Technical Analysis of the Tangle in the IOTA-Environment

Bennet Breier, 23.10.2017, Munich

Chair of Software Engineering for Business Information Systems (sebis)
Faculty of Informatics
Technische Universität München
www.matthes.in.tum.de
Outline

1. Motivation
2. Research Questions
3. Research Approach
4. Findings
   1. Analysis of the Tangle
   2. Comparison of Tangle & Blockchain
   3. The Tangle in the IOTA-environment
5. Conclusion & Outlook
Motivation

Inductive charging:
✓ Instant authentication
✓ Trustless Micro-payments
✓ Fast
✓ Scalable
✓ Immutable
1. Motivation
2. Research Questions
3. Research Approach
4. Findings
   1. Analysis of the Tangle
   2. Comparison of Tangle & Blockchain
   3. The Tangle in the IOTA-environment
5. Conclusion & Outlook
Research Questions

1. What is the theoretical foundation of the Tangle?

2. What are the key similarities & differences between Tangle and Blockchain?

3. How does IOTA use and advance the Tangle in its environment?
Outline

1. Motivation
2. Research Questions
3. Research Approach
4. Findings
   1. Analysis of the Tangle
   2. Comparison of Tangle & Blockchain
   3. The Tangle in the IOTA-environment
5. Conclusion & Outlook
Research Approach

✓ Literature & online research
  (google scholar, Blog posts)

✓ Online-communities
  • Slack team (incl. private messages)
  • forum.iota.org
  • reddit
  • Github (+ code review)

✓ 2 interviews with members of IOTA:
  • Paul Handy (core-developer)
  • Alexander Renz (business advisor)
Outline

1. Motivation
2. Research Questions
3. Research Approach
4. Findings
   1. Analysis of the Tangle
   2. Comparison of Tangle & Blockchain
   3. The Tangle in the IOTA-environment
5. Conclusion & Outlook
Outline

1. Motivation
2. Research Questions
3. Research Approach
4. Findings

1. Analysis of the Tangle
2. Comparison of Tangle & Blockchain
3. The Tangle in the IOTA-environment
5. Conclusion & Outlook
The Tangle

Initialization

genus tx

1  
2  
3  

1  
2  
1  
2  

Cumulative Weight = 5
The Tangle
Issuing a Transaction

1. Bundling & Signing
2. Tip Selection
3. Validation
4. Proof-of-Work (PoW)
5. Publishing
The Tangle
1. Bundling & Signing

Structure of a transaction

<table>
<thead>
<tr>
<th>Field</th>
<th>tx_0</th>
<th>80 iota</th>
<th>output</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>tx_1</td>
<td>-100 iota</td>
<td>input</td>
</tr>
<tr>
<td></td>
<td>tx_2</td>
<td>0 iota</td>
<td>input</td>
</tr>
<tr>
<td></td>
<td>tx_3</td>
<td>20 iota</td>
<td>remainder</td>
</tr>
</tbody>
</table>

- hash
- signatureMessageFragment
  - address
  - value
  - (timestamp)
- currentIndex
- lastIndex
- bundle
- trunkTransaction
- branchTransaction
- nonce
The Tangle

2. Tip Selection

Markov Chain Monte Carlo (MCMC)

\[ P_{xy} = \frac{e^{-\alpha(H_x - H_y)}}{\sum_{z:x \rightarrow z} e^{-\alpha(H_x - H_y)}} \]
The Tangle

3. Validation

1. valid sub-tangle
   valid sub-tangle
   valid sub-tangle
   +

2. Check PoW
   +

3. all address-balances >= 0
   no temporal order!
   A → B (10)
   B → C (10)
The Tangle

4. PoW

Hashcash
✓ DDOS-protection
✓ Immutability
✓ Protection against double-spending

Structure of a transaction

<table>
<thead>
<tr>
<th>Field</th>
</tr>
</thead>
<tbody>
<tr>
<td>hash</td>
</tr>
<tr>
<td>signatureMessageFragment</td>
</tr>
<tr>
<td>address</td>
</tr>
<tr>
<td>value</td>
</tr>
<tr>
<td>(timestamp)</td>
</tr>
<tr>
<td>currentIndex</td>
</tr>
<tr>
<td>lastIndex</td>
</tr>
<tr>
<td>bundle</td>
</tr>
<tr>
<td>trunkTransaction</td>
</tr>
<tr>
<td>branchTransaction</td>
</tr>
<tr>
<td>nonce</td>
</tr>
</tbody>
</table>
The Tangle

5. Publishing

![Diagram of the Tangle]

- tx
- tx
- tx
- tx
- tx
- tx_3
- tx_2
- tx_1
- tx_0

Bundle
The Tangle

Splitting Attack
Outline

1. Motivation
2. Research Questions
3. Research Approach
4. Findings
   1. Analysis of the Tangle
   2. Comparison of Tangle & Blockchain
   3. The Tangle in the IOTA-environment
5. Conclusion & Outlook
Comparison of Tangle & Blockchain
Comparison

Scalability

![Graph showing scalability with network capacity and transactions on the x-axis and number of blocks per day on the y-axis. The graph compares IOTA with Ethereum.](image)

**Blocks per day**

- Oct '15 to Apr '17
## Comparison

### Fees & Time to Confirmation

<table>
<thead>
<tr>
<th>Tangle</th>
<th>Buyer</th>
<th>Merchant</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>PoW↑</td>
<td>Propagation↑</td>
</tr>
<tr>
<td></td>
<td>Specific percentage of consensus.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Blockchain</th>
<th>Fee↑</th>
<th>Mined↑</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Specific number of blocks building on top of this block.</td>
<td></td>
</tr>
</tbody>
</table>
Comparison

Energy Consumption
Outline

1. Motivation
2. Research Questions
3. Research Approach
4. Findings
   1. Analysis of the Tangle
   2. Comparison of Tangle & Blockchain
   3. The Tangle in the IOTA-environment
5. Conclusion & Outlook
The backbone of IoT is here!
IOTA

Specific Concepts

1. The Coordinator
2. Peer discovery
3. Snapshots
Outline

1. Motivation
2. Research Questions
3. Research Approach
4. Findings
   1. Analysis of the Tangle
   2. Comparison of Tangle & Blockchain
   3. The Tangle in the IOTA-environment
5. Conclusion & Outlook
Conclusion & Outlook

Concepts behind IOTA’s Tangle
How to issue transactions
Feeless, scalable, immutable ledger

Smart contracts
Energy consumption
Cryptographic security & the coordinator
Concrete use-cases
Thank you for your attention

Further questions?
B.S. Information Systems

**Bennet Breier**

Technische Universität München
Faculty of Informatics
Chair of Software Engineering for Business Information Systems

Boltzmannstraße 3
85748 Garching bei München

Tel  +49.89.289.
Fax  +49.89.289.17136

bennet.breier@tum.de
www.matthes.in.tum.de
[{
  "address": "ZHITHKLKRZEY9HJCWH9DBLIHZLWB9OUMSKZHNAEQVMPSMQYWYJHUJRZHIJIGJBUSHLXLWETVWNFWLPZAL",
  "balance": "50000000"
},
{
  "address": "DWVNBUBSTUTSEB9KZPATIKHDJPZGEEFATMIGZFQKZTAYVZ99GNQAMQVNRBSUATBNVDOPOLPUYBQUXWHUO",
  "balance": "2000000000000"
}]