An Efficient Blockchain?

Roger Wattenhofer

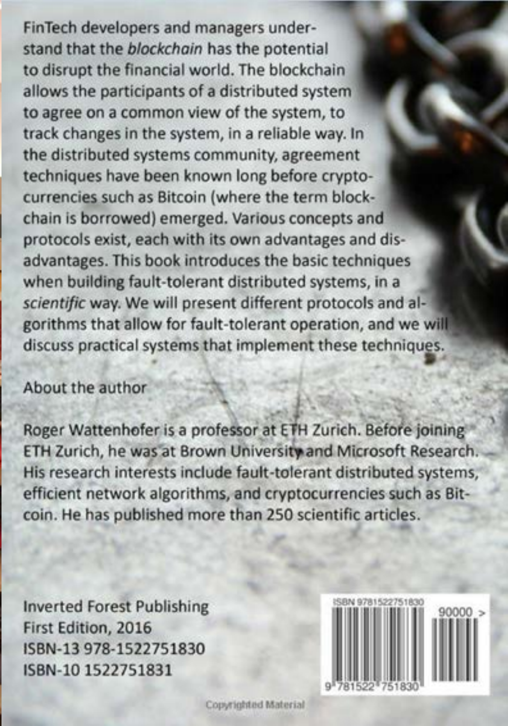
International Workshop on
Cryptocurrencies and Blockchain Technology - CBT'17

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?

What Do You Think?

Ledger of Transactions

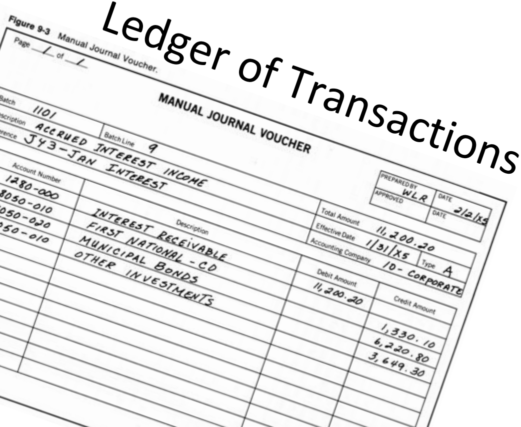


Figure 9-3 Manual Journal Voucher.

Page 1 of 1

MANUAL JOURNAL VOUCHER

Batch	1101
Batch Line	9
escription	ACCRUED INTEREST INCOME
erence	J43-JAN INTEREST
PREPARED BY	WLR
DATE	2/2/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
050-010	OTHER INVESTMENTS		3,649.30

Bitcoin

My Usual Answer

Blockchain

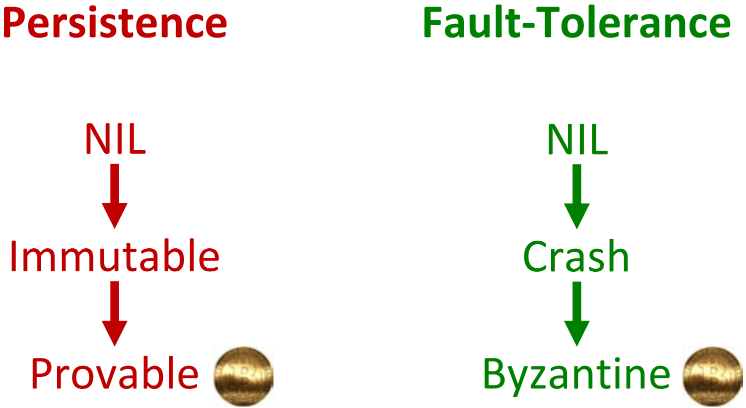
Distributed Systems & Cryptography

(1982) (1976)

Why the Hype?

Let’s Dig Deeper!

Blockchain



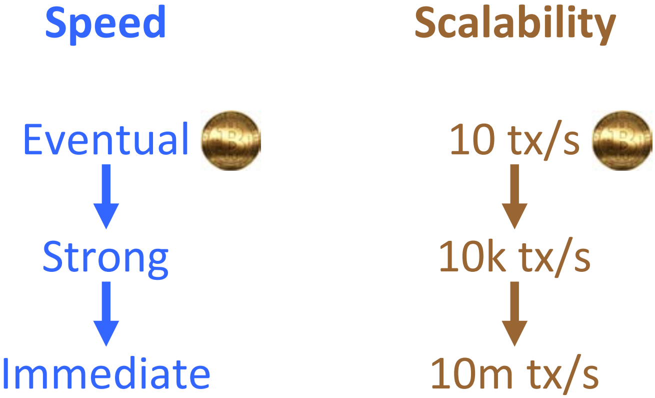
Persistence

NIL ↓ Immutable ↓ Provable

Fault-Tolerance

NIL ↓ Crash ↓ Byzantine

Blockchain



Speed

Eventual

Strong

Immediate

Scalability

10 tx/s

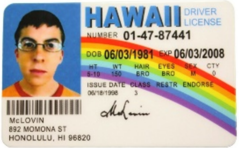
10k tx/s

10m tx/s

What About Privacy?

It’s Complicated.

