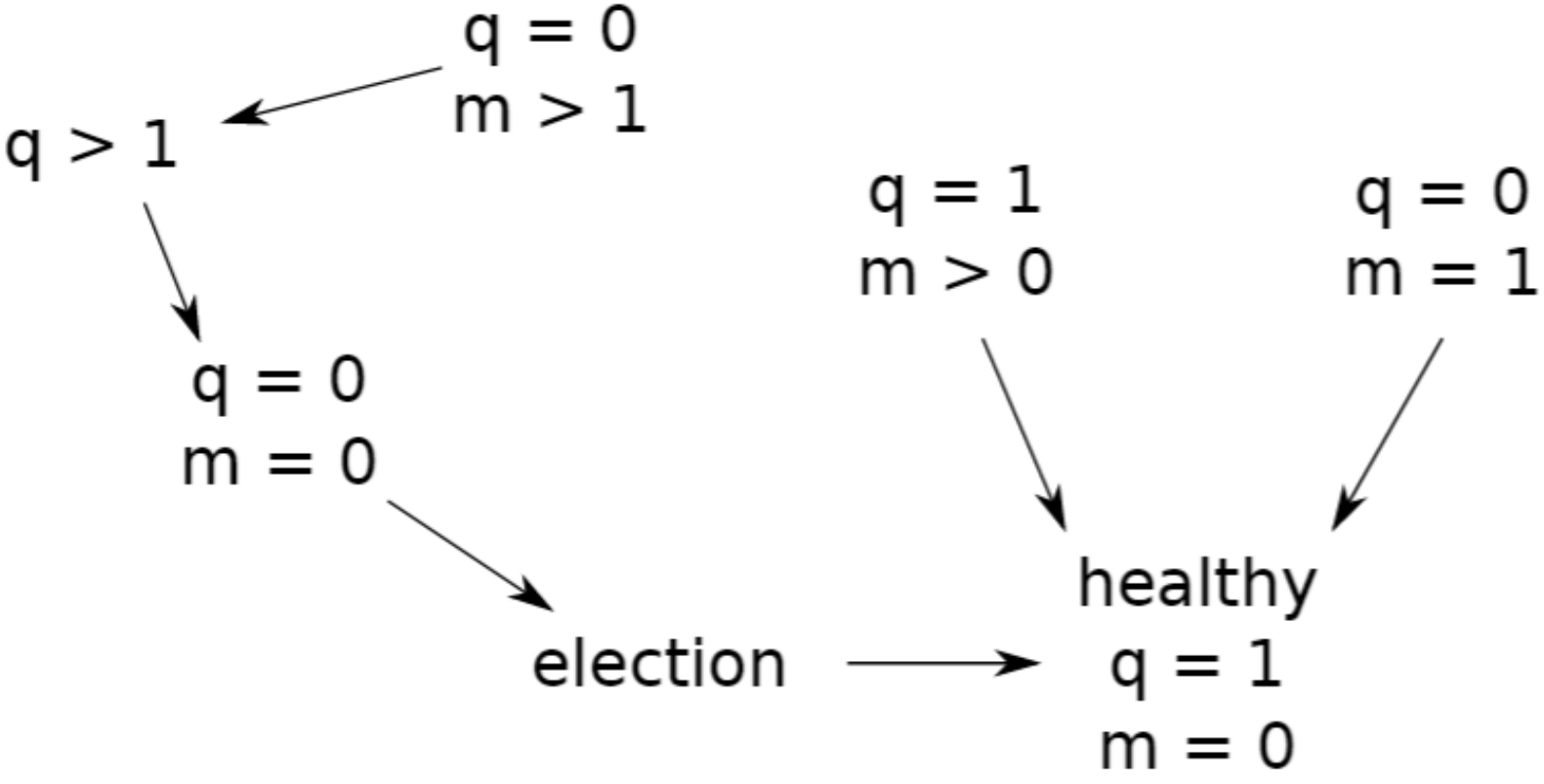


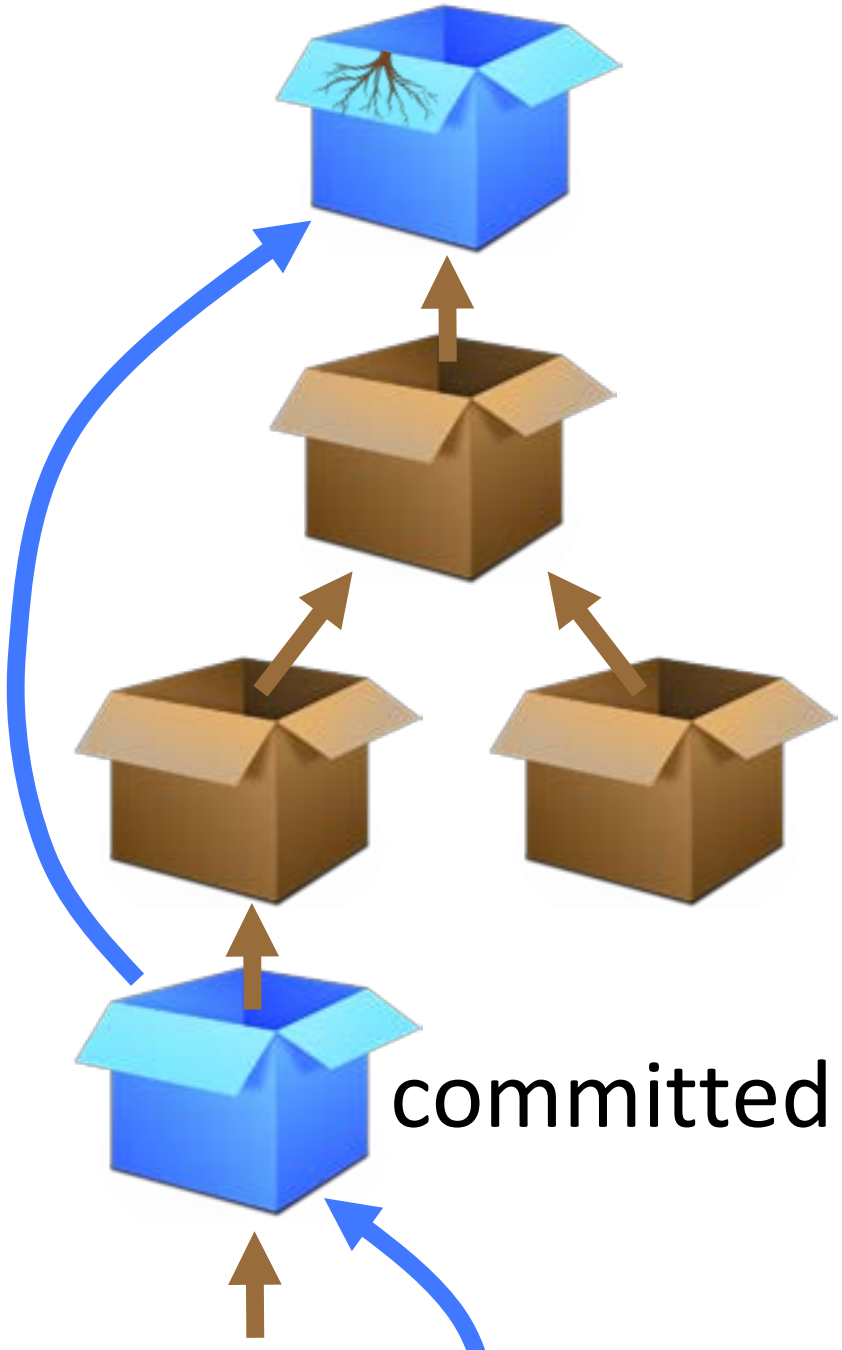
seen  : either deeper or by 

Self-Healing

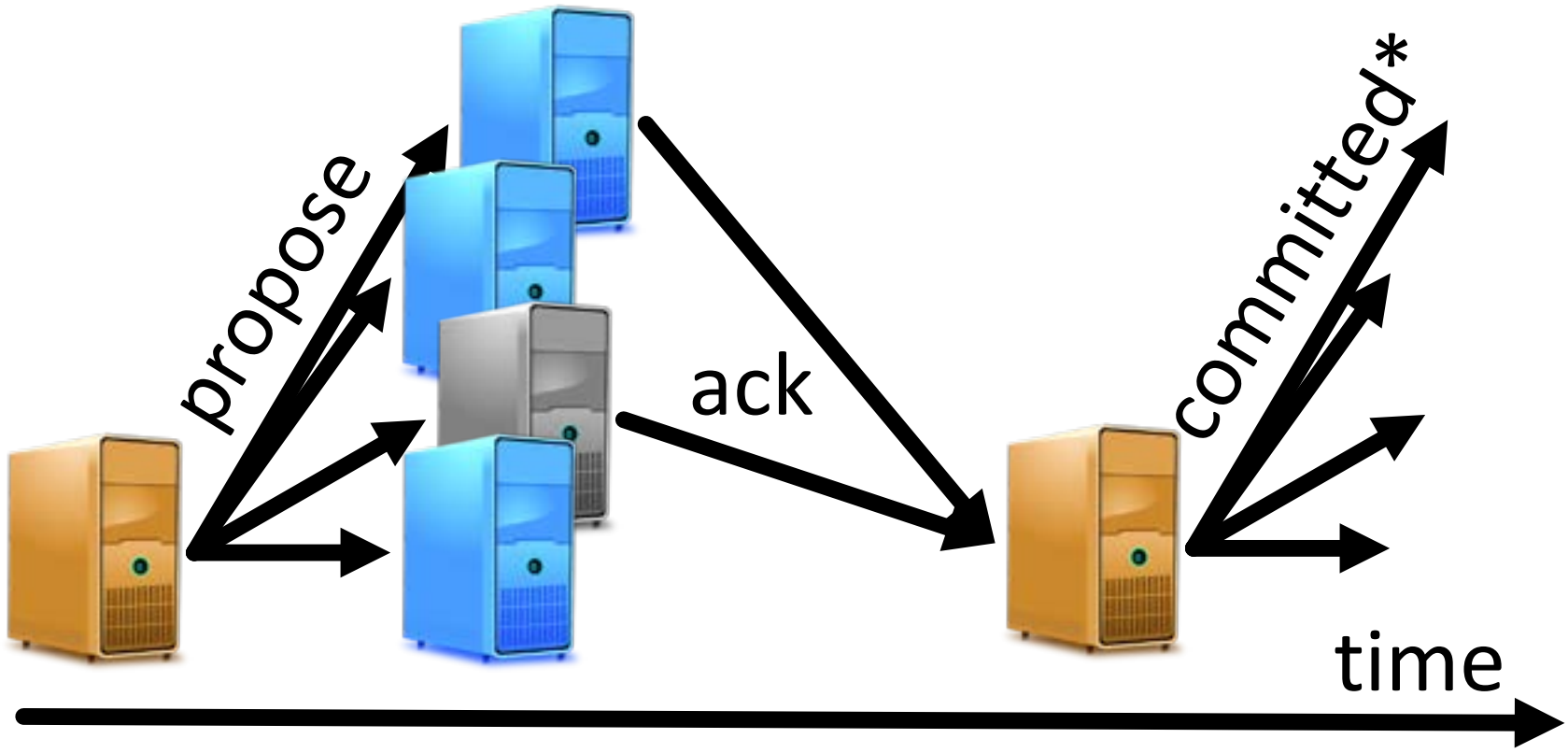
healthy

Self-Healing




committed

Truncated Paxos



*and next propose

Normal Paxos

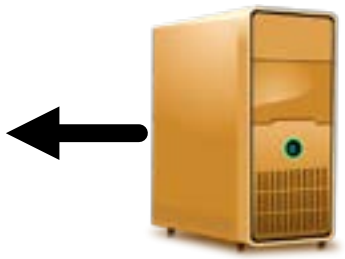
Round 1 .....

1: Quick node q sends "try b_{new}" to all nodes

2: On receiving a try message, all nodes:
3: **if** b_{new} deeper than b_{max} **then**
4: $b_{\text{max}} = b_{\text{new}}$
5: Answer q with "ok b_{prop}, b_{supp}"
6: **end if**

Round 2 .....

