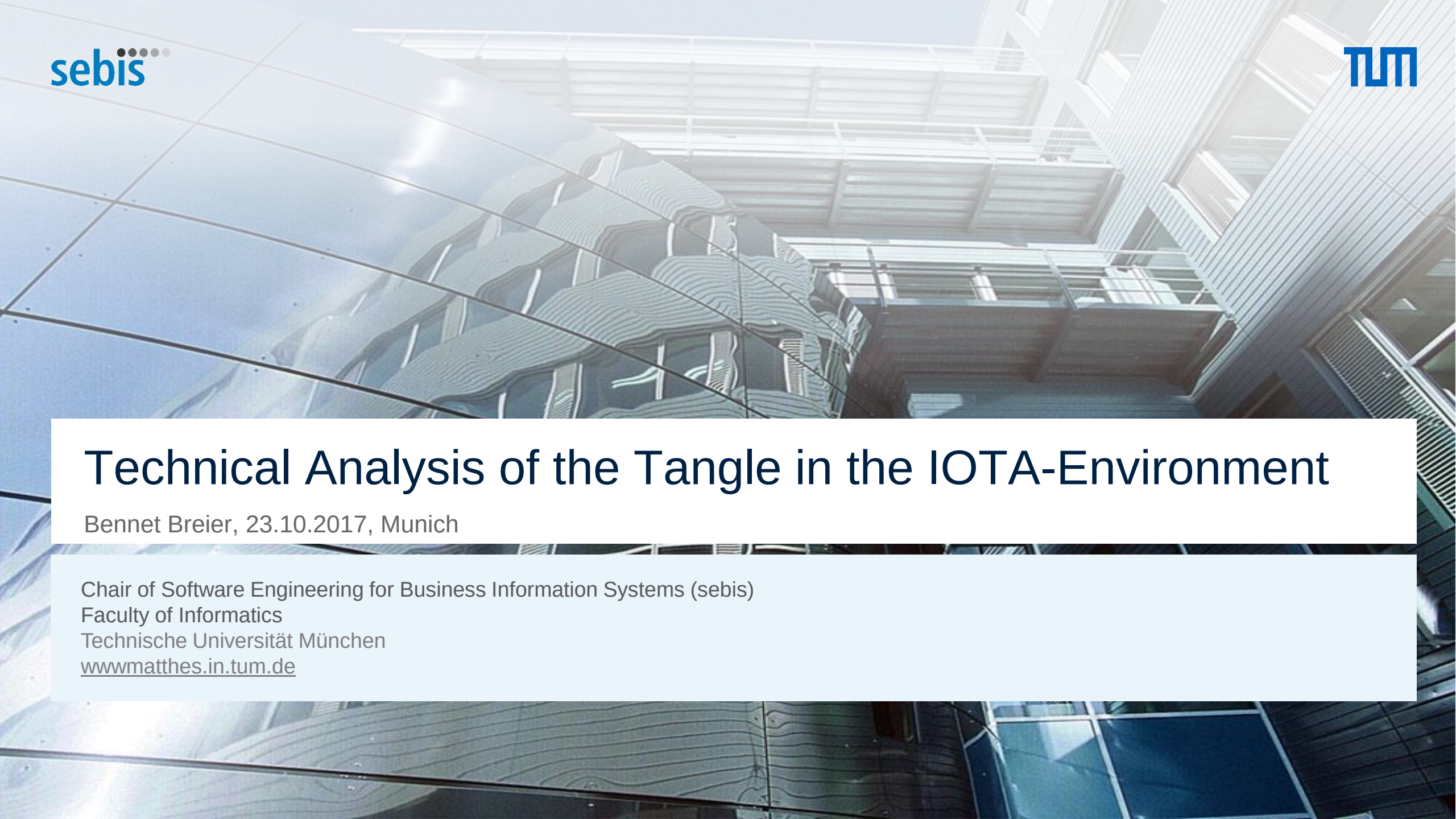


Technical Analysis of the Tangle in the IOTA-Environment

Bennet Breier, 23.10.2017, Munich

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

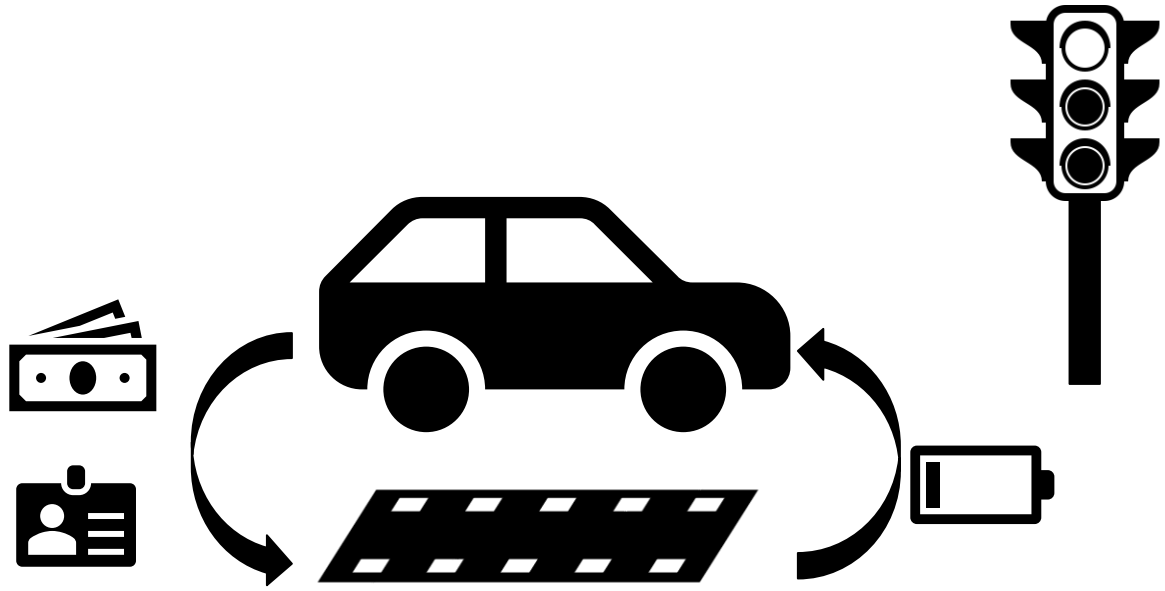
Outline

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