Privacy



Operator

↕

World

↕

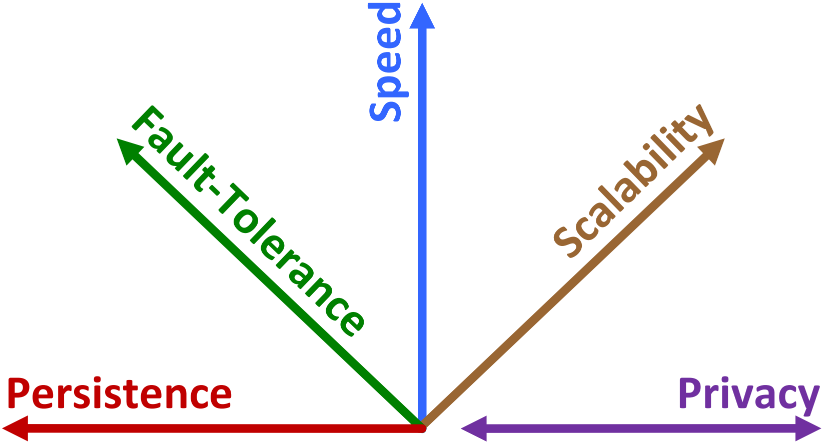
Open PoW

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

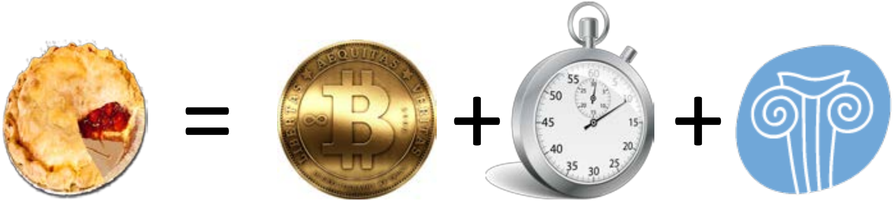
The Five Blockchain Dimensions

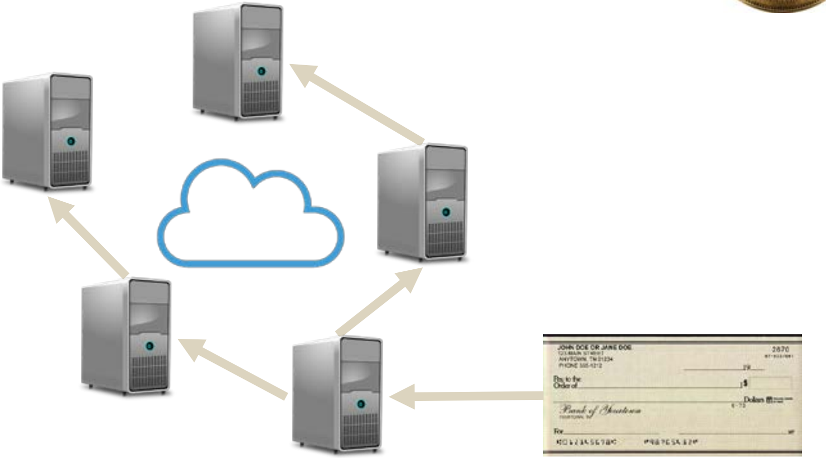


piChain

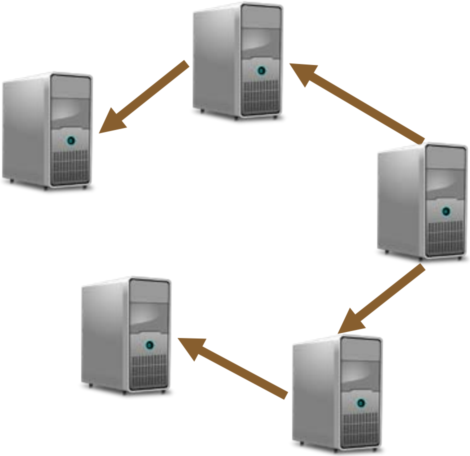
piChain: When a Blockchain Meets Paxos

piChain: When a Blockchain Meets Paxos

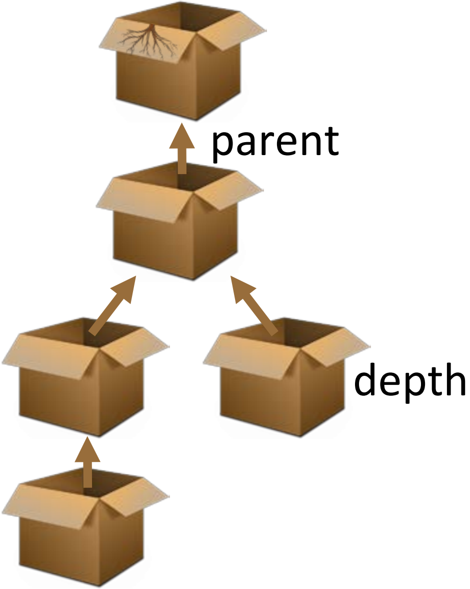


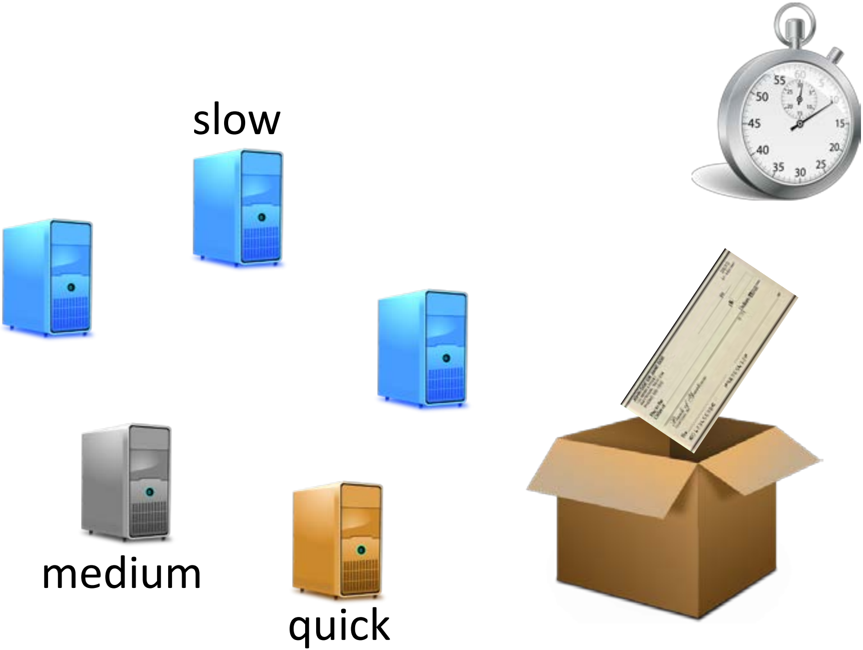


Transaction



Block


parent
depth

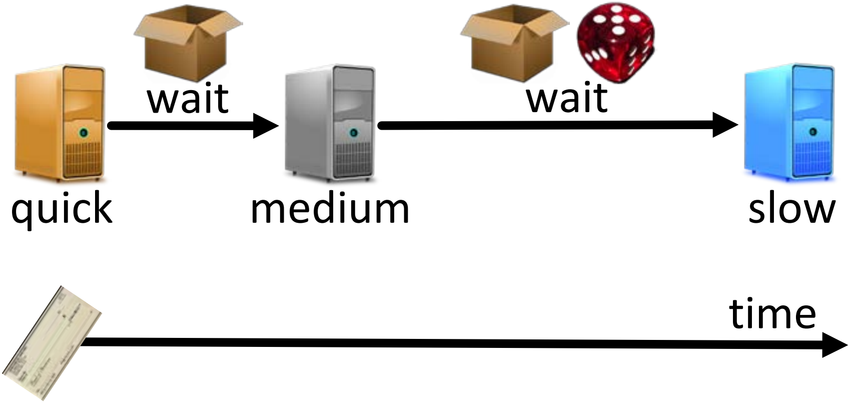


slow

medium

quick

New Transaction: Reaction Time



wait

wait

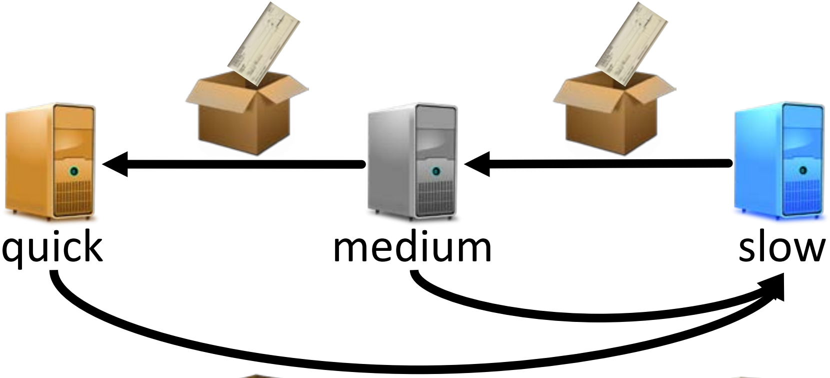
quick

medium

slow

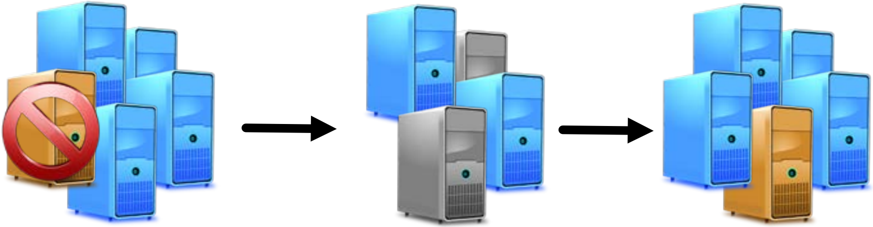
time

State Transitions



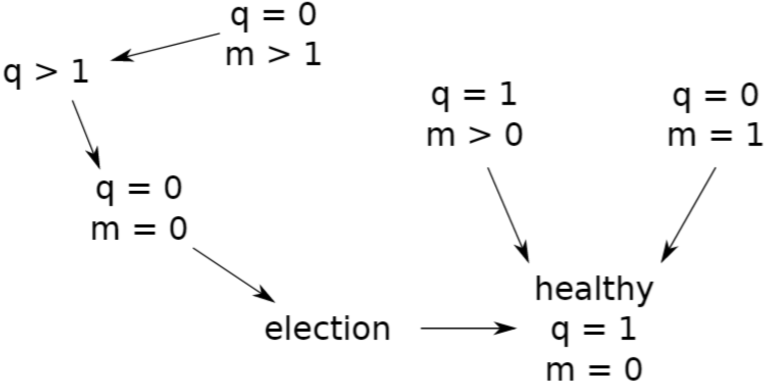
seen 📦: either deeper or by 🖥

Self-Healing



healthy

Self-Healing



q = 0
m > 1

q > 1

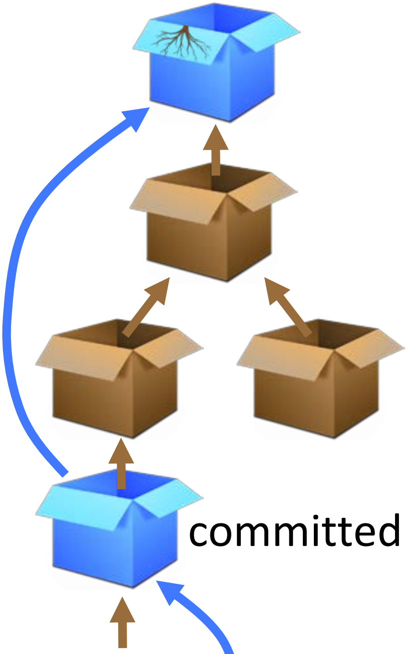
q = 0
m = 0

election

q = 1
m > 0

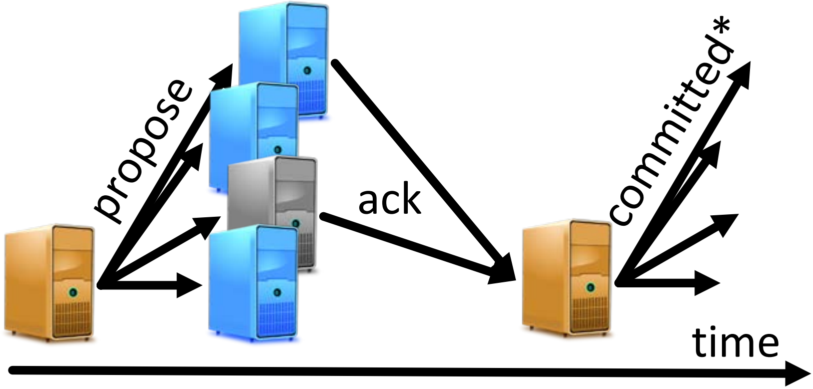
q = 0