7: Node q: If majority responded with ok:
8: $b_{\text{com}} = b_{\text{new}}$
9: **if** some response included $b_{\text{prop}} \neq \perp$ **then**
10: $b_{\text{com}} = b_{\text{prop}}$ with deepest b_{supp}
11: **end if**
12: Node q sends "propose b_{com}, b_{new}" to all nodes

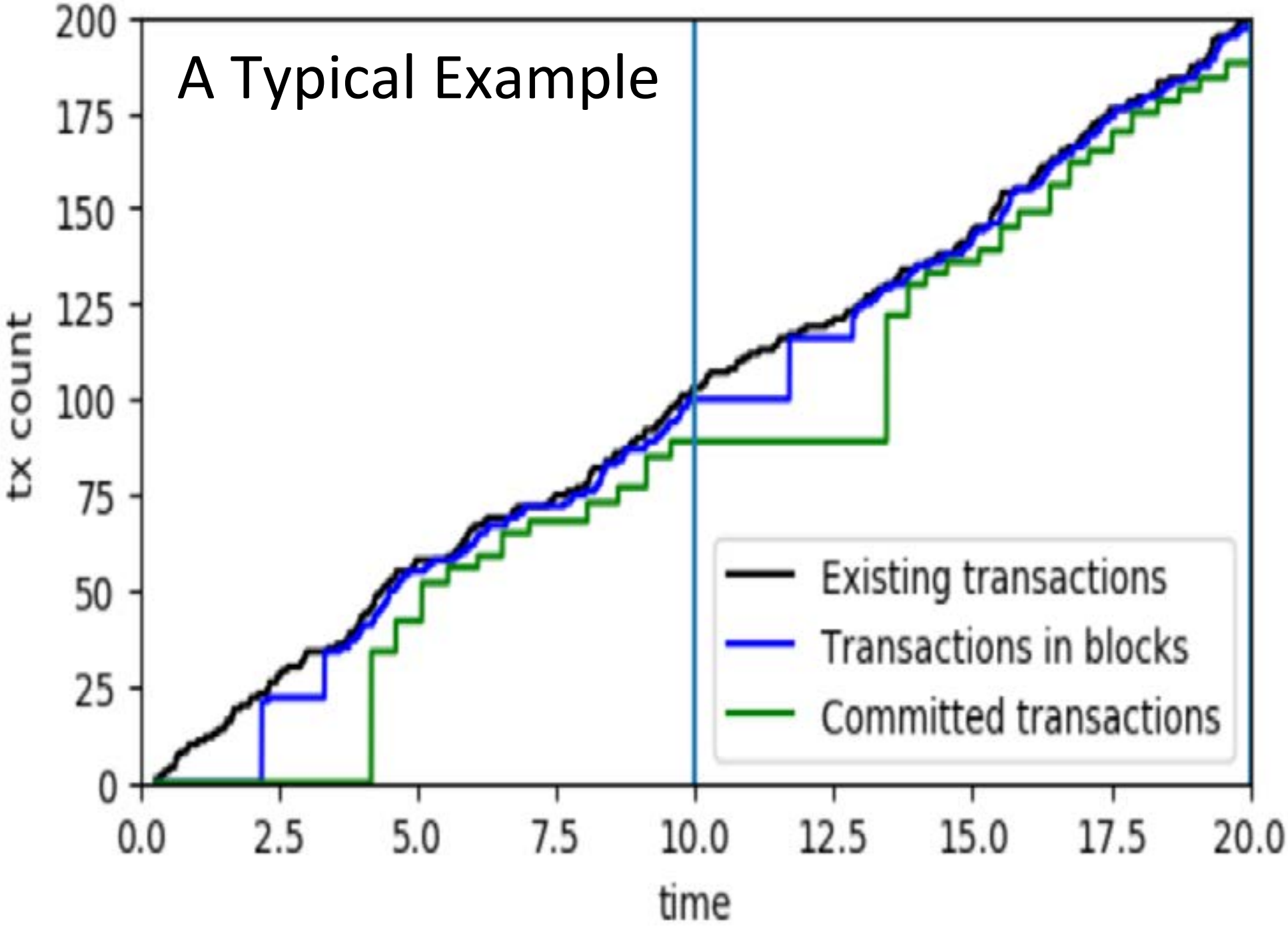


13: On receiving a propose message, all nodes:
14: **if** $b_{\text{new}} = b_{\text{max}}$ **then**
15: $b_{\text{prop}} = b_{\text{com}}$
16: $b_{\text{supp}} = b_{\text{new}}$
17: Answer q with "ack b_{com}"
18: **end if**

Round 3 .....