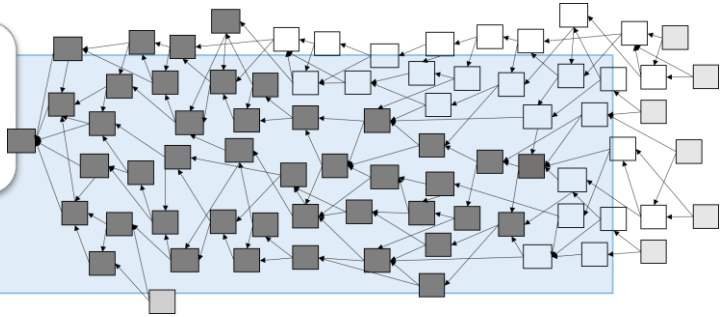


Outline

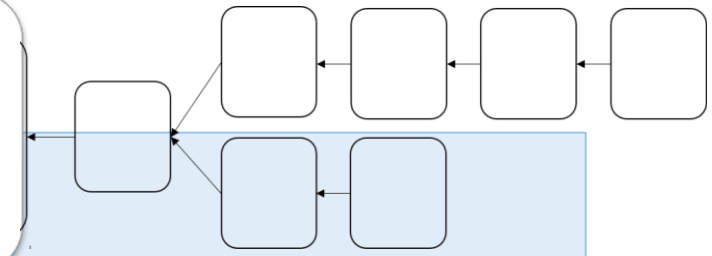
1. Motivation
2. Research Questions
3. Research Approach
4. Findings
    1. Analysis of the Tangle
    2. Comparison of Tangle & Blockchain
    3. The Tangle in the IOTA-environment
5. Conclusion & Outlook