m = 1

healthy
q = 1
m = 0



committed

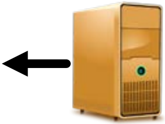
Truncated Paxos



*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 $b_{\text{max}}$ then
    $b_{\text{max}} = b_{\text{new}}$
    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 $b_{\text{new}} = b_{\text{max}}$ 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
```



piChain vs. Raft

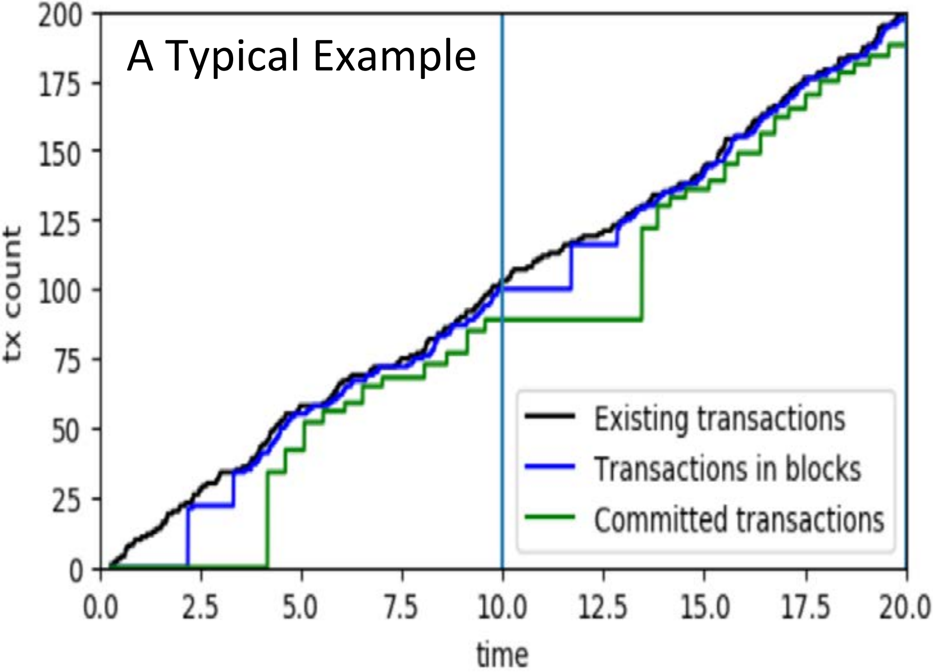
similar essentially same goals

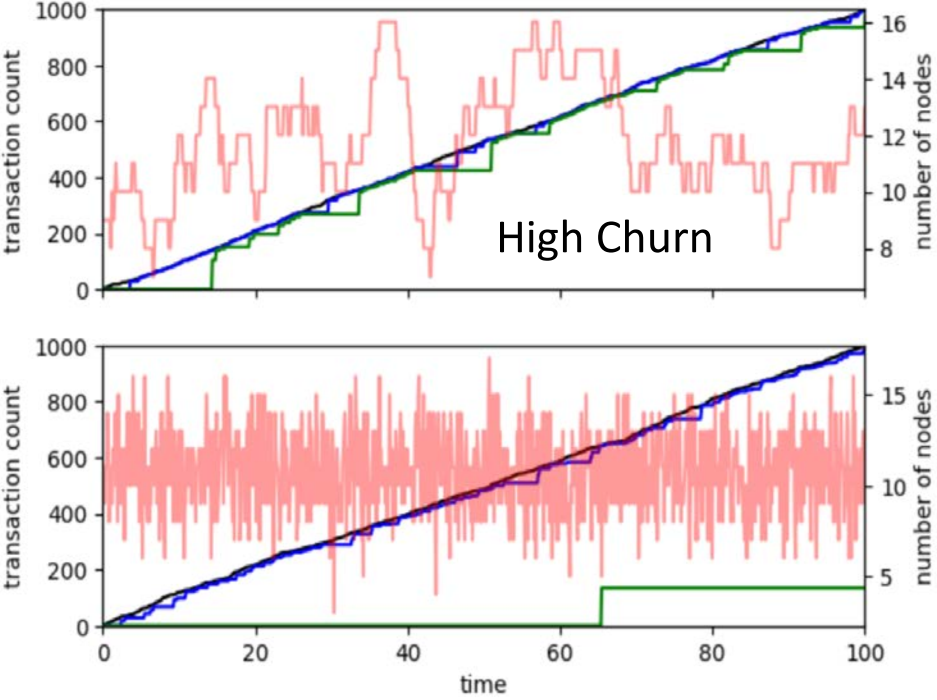
simple e.g., no explicit leader election

silent no msg when no tx, no heartbeat

scalable O(1) msgs per node per tx

A Typical Example

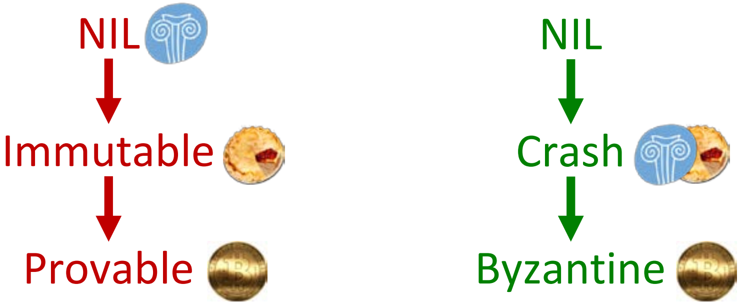




1000
800
600
400
200
0
transaction count
16
14
12
10
8
number of nodes
High Churn
1000
800
600
400
200
0
transaction count
15
10
5
number of nodes
0
20
40
60
80
100
time

Blockchain

Persistence **Fault-Tolerance**



NIL

Immutable

Provable

NIL

Crash

Byzantine

Blockchain

Speed

Eventual

↓

Strong

↓

Immediate

Scalability