19: Node q: If majority responded with ack:
20: Node q sends "commit b_{com}" to all nodes

21: On receiving a commit message, all nodes:
22: Store b_{com} in their list of committed blocks


A Typical Example
200
175
150
125
100
75
50
25
0
tx count
0.0
2.5
5.0
7.5
10.0
12.5
15.0
17.5
20.0
time
Existing transactions
Transactions in blocks
Committed transactions

piChain vs. Raft

similar essentially same goals

simple e.g., no explicit leader election

silent no msg when no tx, no heartbeat

scalable O(1) msgs per node per tx

Blockchain

Persistence

NIL

Immutable

Provable

Fault-Tolerance

NIL

Crash

Byzantine

Blockchain

Speed

Eventual 

↓

Strong

↓

Immediate 

Throughput

10 tx/s 

↓

10k tx/s 

↓

10m tx/s

Blockchain

Scalability

10 nodes 

100 nodes

1000 nodes 

Energy

Country 

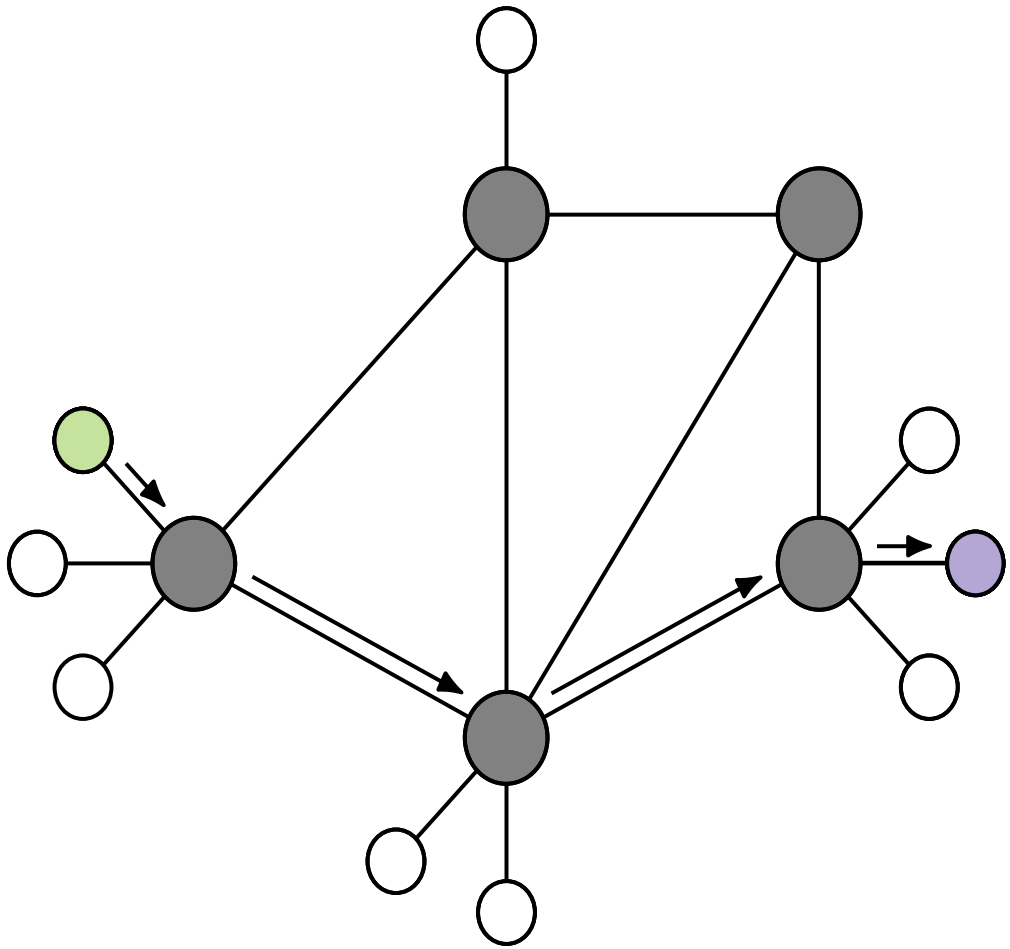
Village

Server Room 

Fundamental Problem
Every Node Sees Every Transaction

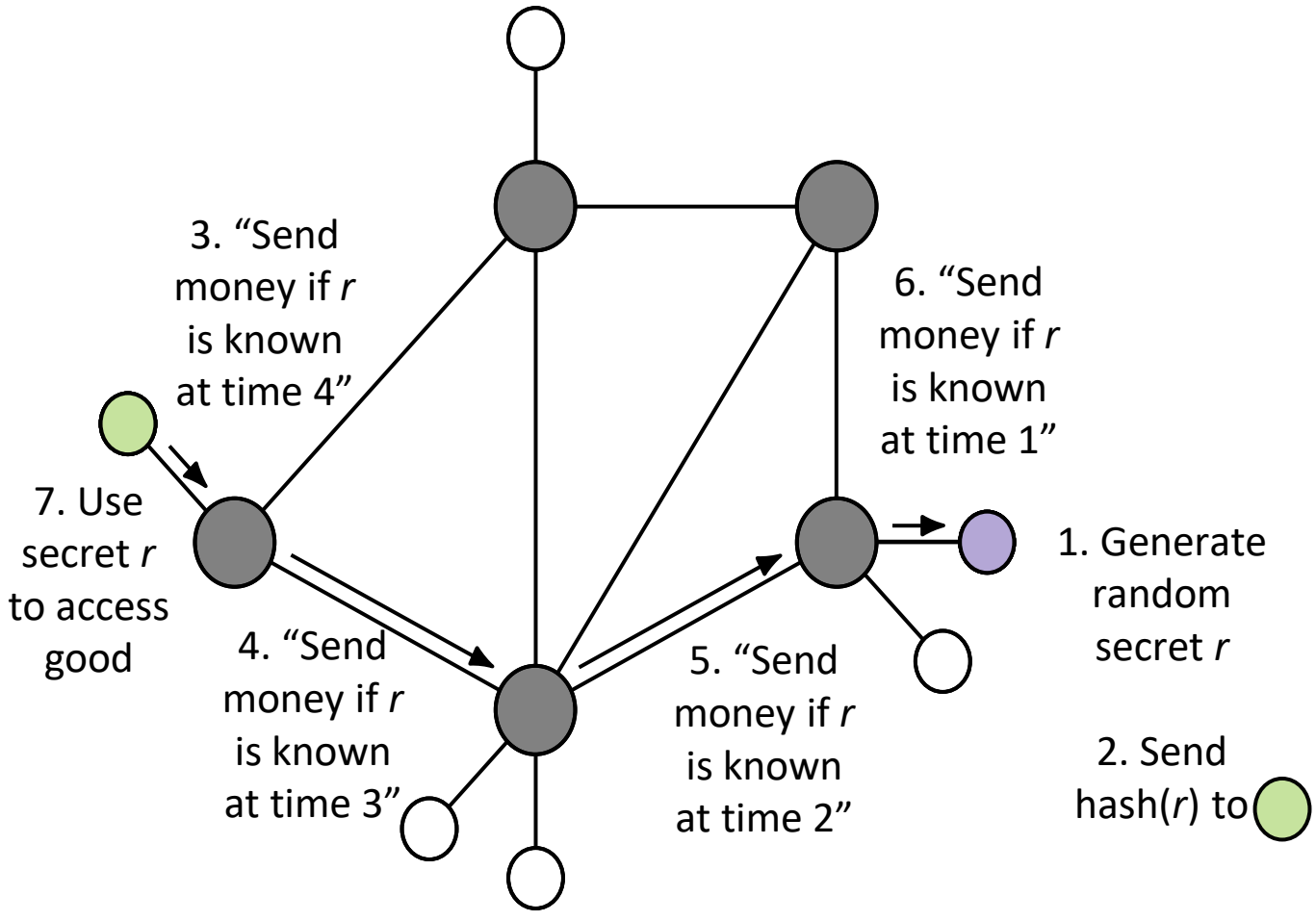
Payment Networks

Payment Network



Hashed Timelocked Contract (HTLC)

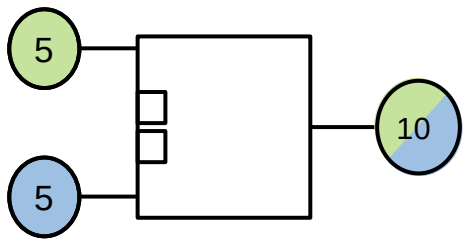
HTLC Example (sells to)



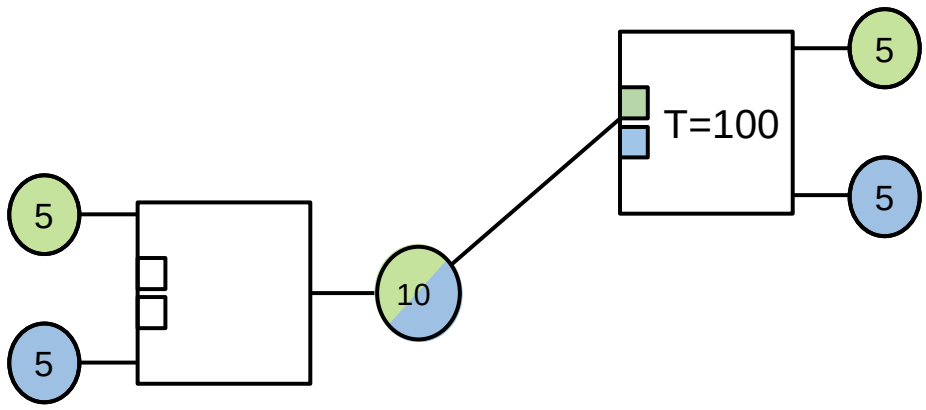
Single Hop in Network

Duplex Micropayment Channels (Example for Smart Contract)

