An Efficient Blockchain?

Roger Wattenhofer
International Workshop on Cryptocurrencies and Blockchain Technology - CBT'17
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?
What Do You Think?
### Ledger of Transactions

**Manual Journal Voucher**

<table>
<thead>
<tr>
<th>Description</th>
<th>Account Number</th>
<th>Total Amount</th>
<th>Date</th>
<th>Effective Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accrued Interest Income</td>
<td>1280-000</td>
<td>11,200.40</td>
<td>2/14/16</td>
<td></td>
</tr>
<tr>
<td>Interest Receivable</td>
<td>6050-010</td>
<td>1,850.10</td>
<td></td>
<td></td>
</tr>
<tr>
<td>First National Co</td>
<td>6050-020</td>
<td>4,220.80</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Municipal Bonds</td>
<td>6050-010</td>
<td>3,649.30</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Other Investments</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Bitcoin**

The term 'Bitcoin' refers to a cryptocurrency that uses blockchain technology to secure and verify transactions. It is known for its decentralized nature and its role in the global economy as a means of exchange and investment.
My Usual Answer
Blockchain

Distributed Systems & Cryptography
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.
Hacker stahlen ETH-Doktoranden Bitcoin für 9 Millionen

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

VON CHRISTIAN BÜTIKOFER 06.12.2013
The Five Blockchain Dimensions

Persisteince

Fault-Tolerance

Speed

Scalability

Privacy
piChain
piChain: When a Blockchain Meets Paxos
piChain: When a Blockchain Meets Paxos
parent

depth
New Transaction: Reaction Time

quick → wait → medium → wait → slow

time
State Transitions

quick → medium → slow

seen : either deeper or by
Self-Healing

healthy
Self-Healing

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

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

*and next propose

*and committed

*and next propose

*and committed

*and next propose
Normal Paxos

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

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

Round 3
13: On receiving a propose message, all nodes:
14: \[ \text{if } b_{\text{new}} = b_{\text{max}} \text{ then} \]
15: \( b_{\text{prop}} = b_{\text{com}} \)
16: \( b_{\text{supp}} = b_{\text{new}} \)
17: Answer \( q \) with “ack \( b_{\text{com}} \)”
18: \[ \text{end if} \]

19: Node \( q \): If majority responded with ack:
20: Node \( q \) sends “commit \( b_{\text{com}} \)” to all nodes
21: On receiving a commit message, all nodes:
22: 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

- **Existing transactions**
- **Transactions in blocks**
- **Committed transactions**

**Graph Details:**
- **Y-axis:** tx count
- **X-axis:** time
- Time range: 0.0 to 20.0
- tx count range: 0 to 200
High Churn
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
Fundamental Problem
Every Node Sees Every Transaction
Payment Networks
Payment Network
Hashed Timelocked Contract (HTLC)
1. Generate random secret $r$

2. Send $\text{hash}(r)$ to \text{buyer}.

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

Blockchain

T=100

5

5

10

5

5
Duplex Micropayment Channel

[Decker, W, 2015]
Duplex Micropayment Channel

Blockchain

Channel must be renewed often?
Relative timelocks to keep channel alive forever!
But only 99 transactions?
Duplex Micropayment Channel

[Decker, W, 2015]
Why 2017 may be the year the industry figures out smart contracts... via Bitcoin

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.

Is smart contract possible on the Bitcoin blockchain? I thought that was said, but it didn't happen this year. Only Ethereum did.
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.

 HTLC Revisited

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

[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 6 to green instantly with secret $s_b$

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 $s_b'$

[References: 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

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 $s_b$.

[Poone,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 \cong \text{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

[Burchert, Decker, W 2017]
Multi Layer Networks

$\Delta T = 100$

$\Delta T = 99$

[Burchert, Decker, W 2017]
Multi Layer Networks
Multi Layer Networks

Settlement Transaction

Actual channels never reach the blockchain!

$\Delta T = 100$

$\Delta T = 99$

[Burchert, Decker, W 2017]
Blockchain Transactions

Old

New

4 signatures per channel

2 signatures per user, independent of channels
Blockchain

Persistence
- NIL
- Immutable
- Provable

Fault-Tolerance
- NIL
- Crash
- Byzantine
Blockchain

**Speed**

- Eventual
- Strong
- Immediate

10 tx/s

**Scalability**

- 10k tx/s
- 10m tx/s
Summary
Thank You!

Questions & Comments?

Thanks to my co-authors
Conrad Burchert
Christian Decker