10 tx/s

↓

10k tx/s

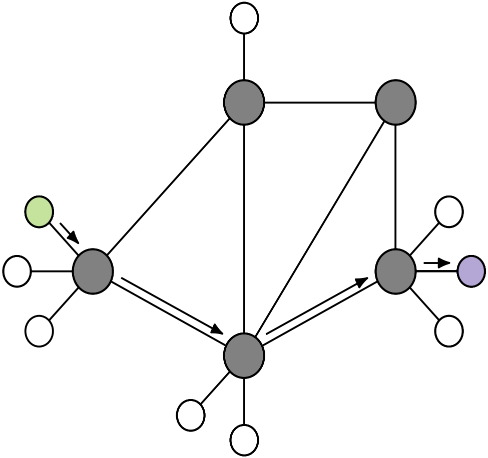
↓

10m tx/s

Fundamental Problem
Every Node Sees Every Transaction

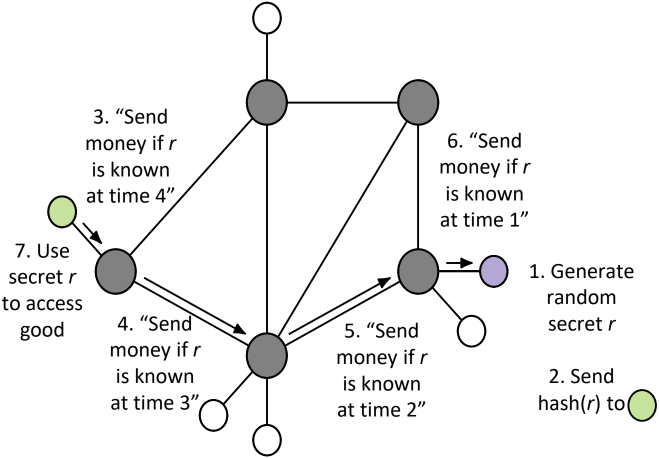
Payment Networks

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”

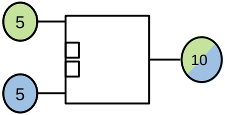
6. “Send money if *r* is known at time 1”

7. Use secret *r* to access good

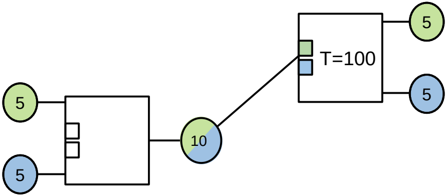
Single Hop in Network

Duplex Micropayment Channels
(Example for Smart Contract)

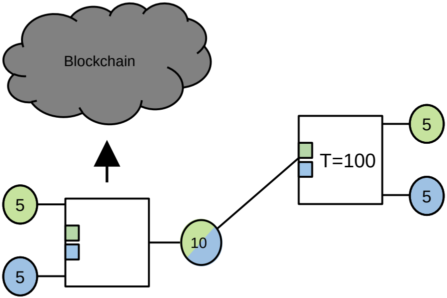
Duplex Micropayment Channel



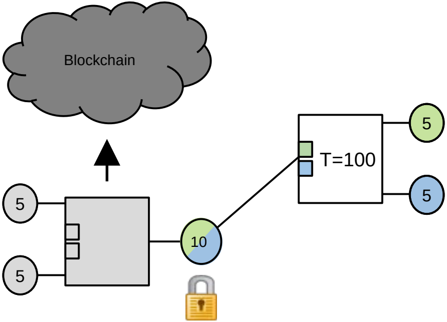
Duplex Micropayment Channel



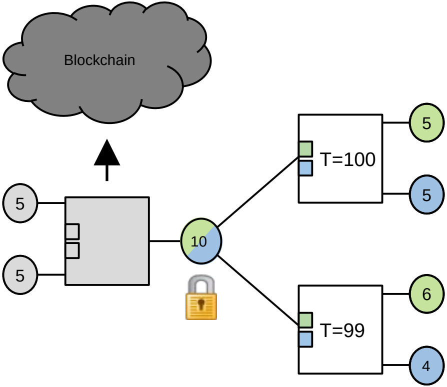
Duplex Micropayment Channel



Duplex Micropayment Channel

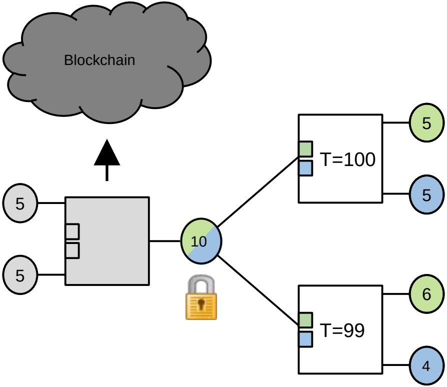


Duplex Micropayment Channel



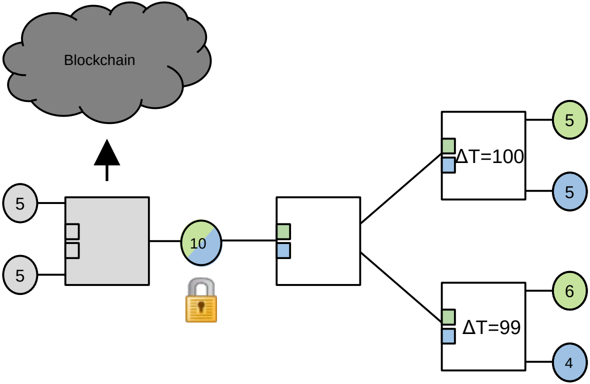
[Decker,W,2015]

Duplex Micropayment Channel



Channel must be renewed often?

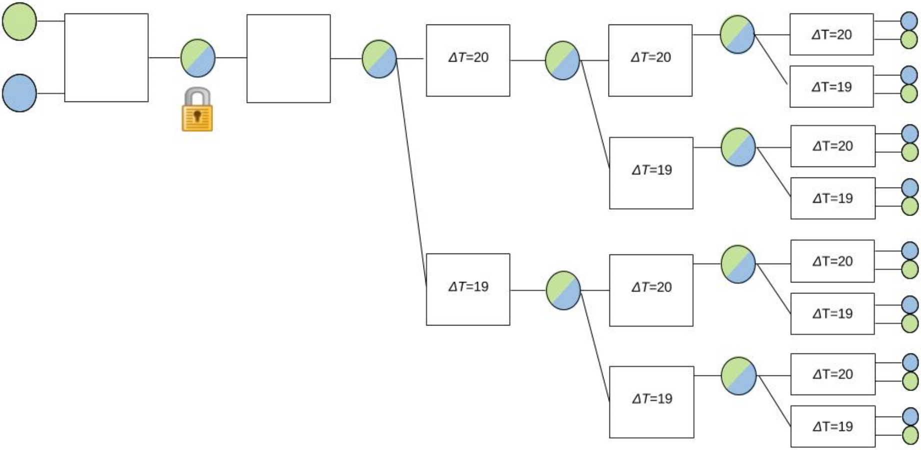
Duplex Micropayment Channel