Research 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

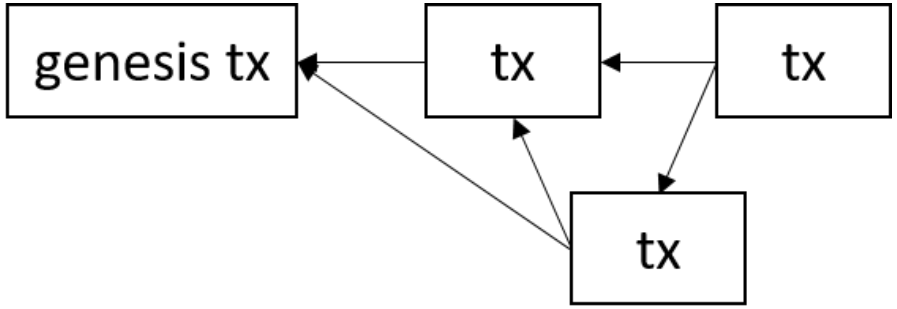
1. Motivation
2. Research Questions
3. Research Approach
4. Findings
    1. Analysis of the Tangle
    2. Comparison of Tangle & Blockchain
    3. The Tangle in the IOTA-environment
5. Conclusion & Outlook

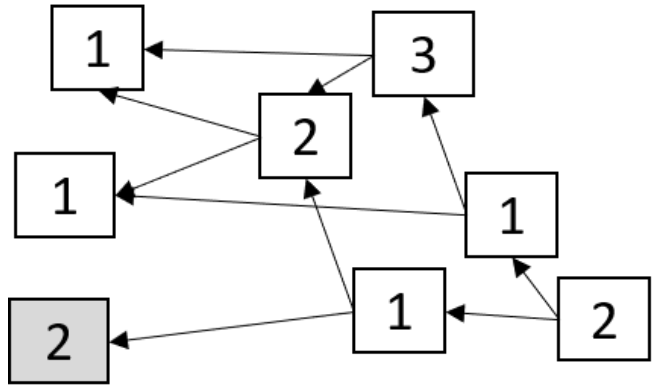
Outline

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





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

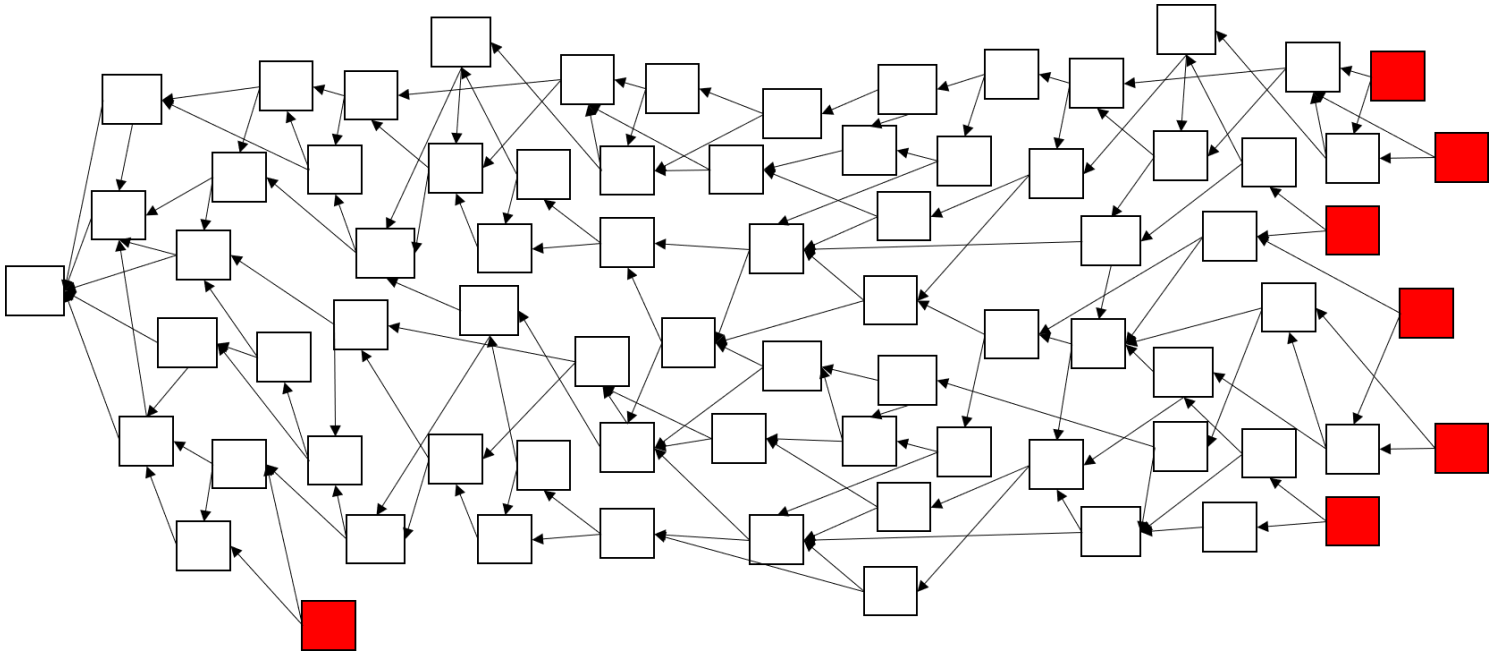
hash
