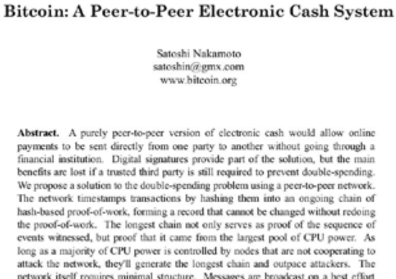
Happy 10th Birthday, Nakamoto!

Roger Wattenhofer

2008



Bitcoin: A Peer-to-Peer Electronic Cash System

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

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort

HAPPY BIRTHDAY
Not Me!

Blockchain: The Biggest Story in Distributed Computing Since …

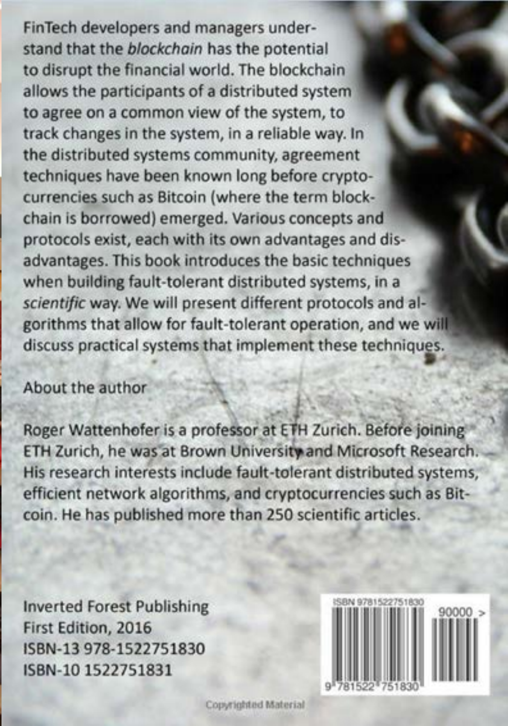
… the Internet?!?

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

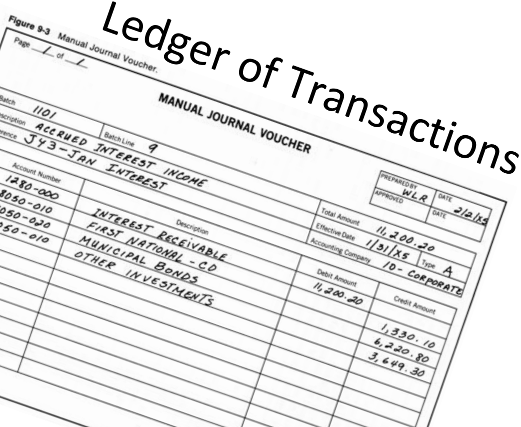


Figure 9-3 Manual Journal Voucher.

Page 1 of 1

MANUAL JOURNAL VOUCHER

Batch 1101

scription ACCRUED INTEREST INCOME

Batch Line 9

erence J43-JAN INTEREST

PREPARED BY WLR DATE 2/12/X5

APPROVED DATE

Total Amount 11,200.20

Effective Date 1/31/X5

Accounting Company 10- CORPORATE

Type A

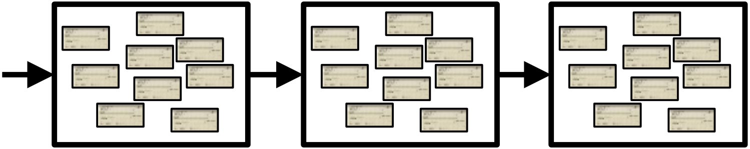
Account Number	Description	Debit Amount	Credit Amount
1280-000	INTEREST RECEIVABLE	11,200.20	
8050-010	FIRST NATIONAL - CD		1,330.10
050-020	MUNICIPAL BONDS		6,220.80
50-010	OTHER INVESTMENTS		3,649.30

Bitcoin

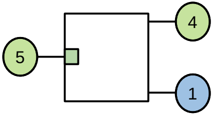
Blockchain

Distributed Systems (1982)	&	Cryptography (1976)

Blockchain



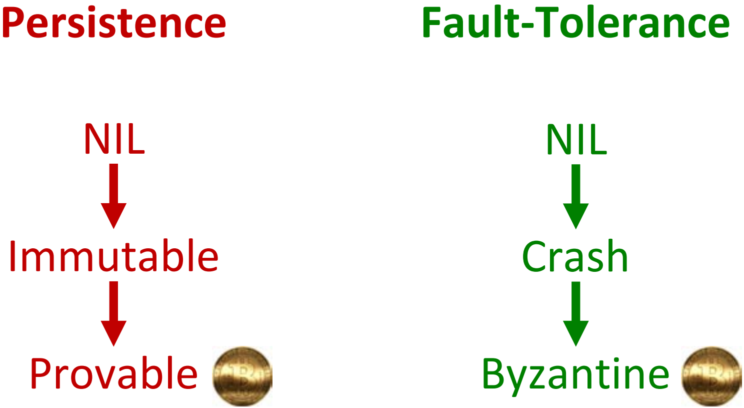
Transaction



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

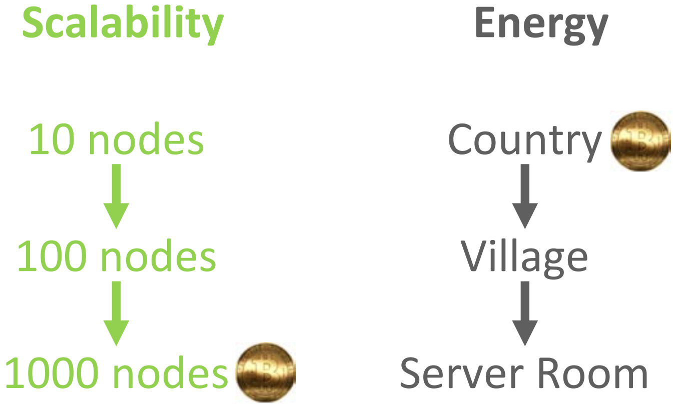
Upper Bound 19 GW

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.