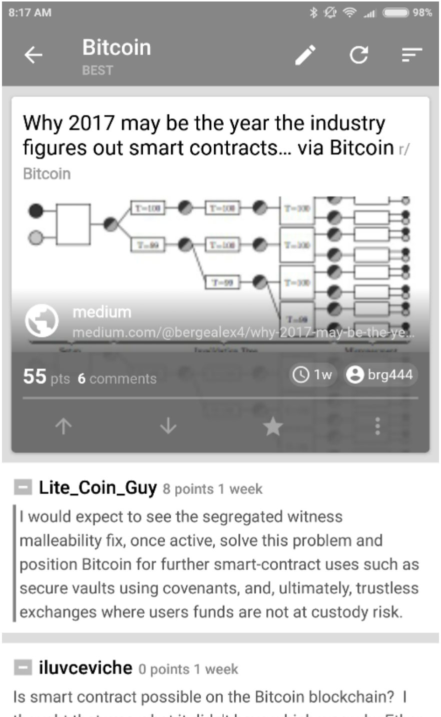
Relative timelocks to keep channel alive forever!

But only 99 transactions?

Duplex Micropayment Channel



[Decker,W,2015]



8:17 AM 98%

Bitcoin
BEST

Why 2017 may be the year the industry figures out smart contracts… via Bitcoin r/Bitcoin

medium
medium.com/@bergealex4/why-2017-may-be-the-ye...

55 pts 6 comments 1w brg444

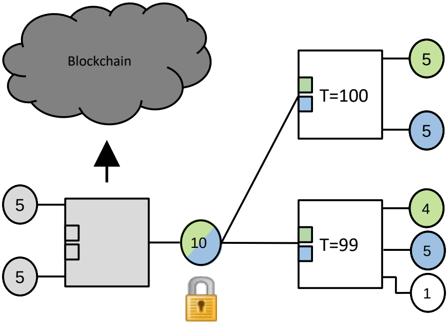
Lite_Coin_Guy 8 points 1 week

I would expect to see the segregated witness malleability fix, once active, solve this problem and position Bitcoin for further smart-contract uses such as secure vaults using covenants, and, ultimately, trustless exchanges where users funds are not at custody risk.

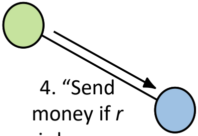
iluvceviche 0 points 1 week

Is smart contract possible on the Bitcoin blockchain? I

HTLC Revisited

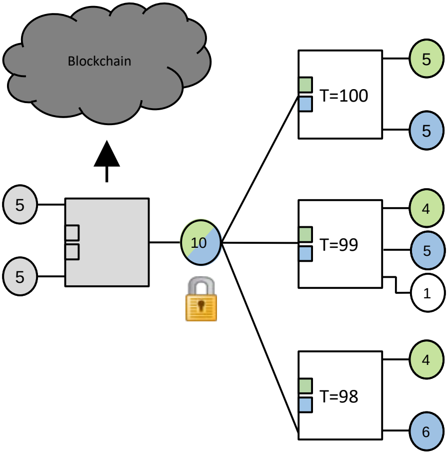


can be spent
by blue with secret *r* or
by green after 3 days

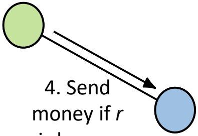


4. “Send