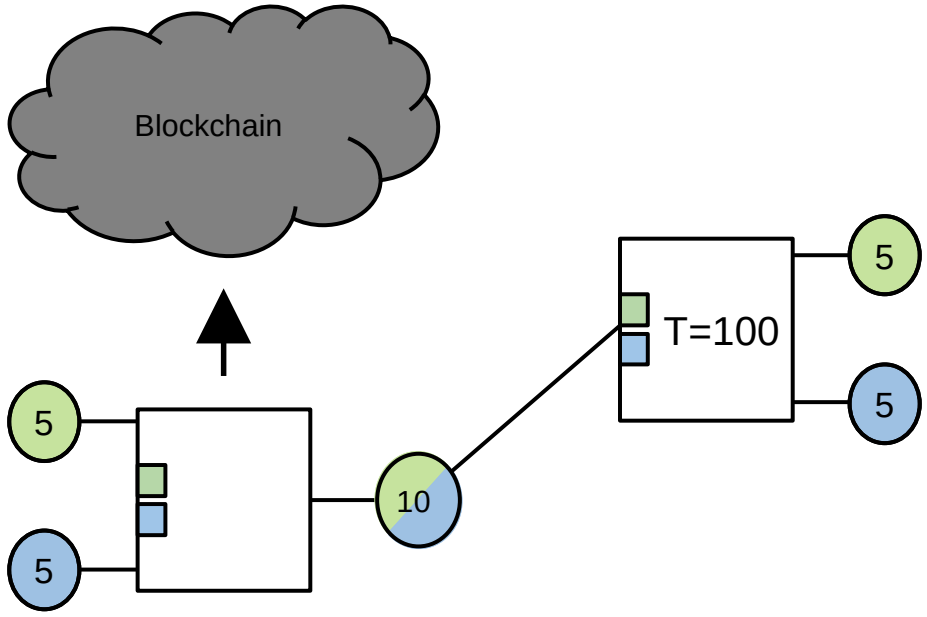
Duplex Micropayment Channel



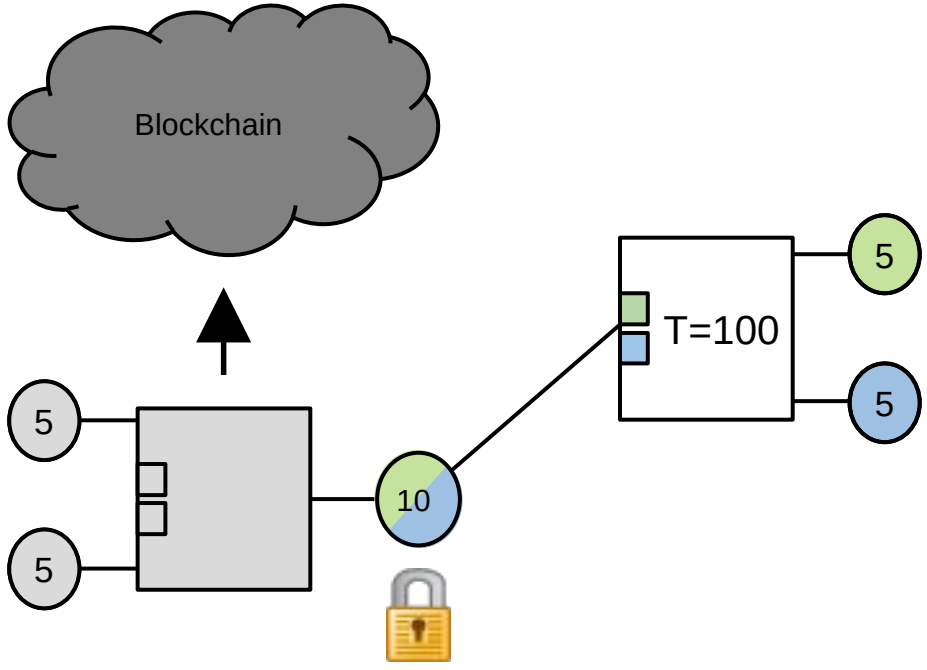
Duplex Micropayment Channel



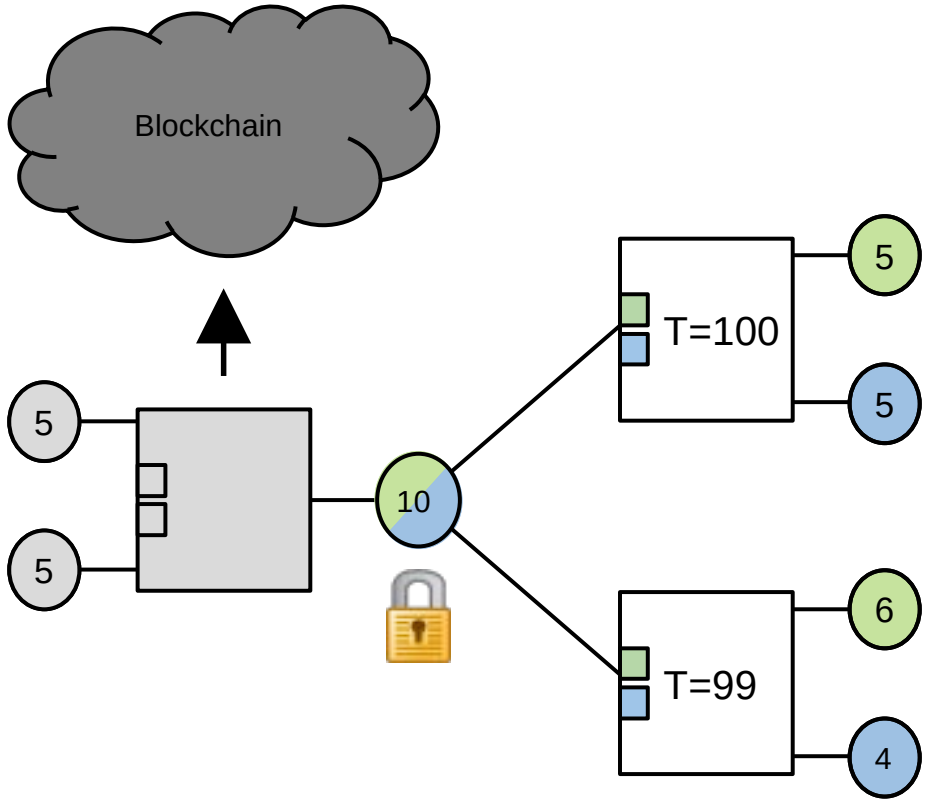
Duplex Micropayment Channel



Duplex Micropayment Channel

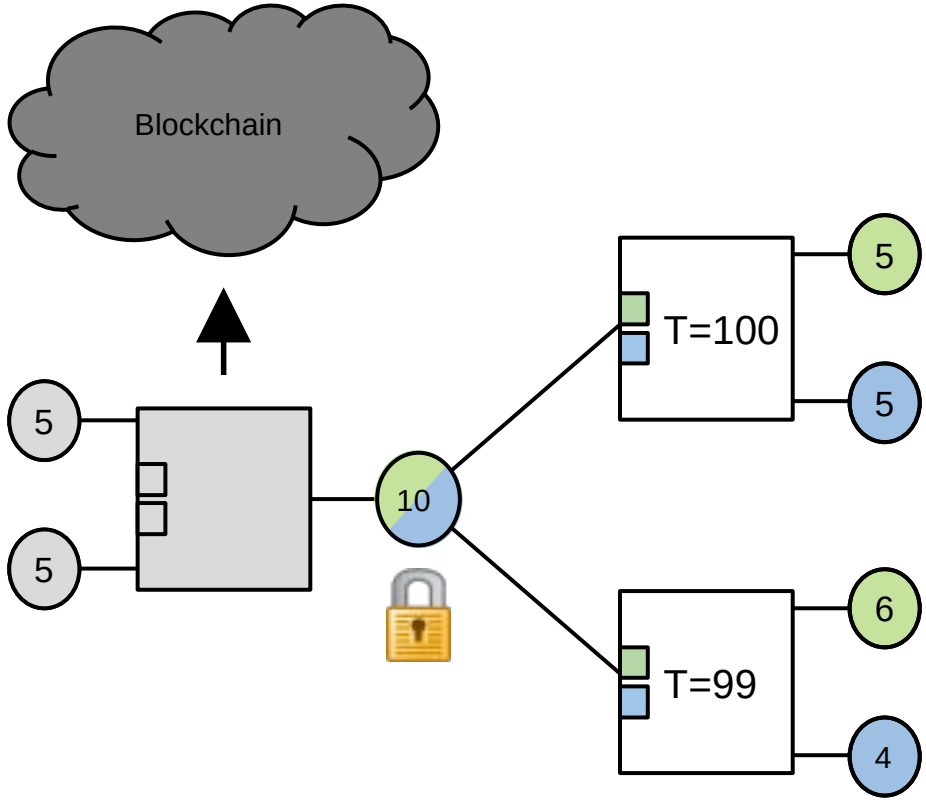


Duplex Micropayment Channel