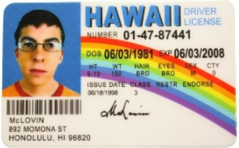
Privacy

ANONYMOUS GLOBAL ID CARD

Name: Anonymous
Address: Anywhere
Occupation: Enturbulator

Country: Global
Exp: Never

ANONYMOUS
DOES NOT FORGIVE



HAWAII DRIVER LICENSE

NUMBER 01-47-87441
DOB 06/03/1981 EXP 06/03/2008
HT 5-10 WT 150 HAIR BRO EYES BRO SEX M CTY 0
ISSUE DATE 06/18/1998 CLASS 3 RESTR ENDORSE

McLOVIN
892 MOMONA ST
HONOLULU, HI 96820

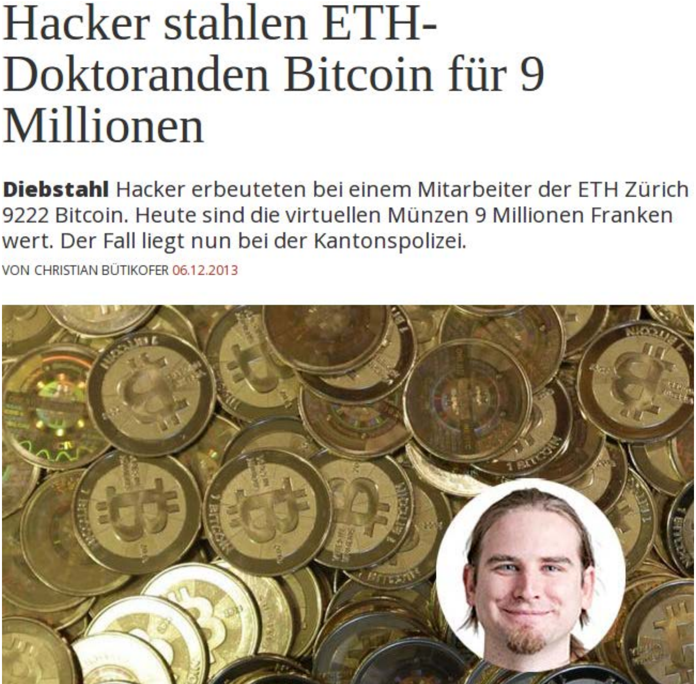
Operator

↕

World

↕

Open PoW

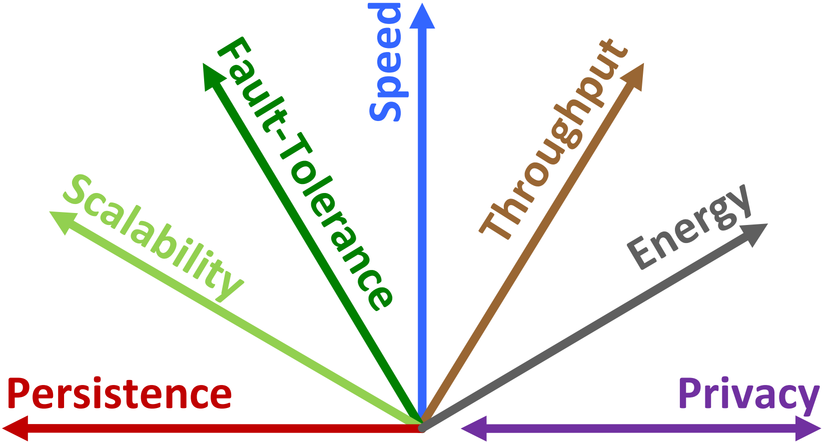


Hacker stahlen ETH-Doktoranden Bitcoin für 9 Millionen

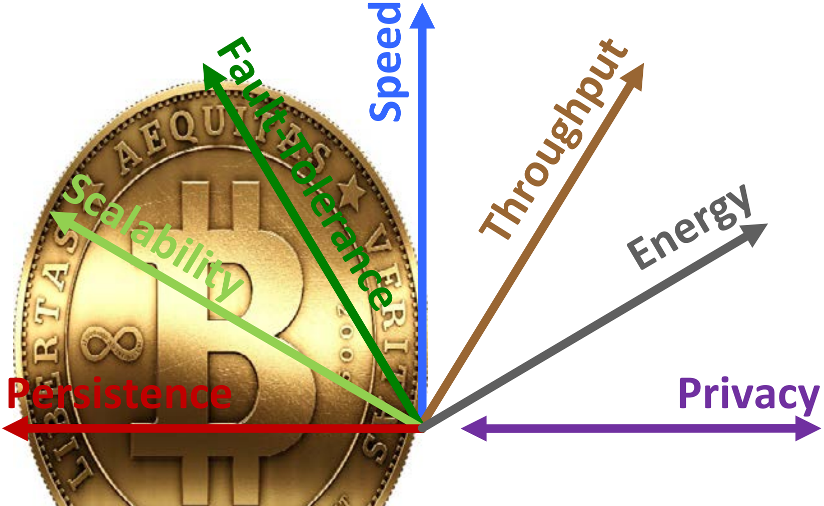
Diebstahl Hacker erbeuteten bei einem Mitarbeiter der ETH Zürich 9222 Bitcoin. Heute sind die virtuellen Münzen 9 Millionen Franken wert. Der Fall liegt nun bei der Kantonspolizei.

