What Should We Learn From Nakamoto's Blockchain?

Roger Wattenhofer
Not Me!
Blockchain: The Biggest Story in Distributed Systems Since ...
... the Internet?!?
Cryptocurrencies
Blockchain
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
ISBN-13 978-1522751830
ISBN-10 1522751831
So What Is a Blockchain?
**Ledger of Transactions**

<table>
<thead>
<tr>
<th>Description</th>
<th>Batch Line</th>
<th>Account Number</th>
<th>Description</th>
<th>Batch Line</th>
<th>Account Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interest Receivable</td>
<td>9</td>
<td>1280-000</td>
<td>Interest Receivable</td>
<td>9</td>
<td>1280-000</td>
</tr>
<tr>
<td>First National - Co</td>
<td>050-010</td>
<td>1050-000</td>
<td>First National - Co</td>
<td>050-010</td>
<td>1050-000</td>
</tr>
<tr>
<td>Municipal Bonds</td>
<td>050-010</td>
<td>1050-000</td>
<td>Municipal Bonds</td>
<td>050-010</td>
<td>1050-000</td>
</tr>
<tr>
<td>Other Investments</td>
<td></td>
<td></td>
<td>Other Investments</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Total Amount</strong></td>
<td></td>
<td></td>
<td><strong>Total Amount</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Debit Amount</strong></td>
<td></td>
<td></td>
<td><strong>Credit Amount</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11/200.20</td>
<td></td>
<td></td>
<td>1,830.10</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6,220.20</td>
<td></td>
<td></td>
<td>4,220.80</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3,664.30</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Blockchain

Distributed Systems & Cryptography
Blockchain
Transaction

![Diagram](image.png)
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 $\cdot$ Energy/Hash $\approx 1.3$ GW

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

Market / Energy Value \approx 19 \text{ GW}

\$20k/\text{BTC} \quad 12.5 \text{ BTC} \quad \$0.08/\text{kWh}

6/\text{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

PAY UP

OPEN
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

- Persistence
- Speed
- Privacy
- Fault-Tolerance
- Scalability
- Throughput
- Energy

Diagram showing the seven blockchain dimensions: Persistence, Speed, Privacy, Fault-Tolerance, Scalability, Throughput, and Energy.
The Seven Blockchain Dimensions

- Persistence
- Speed
- Privacy
- Fault-Tolerance
- Scalability
- Throughput
- Energy
- Privacy
Plenty of Research Dimensions
piChain
piChain: When a Blockchain Meets Paxos
piChain: When a Blockchain Meets Paxos
parent

depth
New Transaction: Reaction Time

- quick
- medium
- slow

wait → wait → time
quick \rightarrow medium \rightarrow slow

seen : either deeper or by
Self-Healing

healthy
Self-Healing

\[ q > 1 \]
\[ q = 0 \quad m > 1 \]
\[ q = 0 \quad m = 0 \]
\[ \text{election} \]

\[ q = 1 \quad m > 0 \]
\[ \text{healthy} \]
\[ q = 1 \quad m = 0 \]
committed
Truncated Paxos

*and next propose
Round 1  
1: Quick node $q$ sends “try $b_{new}$” to all nodes
2: On receiving a try message, all nodes:
3: \[\text{if } b_{new} \text{ deeper than } b_{max} \text{ then}\]
4: \[b_{max} = b_{new}\]
5: \[\text{Answer } q \text{ with “ok } b_{prop}, b_{supp} “\]
6: \[\text{end if}\]

Round 2  
7: Node $q$: If majority responded with ok:
8: \[b_{com} = b_{new}\]
9: \[\text{if some response included } b_{prop} \neq \bot \text{ then}\]
10: \[b_{com} = b_{prop} \text{ with deepest } b_{supp}\]
11: \[\text{end if}\]
12: Node $q$ sends “propose $b_{com}, b_{new}$” to all nodes

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

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

The graph shows the transaction count (`tx count`) over time (`time`). The lines represent different types of transactions:

- **Existing transactions** (black line)
- **Transactions in blocks** (blue line)
- **Commited transactions** (green line)

The graph illustrates how the transaction count increases over time, with distinct steps indicating the addition of new 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

---

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 $\text{hash}(r)$ 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

Blockchain

T=100

5

T=100

5

5

5

10
Duplex Micropayment Channel
Duplex Micropayment Channel

[Decker, W, 2015]
Duplex Micropayment Channel

Channel must be renewed often?
Relative timelocks to keep channel alive forever!

But only 99 transactions?
Duplex Micropayment Channel

[Decker,W,2015]
HTLC Revisited

4. “Send money if \( r \) is known at time 3”

can be spent by blue with secret \( r \) or by green after 3 days
4. Send money if $r$ is known at time 3.

Can be spent by blue with secret $r$ or by green after 3 days.
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

[Burchert, Decker, W 2017]
Multi Layer Networks

ΔΤ=100

ΔΤ=99

[Burchert, Decker, W 2017]
Multi Layer Networks

Settlement Transaction

\[ \Delta T = 100 \]

\[ \Delta T = 99 \]

[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...
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

- Village
- Server Room
- Country

100 nodes
Summary
Thank You!
Questions & Comments?

Thanks to my co-authors
Conrad Burchert
Christian Decker

www.disco.ethz.ch