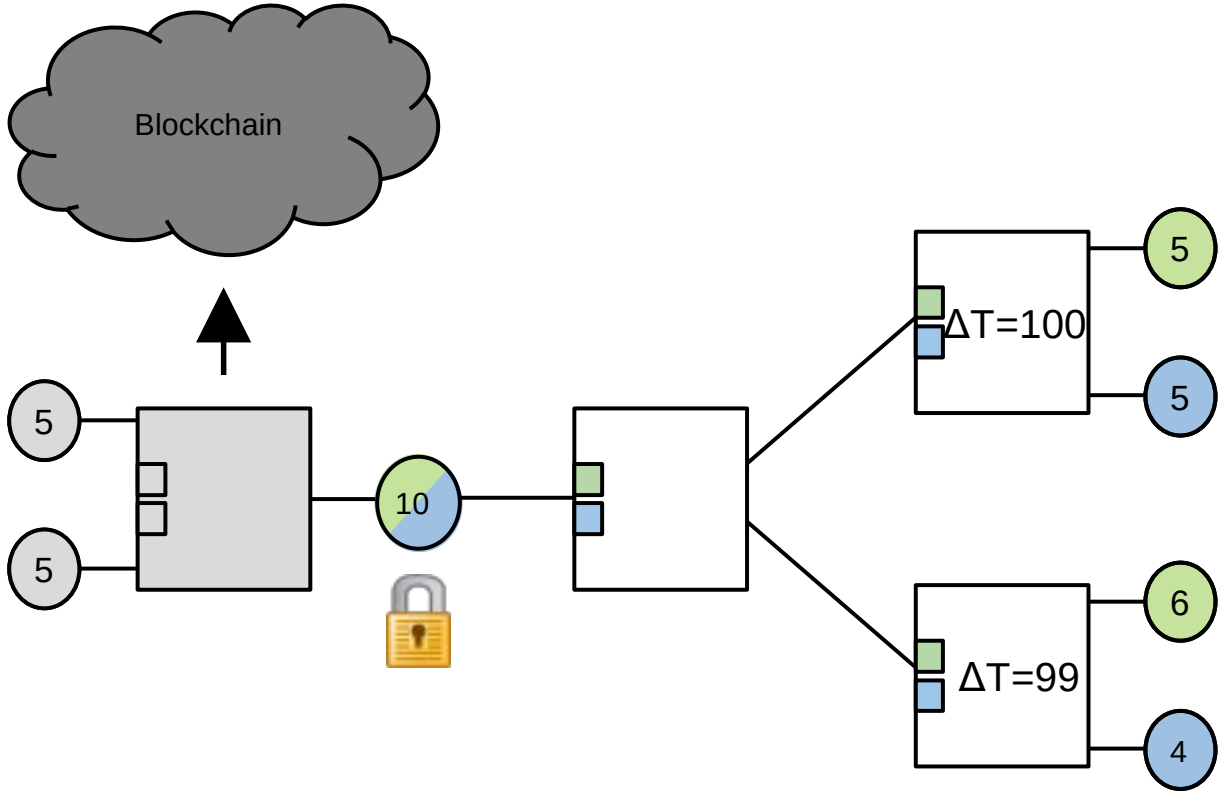
[Decker,W,2015]

Duplex Micropayment Channel



Channel must be renewed often?

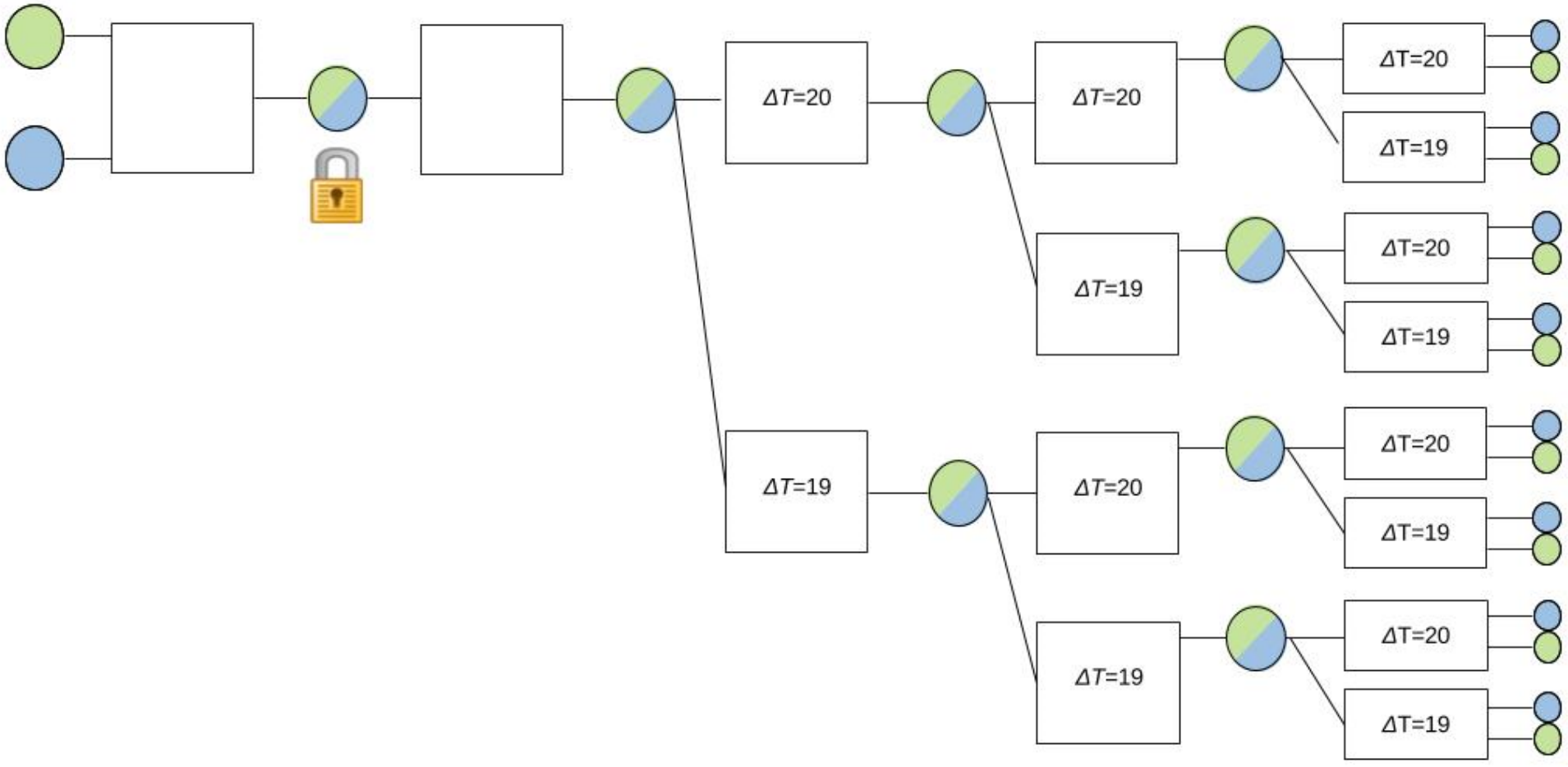
Duplex Micropayment Channel



Relative timelocks to keep channel alive forever!

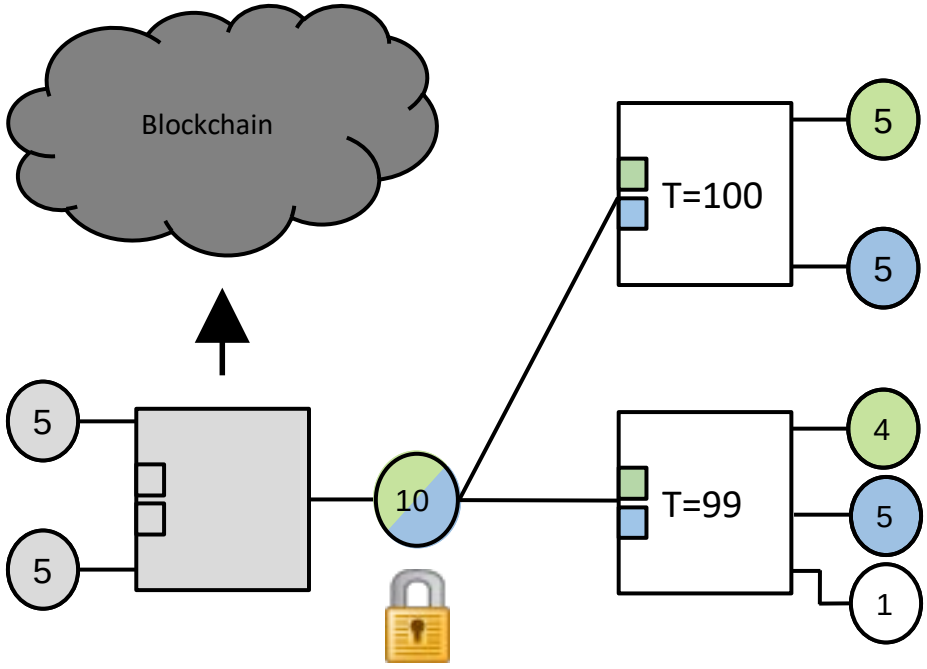
But only 99 transactions?