VON CHRISTIAN BÜTIKOFER 06.12.2013

The Seven Blockchain Dimensions



The Seven Blockchain Dimensions



Plenty of Research Dimensions

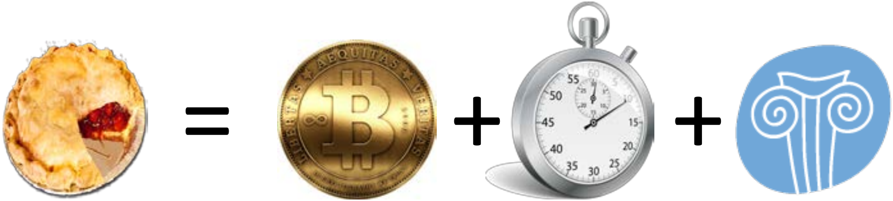
piChain

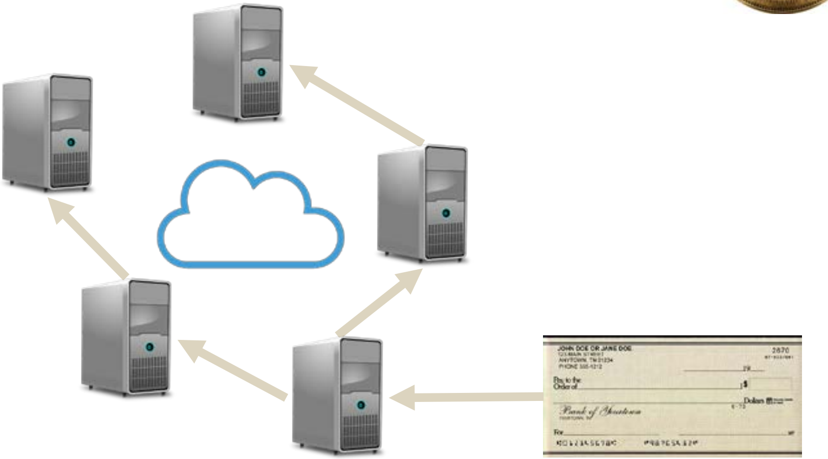
piChain: When a Blockchain Meets Paxos

=

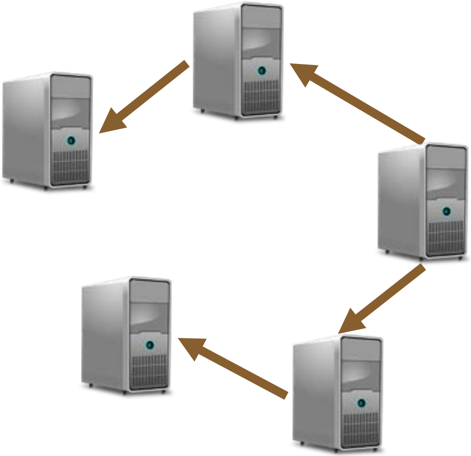
+

piChain: When a Blockchain Meets Paxos

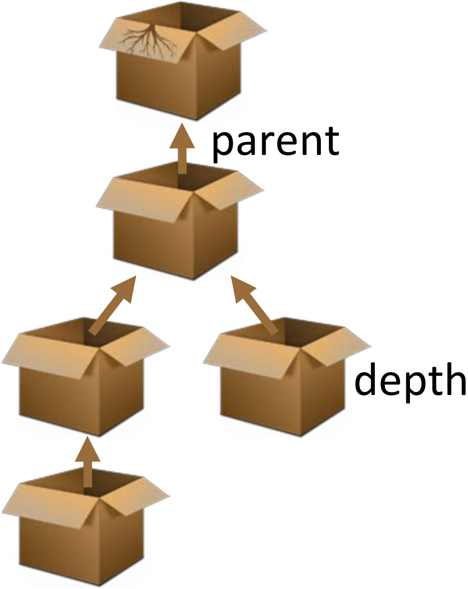




Transaction

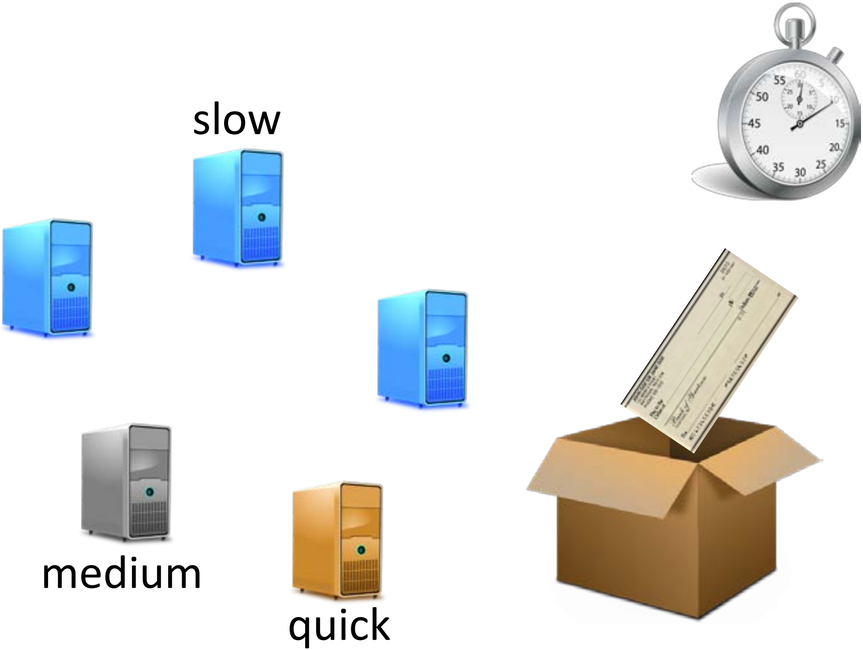


Block



parent

depth

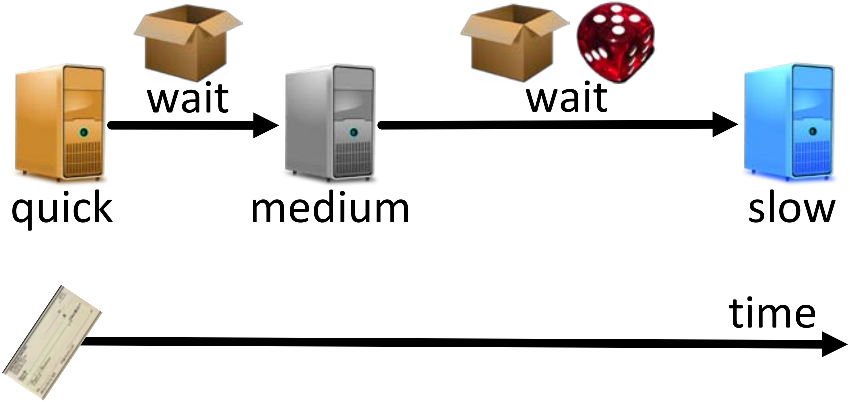


slow

medium

quick

New Transaction: Reaction Time



wait

wait

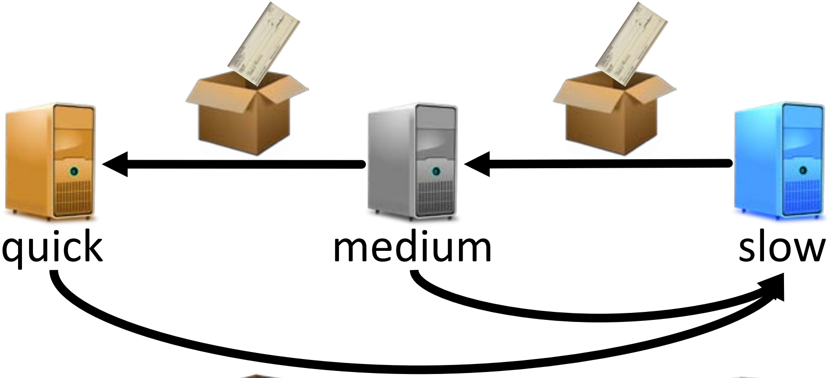
quick

medium

slow

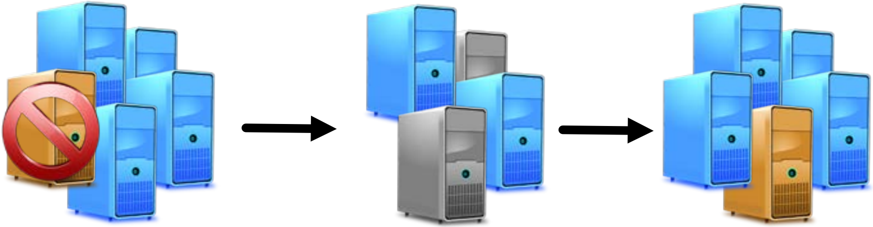
time

State Transitions



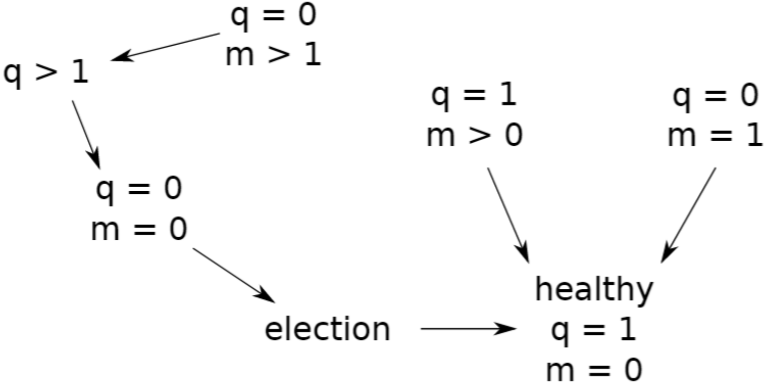