money if *r*
is known
at time 3”

HTLC Revisited



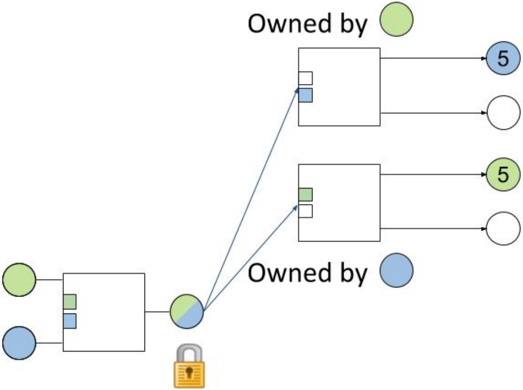
can be spent
by blue with secret *r* or
by green after 3 days



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

Lightning Network

Lightning Network Channel



Owned by 🟢

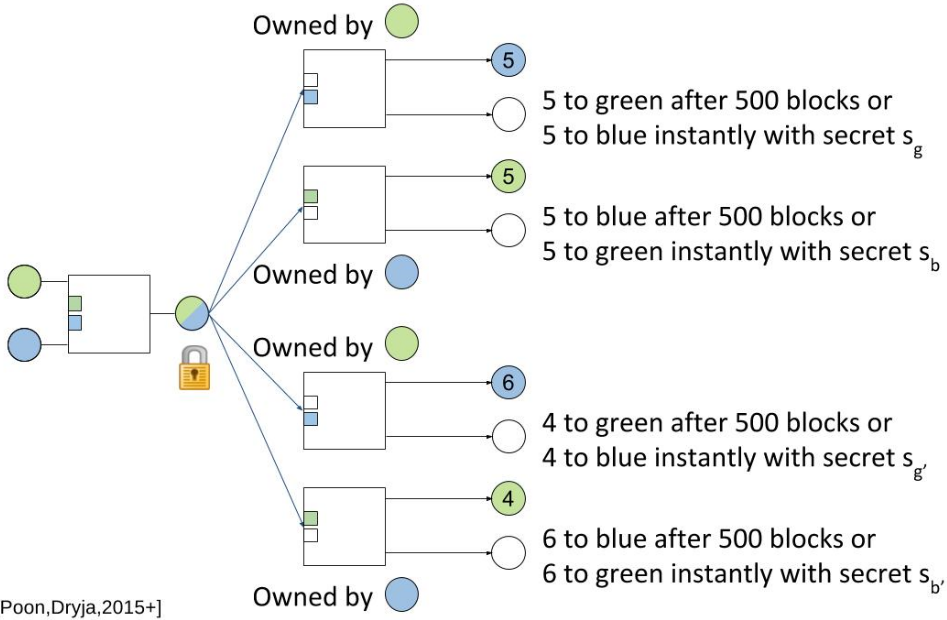
5 to green after 500 blocks or
5 to blue instantly with secret s_g

5 to blue after 500 blocks or
5 to green instantly with secret s_b

Owned by 🔵

[Poon,Dryja,2015+]

Lightning Network Channel



Owned by

5 to green after 500 blocks or
5 to blue instantly with secret s_g

5 to blue after 500 blocks or
5 to green instantly with secret s_b

Owned by

Owned by

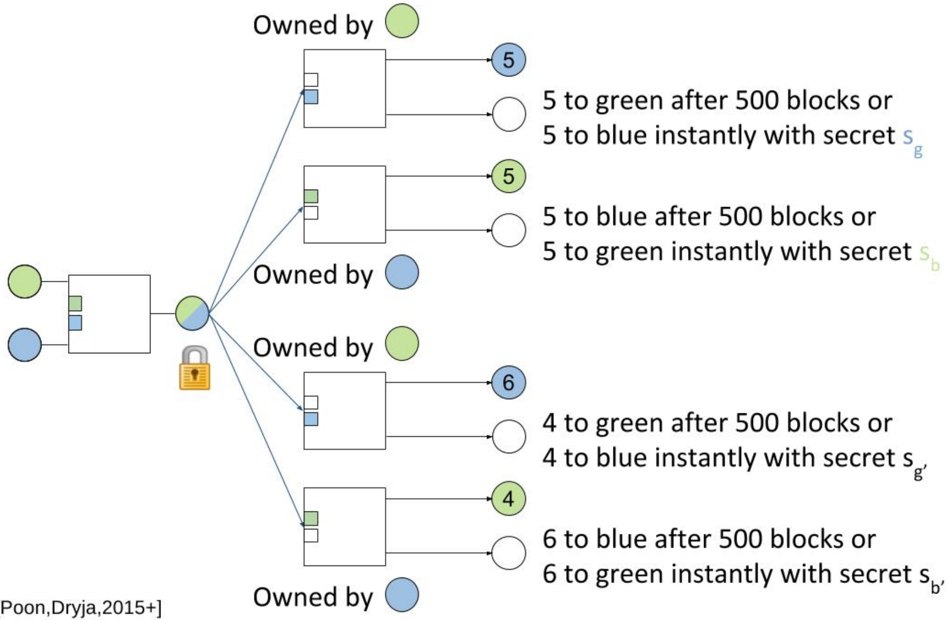
4 to green after 500 blocks or
4 to blue instantly with secret $s_{g'}$

6 to blue after 500 blocks or
6 to green instantly with secret $s_{b'}$

Owned by

[Poon,Dryja,2015+]

Lightning Network Channel



5 to green after 500 blocks or
5 to blue instantly with secret s_g