Duplex Micropayment Channel

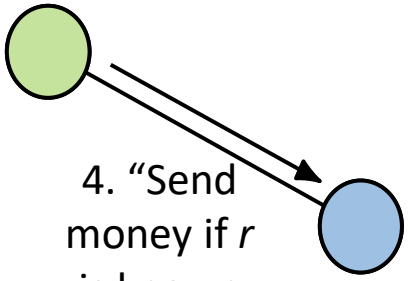


[Decker,W,2015]

HTLC Revisited

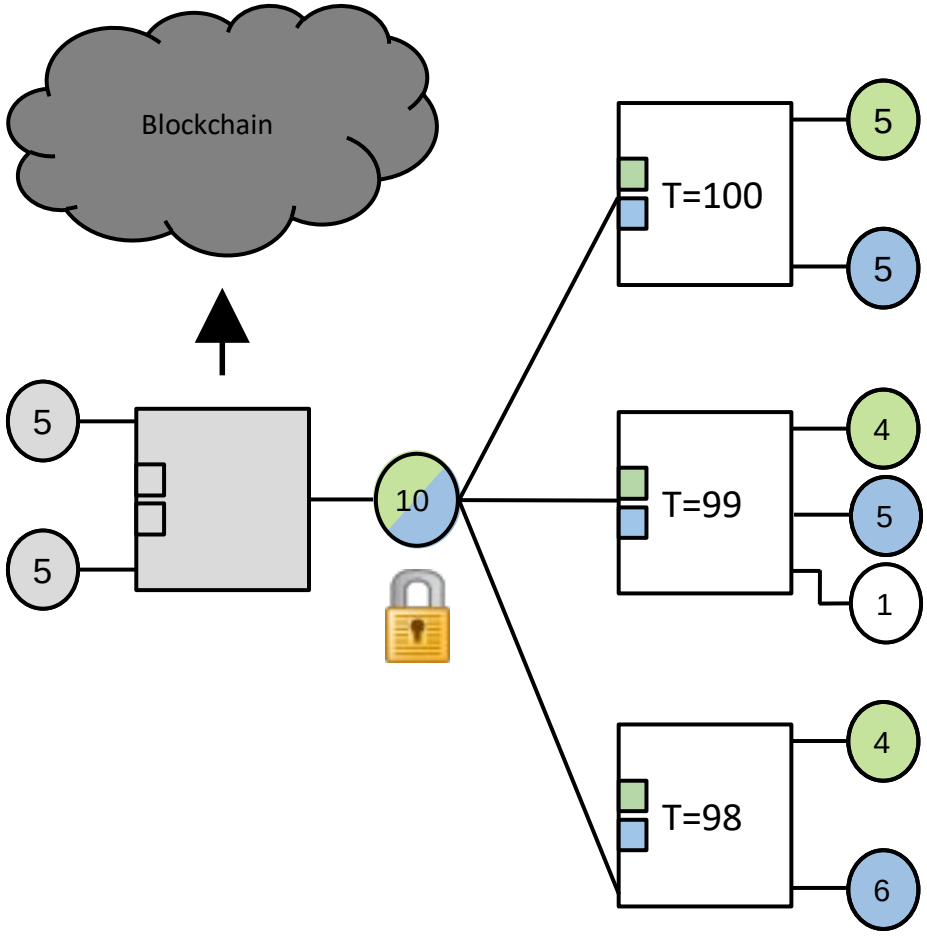


can be spent
by blue with secret *r* or
by green after 3 days

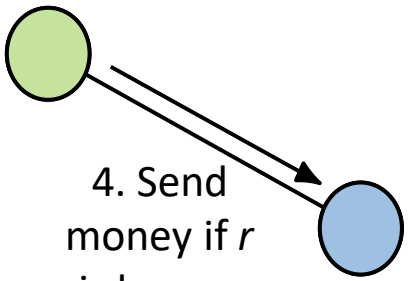


4. “Send money if *r* is known at time 3”

HTLC Revisited



can be spent
by blue with secret *r* or
by green after 3 days



4. Send
money if *r*
is known
at time 3

Solved?

Still Too Many Channels!?

Each and Every Channel

… needs two transactions on blockchain

… has locked-in funds by both parties

Each and Every Channel

… needs two transactions on blockchain

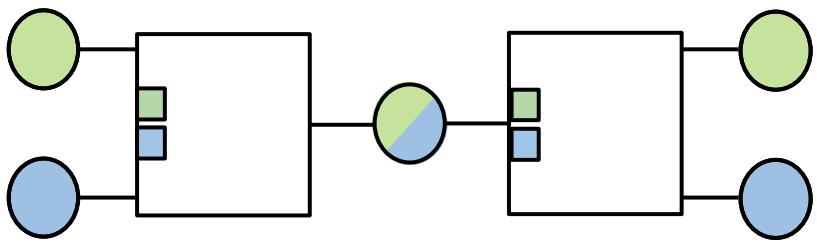
200-800M channels only

… has locked-in funds by both parties

all my bitcoins are locked-in… sad.