seen 📦: either deeper or by 🖥

Self-Healing



healthy

Self-Healing



$q = 0$
$m > 1$

$q > 1$

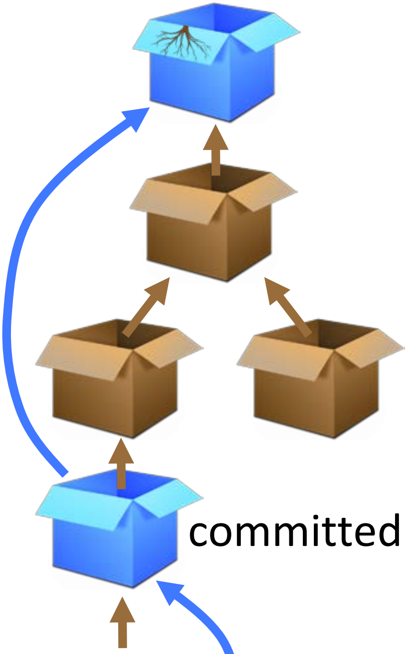
$q = 0$
$m = 0$

election

$q = 1$
$m > 0$

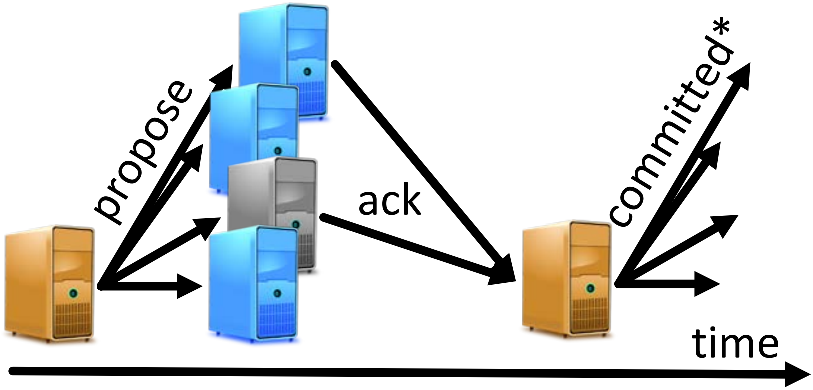
$q = 0$
$m = 1$

healthy
$q = 1$
$m = 0$



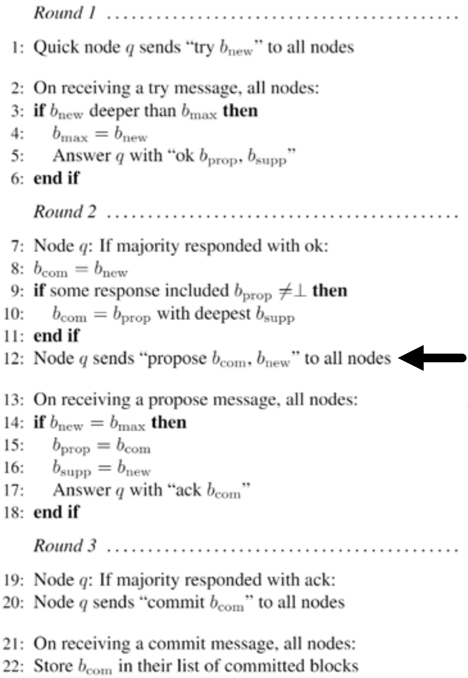
committed

Truncated Paxos



*and next propose

Normal Paxos



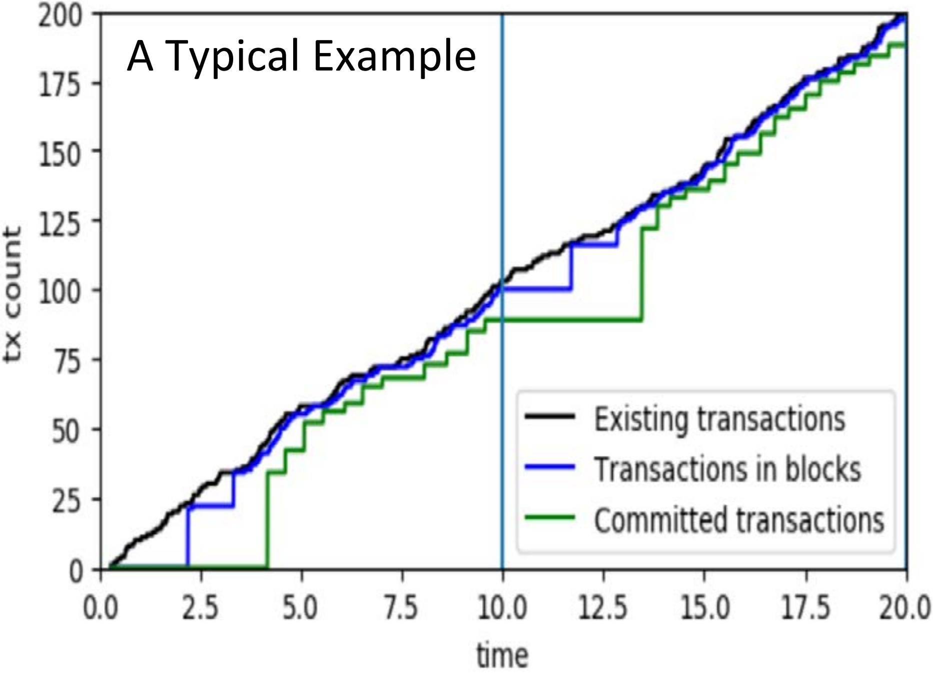
```
Round 1 ........................................
Quick node $q$ sends "try $b_{\text{new}}$" to all nodes

On receiving a try message, all nodes:
if $b_{\text{new}}$ deeper than $b_{\max}$ then
    $b_{\max} = b_{\text{new}}$
    Answer $q$ with "ok $b_{\text{prop}}, b_{\text{supp}}$"
end if
Round 2 ........................................
Node $q$: If majority responded with ok:
$b_{\text{com}} = b_{\text{new}}$
if some response included $b_{\text{prop}} \neq \perp$ then
    $b_{\text{com}} = b_{\text{prop}}$ with deepest $b_{\text{supp}}$
end if
Node $q$ sends "propose $b_{\text{com}}, b_{\text{new}}$" to all nodes

On receiving a propose message, all nodes:
if $b_{\text{new}} = b_{\max}$ then
    $b_{\text{prop}} = b_{\text{com}}$
    $b_{\text{supp}} = b_{\text{new}}$
    Answer $q$ with "ack $b_{\text{com}}$"
end if
Round 3 ........................................
Node $q$: If majority responded with ack:
Node $q$ sends "commit $b_{\text{com}}$" to all nodes

On receiving a commit message, all nodes:
Store $b_{\text{com}}$ in their list of committed blocks
```