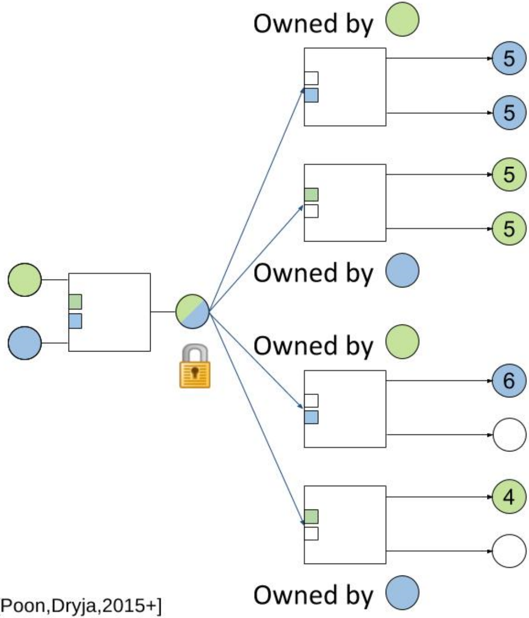
5 to blue after 500 blocks or
5 to green instantly with secret s_b

4 to green after 500 blocks or
4 to blue instantly with secret $s_{g'}$

6 to blue after 500 blocks or
6 to green instantly with secret $s_{b'}$

[Poon,Dryja,2015+]

Lightning Network Channel



4 to green after 500 blocks or
4 to blue instantly with secret $s_{g'}$

6 to blue after 500 blocks or
6 to green instantly with secret $s_{b'}$

[Poon,Dryja,2015+]

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

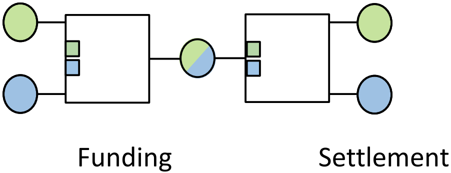
200-800M channels only

… has locked-in funds by both parties

all my bitcoins are locked-in… sad.

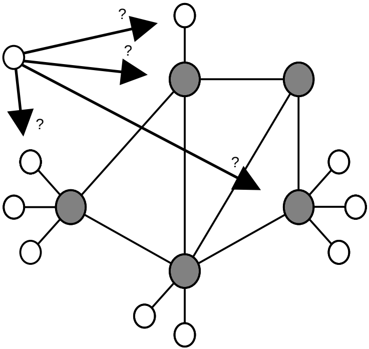
Blockchain Space

Blockchain space ≅ number of signatures



so far 4 signatures
for every channel

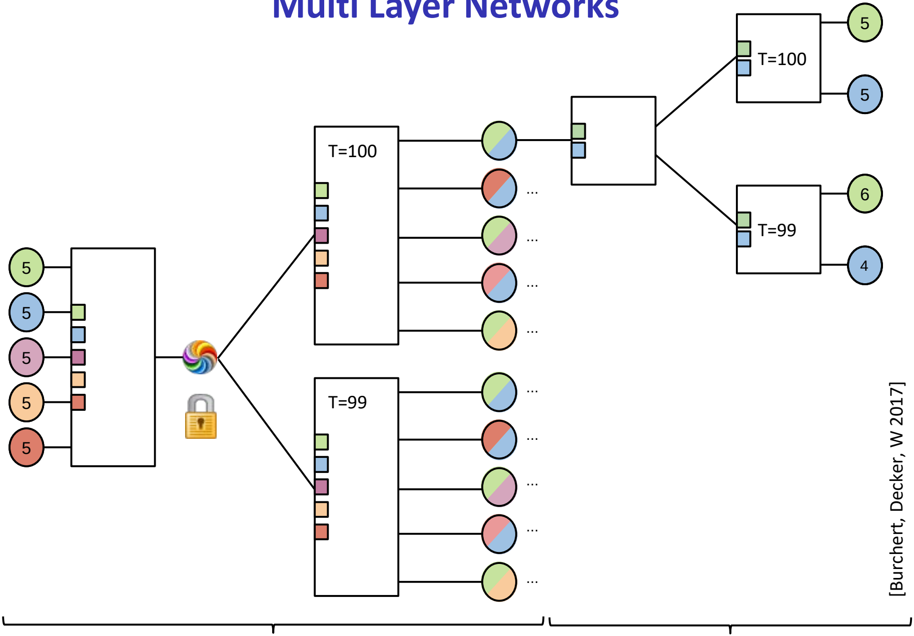
Locked Funds



A node wants to make connections…

Where does it lock the funds?

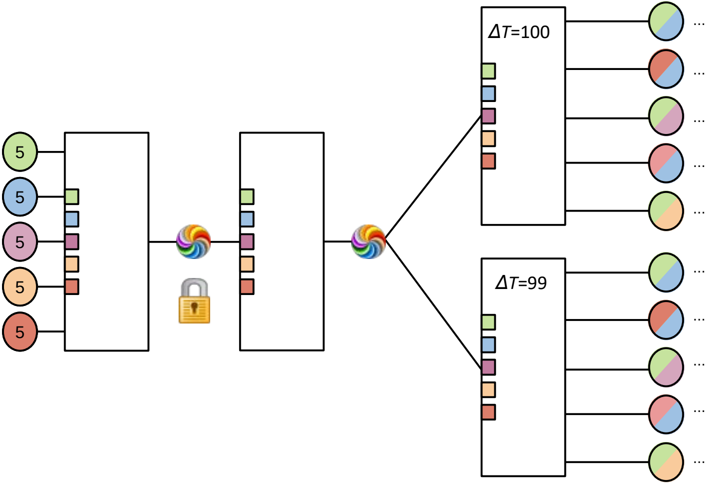
Multi Layer Networks



Channel funding layer