Blockchain Space

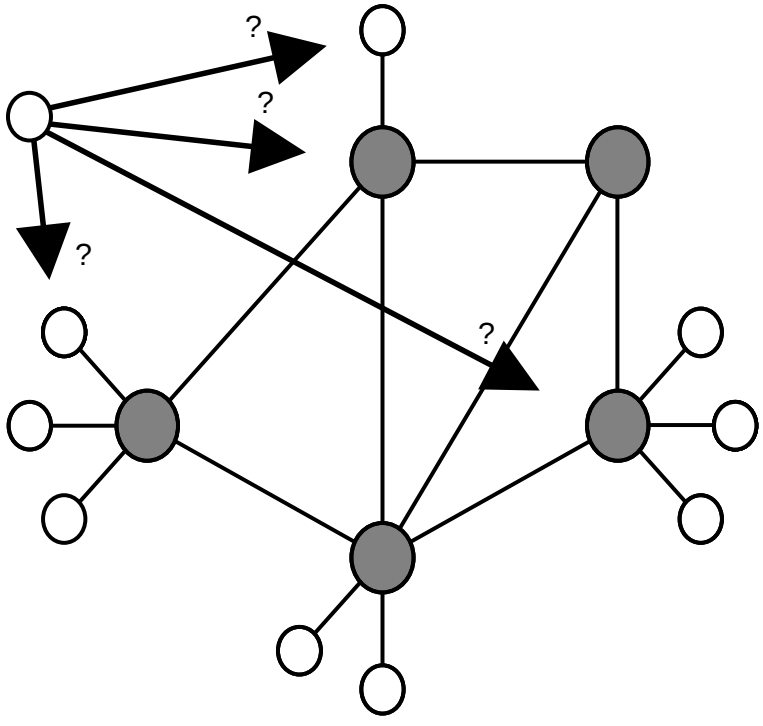
Blockchain Space ~ Number of Signatures



Funding Settlement

so far 4 signatures
for every channel

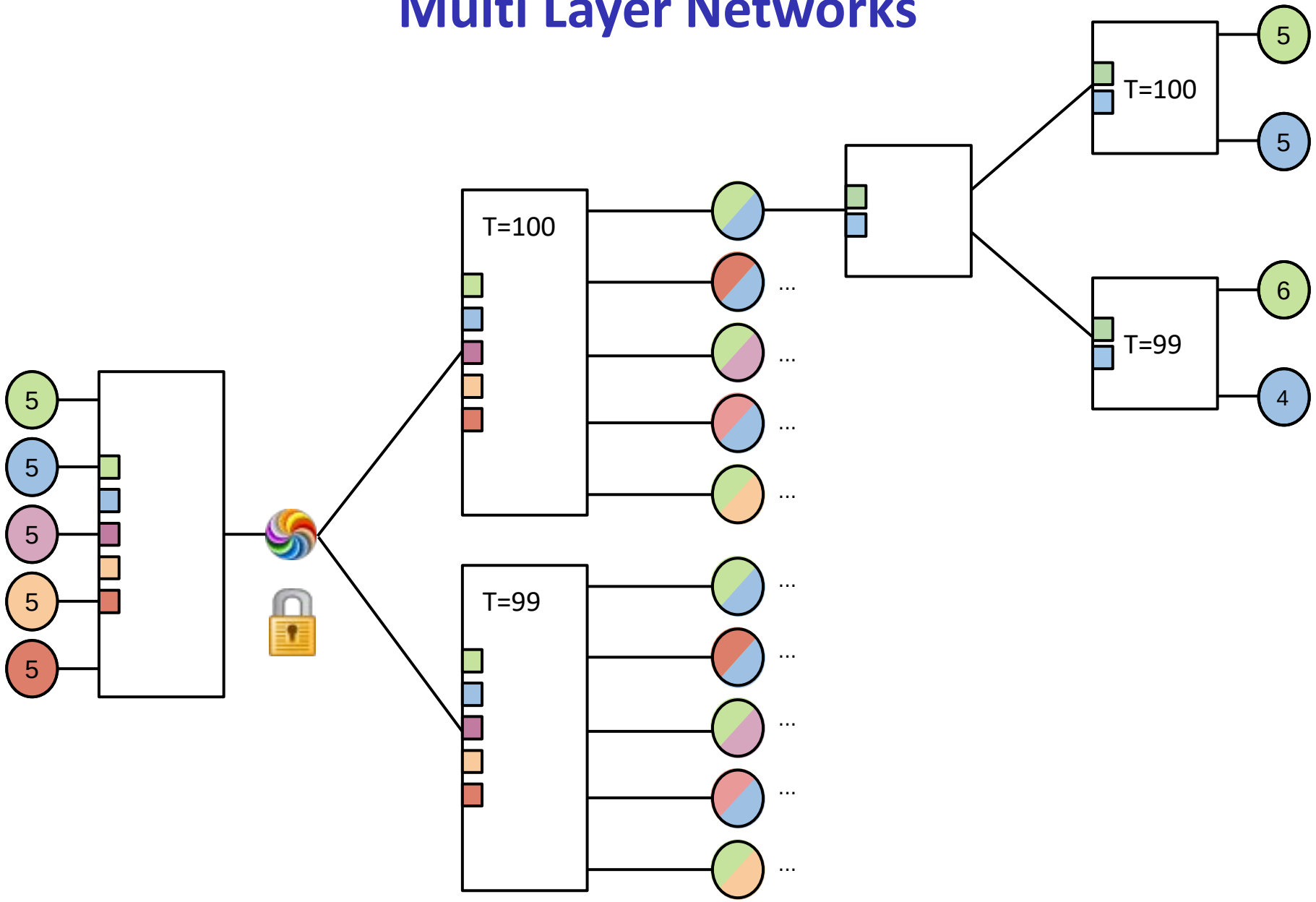
Locked Funds



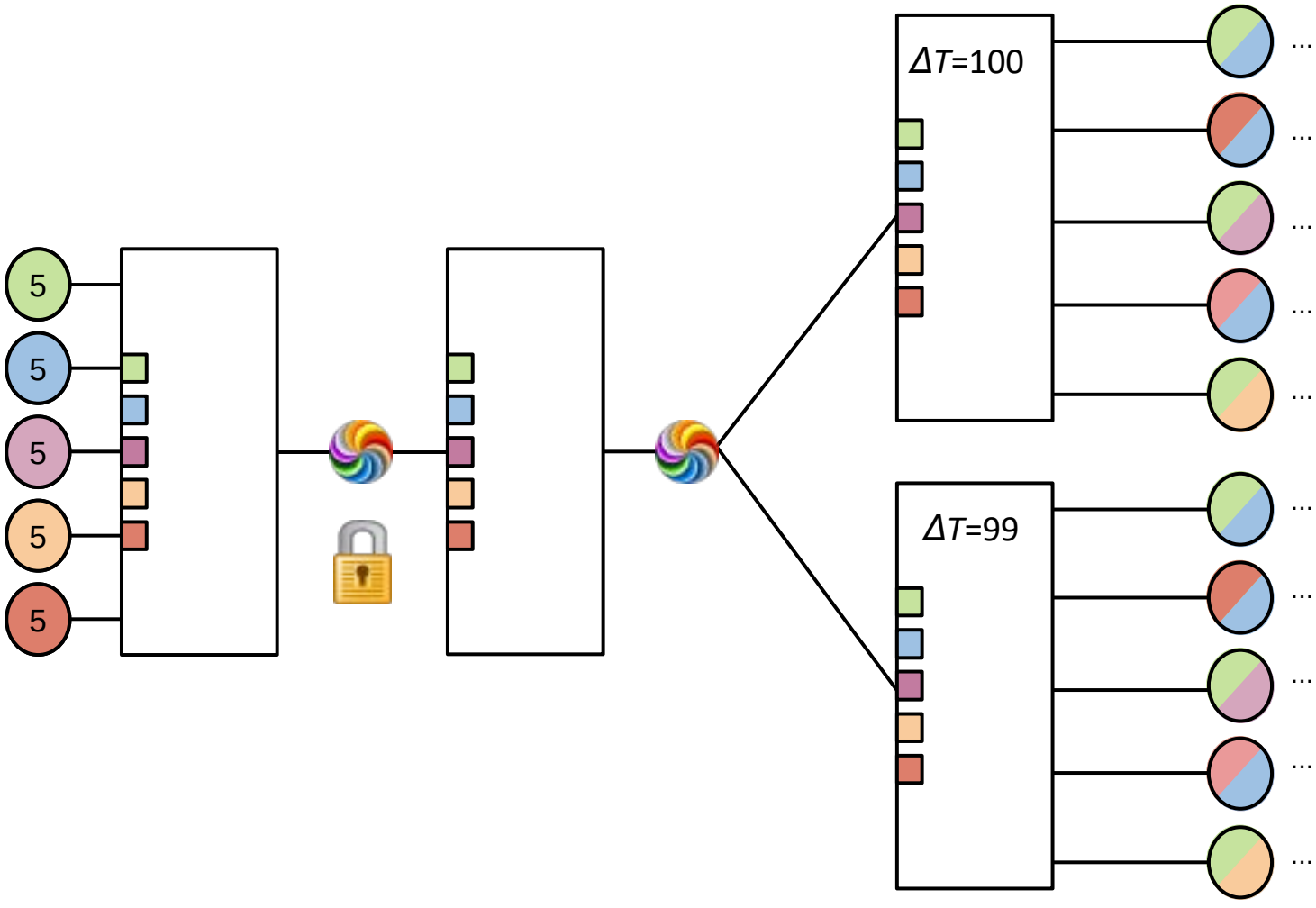
A node wants to make connections…

Where does it lock the funds?