A Typical Example



piChain vs. Raft

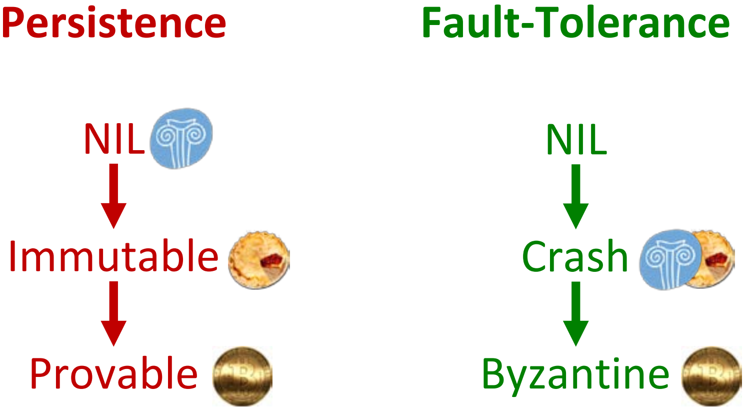
similar essentially same goals

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

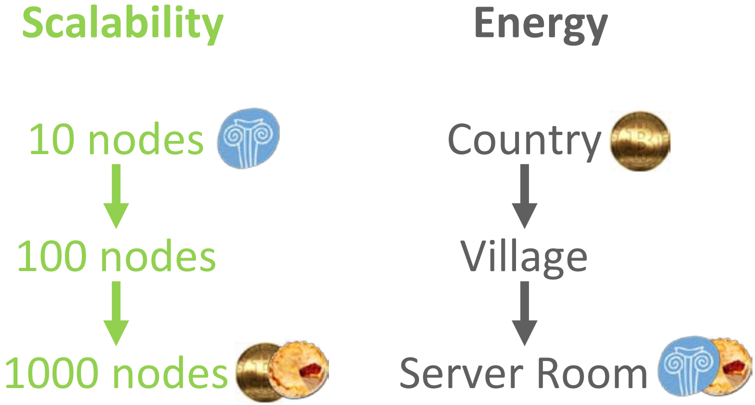
↓

10k tx/s

↓

10m tx/s

Blockchain



Scalability

10 nodes

100 nodes

1000 nodes

Energy

Country

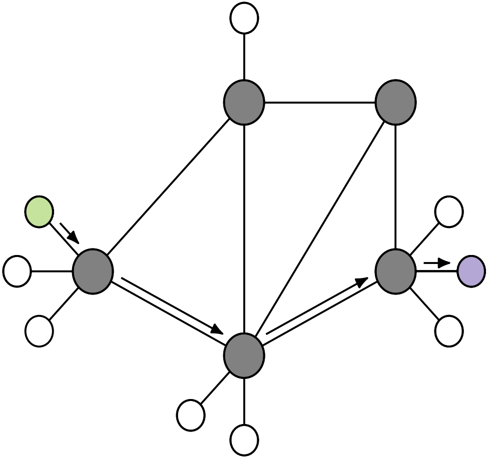
Village

Server Room

Fundamental Problem
Every Node Sees Every Transaction

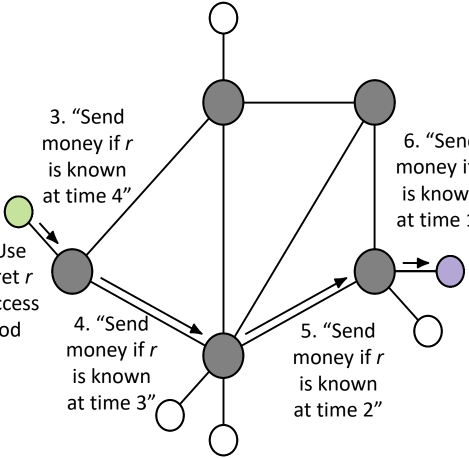
Payment Networks

Payment Network



Hashed Timelocked Contract (HTLC)

HTLC Example (🟣 sells to 🟢)



1. Generate random secret *r*

2. Send hash(*r*) to 🟢

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

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

5. “Send money if *r* is known at time 2”

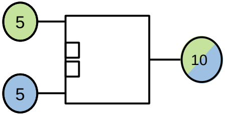
6. “Send money if *r* is known at time 1”

7. Use secret *r* to access good

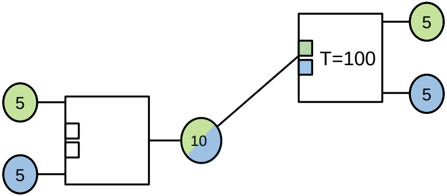
Single Hop in Network

Duplex Micropayment Channels
(Example for Smart Contract)

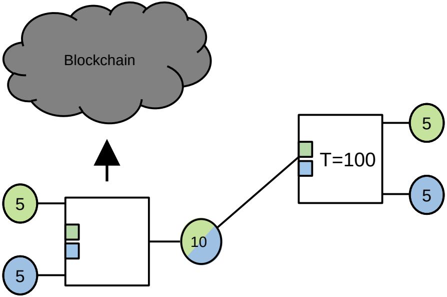
Duplex Micropayment Channel



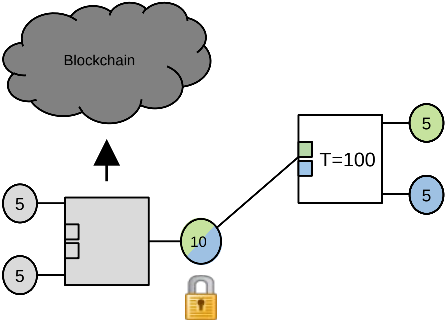
Duplex Micropayment Channel



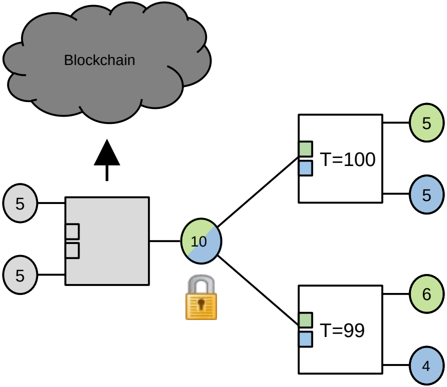
Duplex Micropayment Channel



Duplex Micropayment Channel

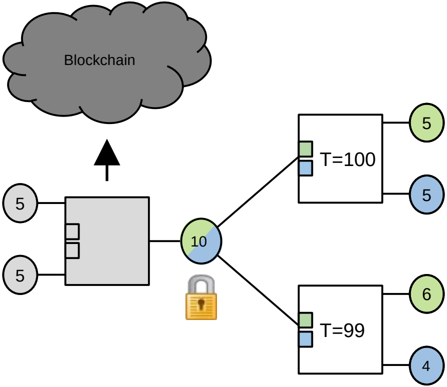


Duplex Micropayment Channel



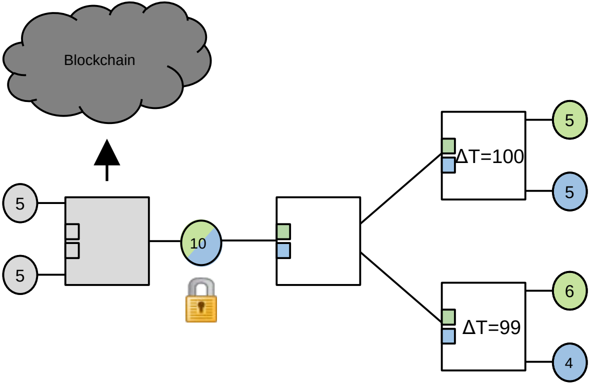
[Decker,W,2015]

Duplex Micropayment Channel



Channel must be renewed often?

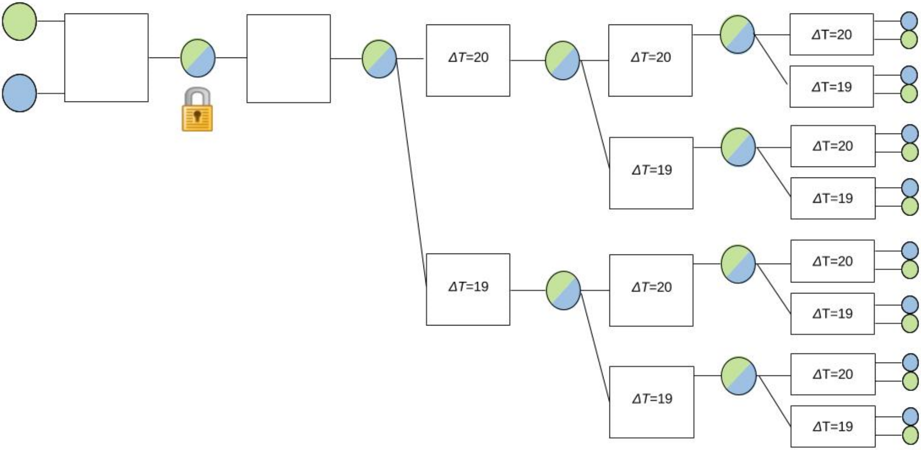
Duplex Micropayment Channel



Relative timelocks to keep channel alive forever!