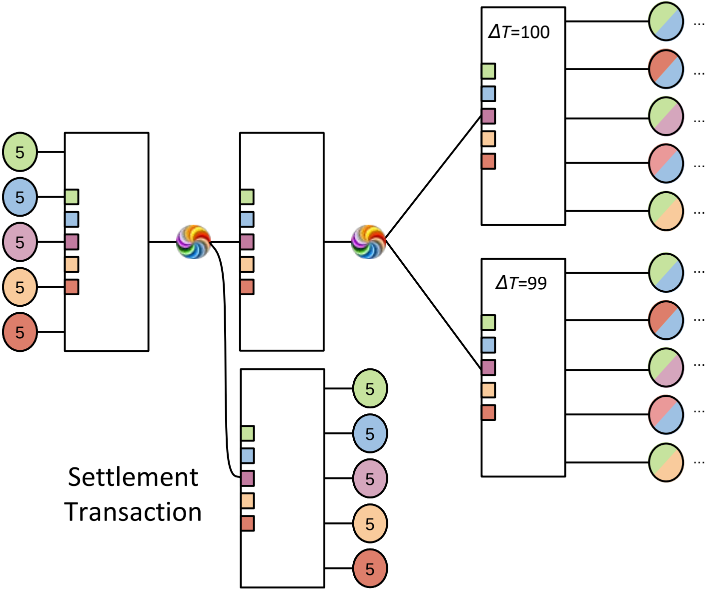
Payment network layer

Multi Layer Networks



[Burchert, Decker, W 2017]

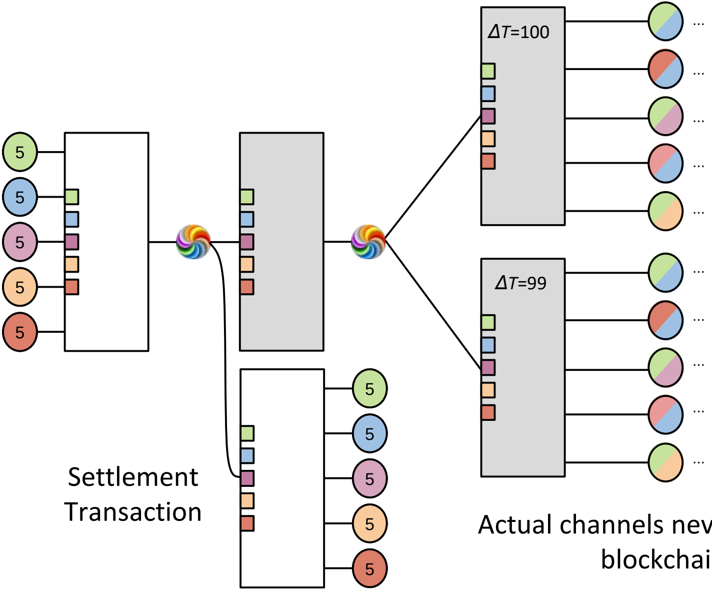
Multi Layer Networks



Settlement Transaction

[Burchert, Decker, W 2017]

Multi Layer Networks



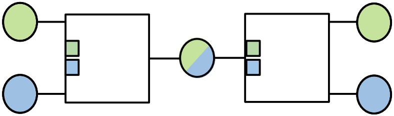
Settlement Transaction

Actual channels never reach the blockchain!

[Burchert, Decker, W 2017]

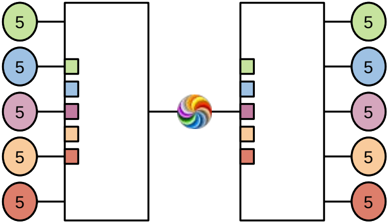
Blockchain Transactions

old



4 signatures per channel

new



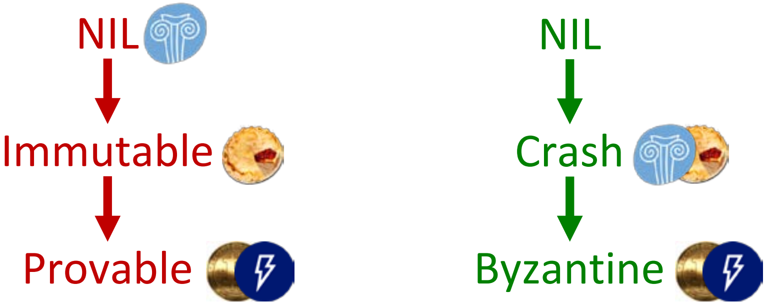
2 signatures per user

independent of channels

Blockchain

Persistence

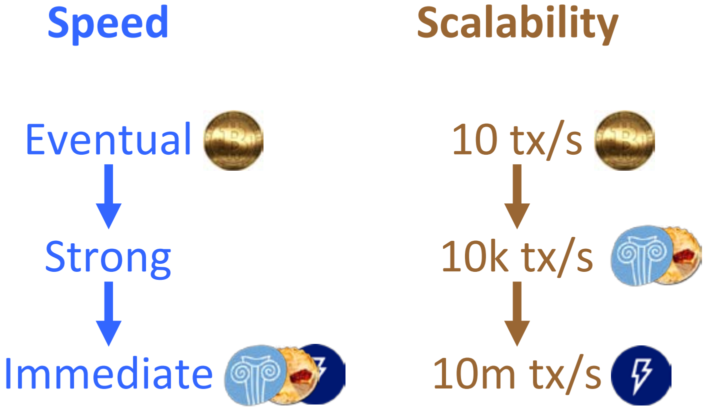
Fault-Tolerance



NIL → Immutable → Provable

NIL → Crash → Byzantine

Blockchain



Speed

Eventual

↓

Strong

↓

Immediate

Scalability

10 tx/s

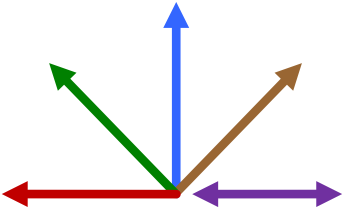
↓

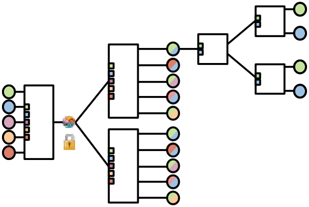
10k tx/s

↓

10m tx/s

Summary





Thank You!

Questions & Comments?

Thanks to my co-authors
Conrad Burchert
Christian Decker