Multi Layer Networks

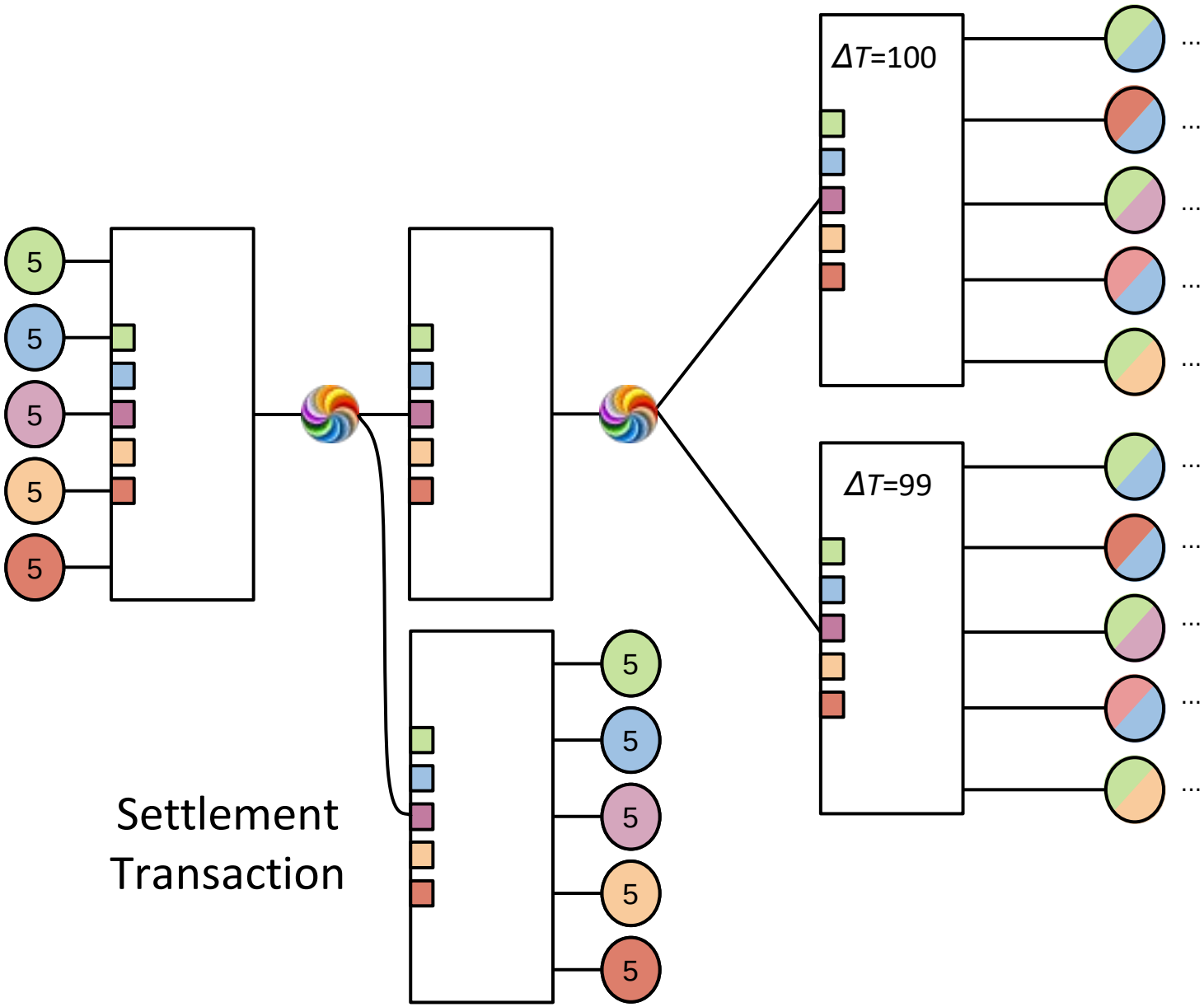


Multi Layer Networks



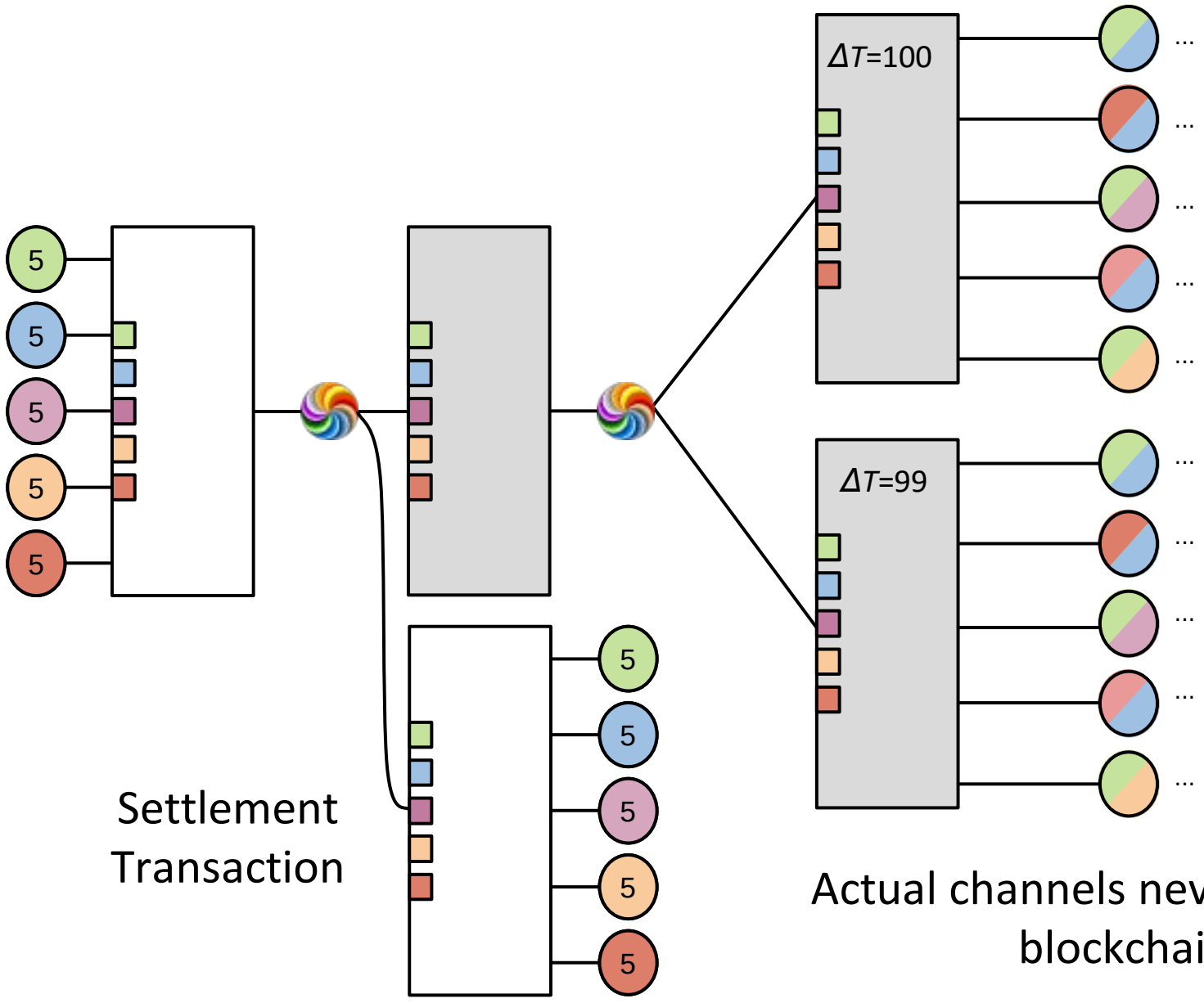
[Burchert, Decker, W 2017]

Multi Layer Networks



[Burchert, Decker, W 2017]

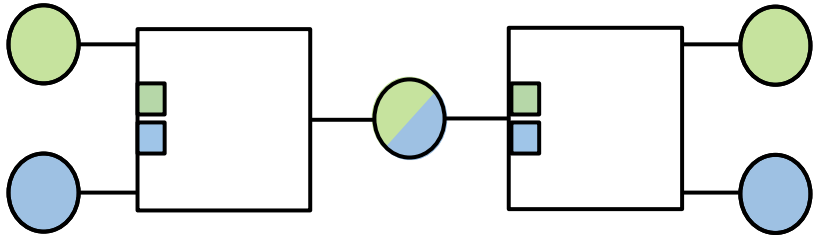
Multi Layer Networks



[Burchert, Decker, W 2017]

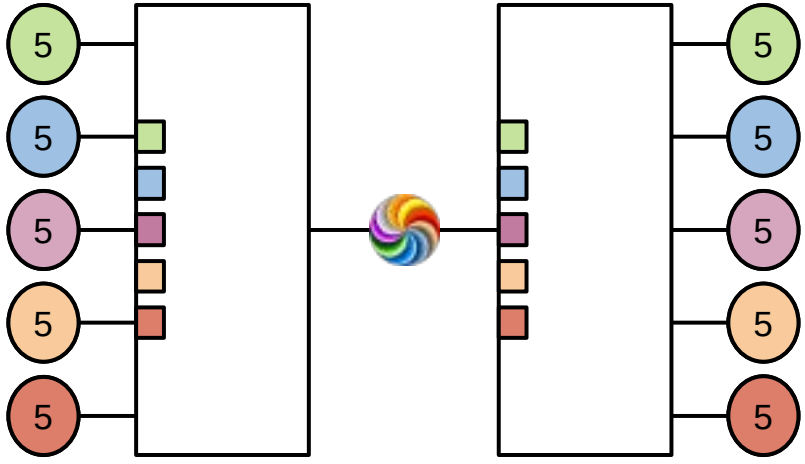
Blockchain Transactions

old



4 signatures per channel

new



2 signatures per user

independent of channels

Are We Finally Done?!?

Yes, unless you have Bitcoin Cash…

Blockchain

Persistence

NIL

Immutable

Provable

Fault-Tolerance

NIL

Crash

Byzantine

Blockchain

Speed

Eventual 

↓

Strong

↓

Immediate 

Throughput

10 tx/s 

↓

10k tx/s 

↓

10m tx/s 

Blockchain

Scalability

10 nodes

100 nodes

1000 nodes

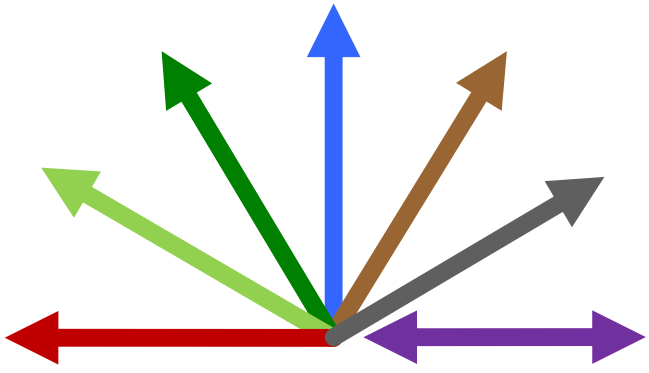
Energy

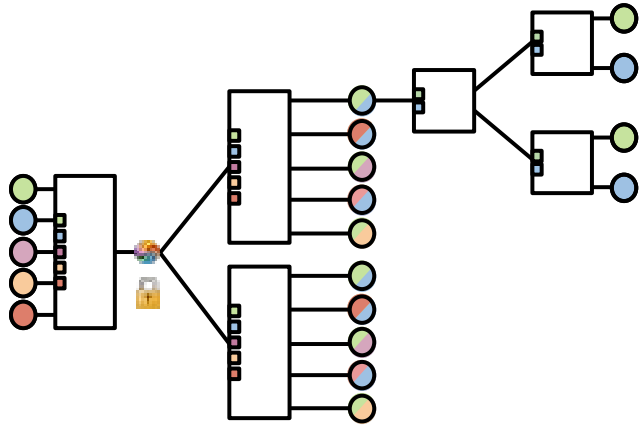
Country

Village

Server Room

Summary






Thank You!
Questions & Comments?
Thanks to my co-authors
Conrad Burchert
Christian Decker
www.disco.ethz.ch