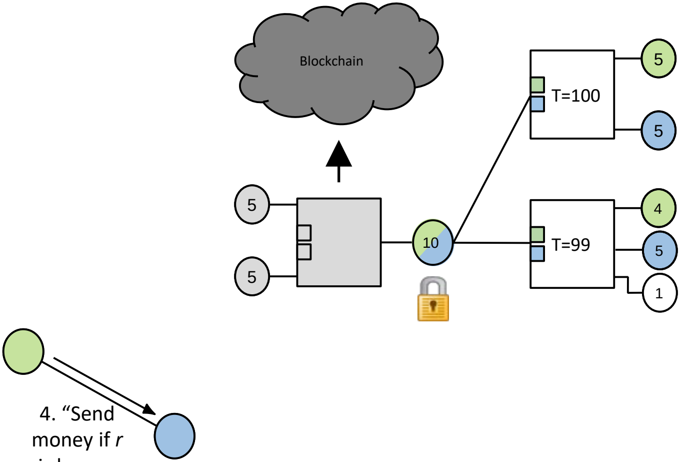
But only 99 transactions?

Duplex Micropayment Channel



[Decker,W,2015]

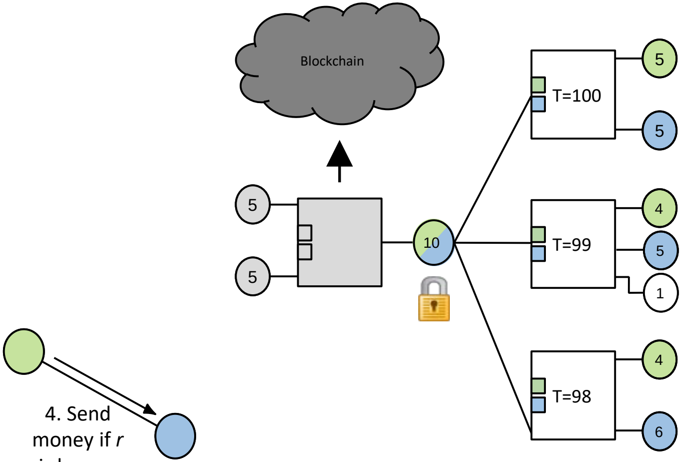
HTLC Revisited



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

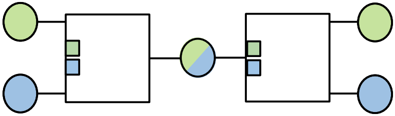
200-800M channels only

… has locked-in funds by both parties

all my bitcoins are locked-in… sad.

Blockchain Space

Blockchain Space ~ Number of Signatures

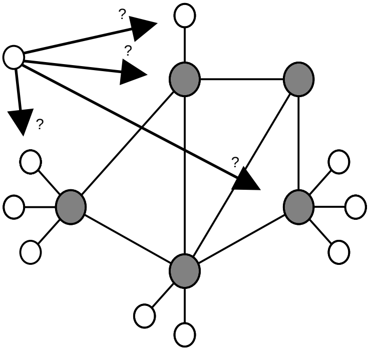


Funding

Settlement

so far 4 signatures
for every channel

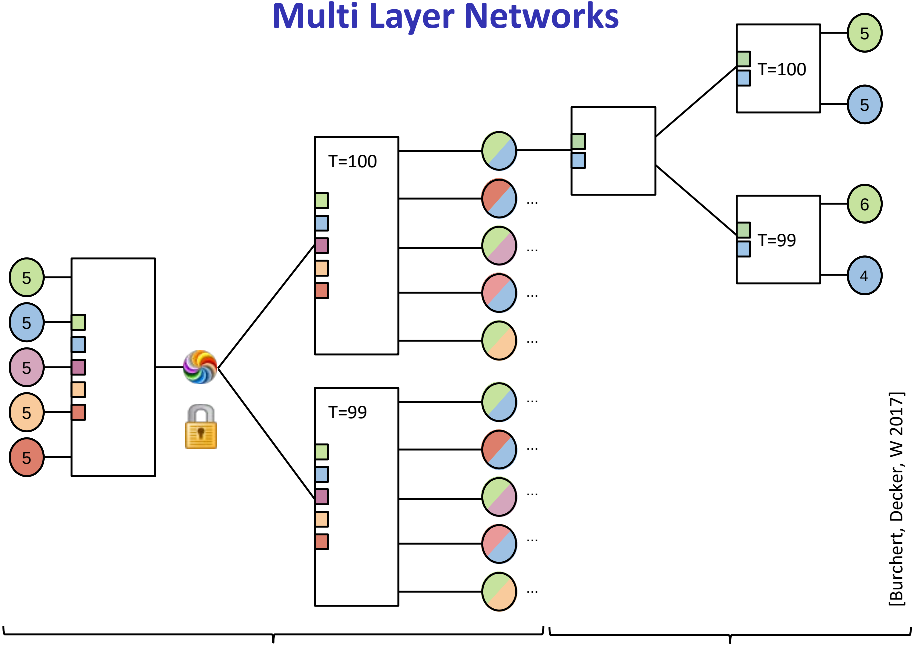
Locked Funds



A node wants to make connections…

Where does it lock the funds?

Multi Layer Networks

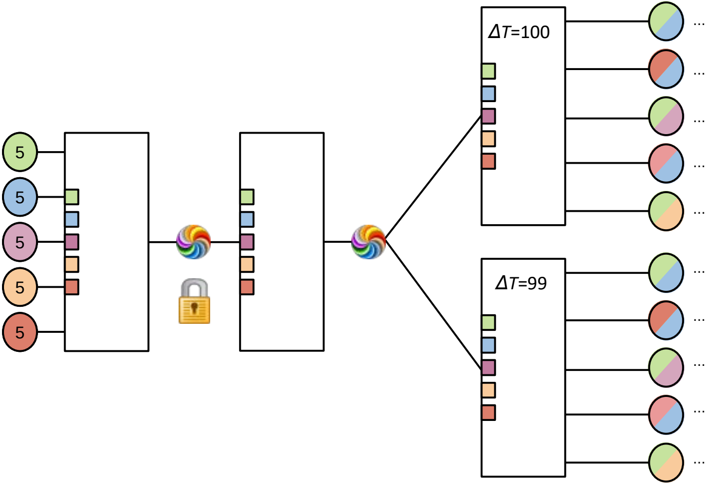


[Burchert, Decker, W 2017]

Channel funding layer

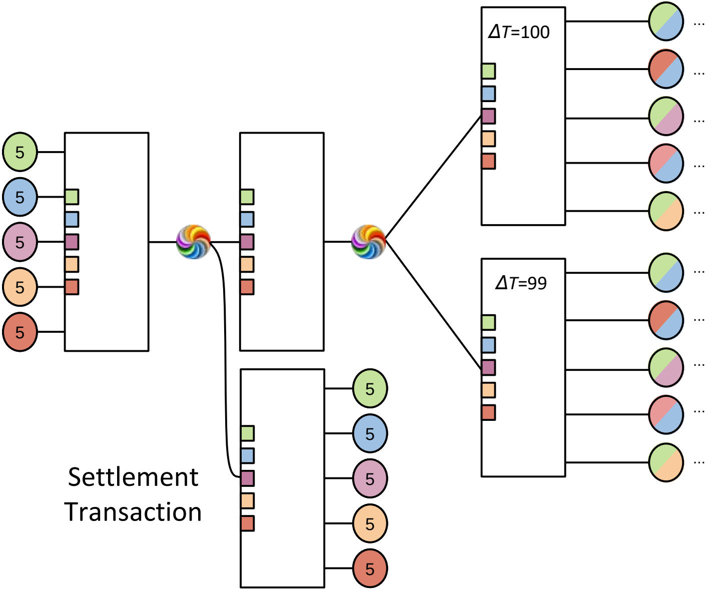
Payment network layer

Multi Layer Networks



[Burchert, Decker, W 2017]

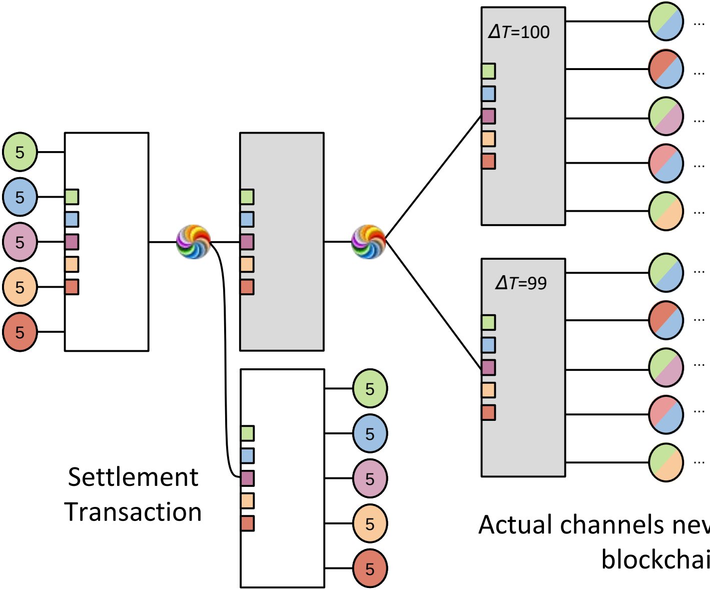
Multi Layer Networks



Settlement Transaction

[Burchert, Decker, W 2017]

Multi Layer Networks



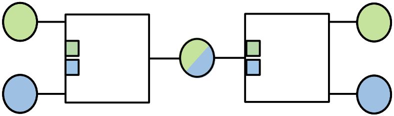
Settlement Transaction

Actual channels never reach the blockchain!

[Burchert, Decker, W 2017]

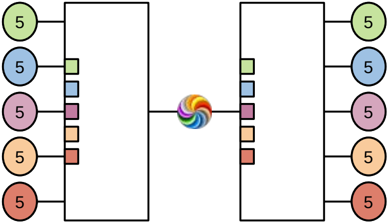
Blockchain Transactions

old



4 signatures per channel

new



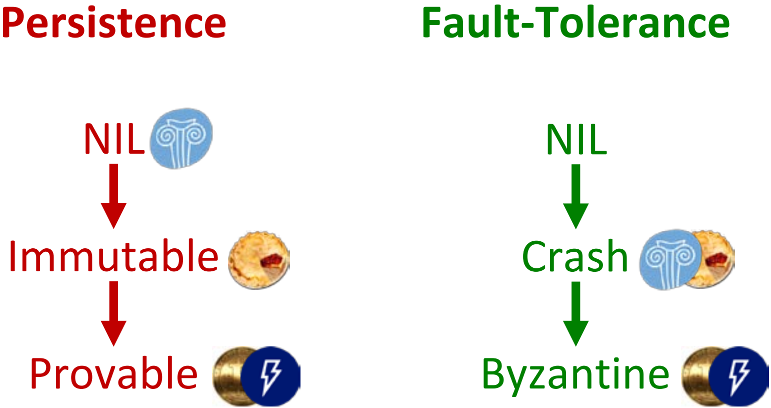
2 signatures per user

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

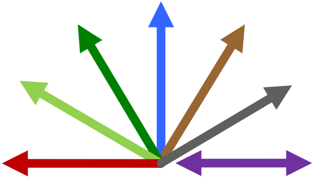
↓

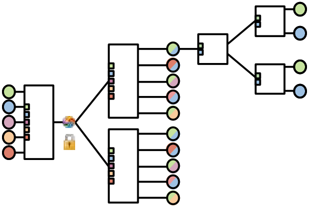
Village

↓

Server Room

Summary





Thank You!

Questions & Comments?

Thanks to my co-authors
Conrad Burchert
Christian Decker

www.disco.ethz.ch