signatureMessageFragment address value (timestamp)
currentIndex lastIndex bundle
trunkTransaction branchTransaction
nonce

tx_0	80 iota	output
tx_1	-100 iota	input
tx_2	0 iota	input
tx_3	20 iota	remainder

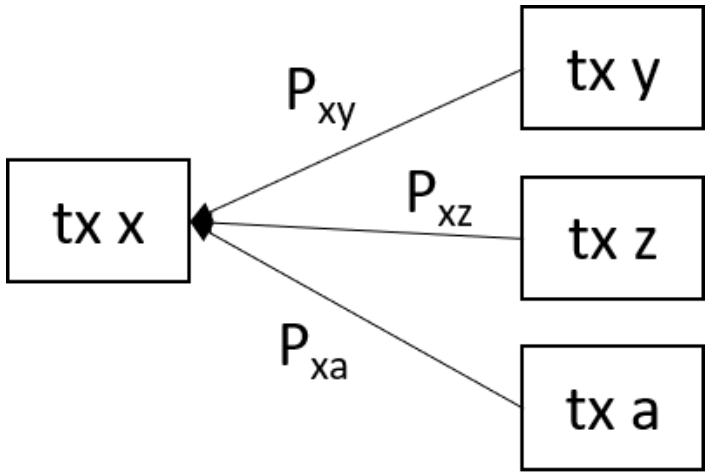
The Tangle

2. Tip Selection

Markov Chain Monte Carlo (MCMC)



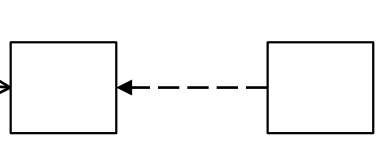
$$P_{xy} = \frac{e^{-\alpha(H_x - H_y)}}{\sum_{z:x \leftsquigarrow z} e^{-\alpha(H_x - H_y)}}$$



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!

$$A \rightarrow B\ (10)$$
$$B \rightarrow C\ (10)$$

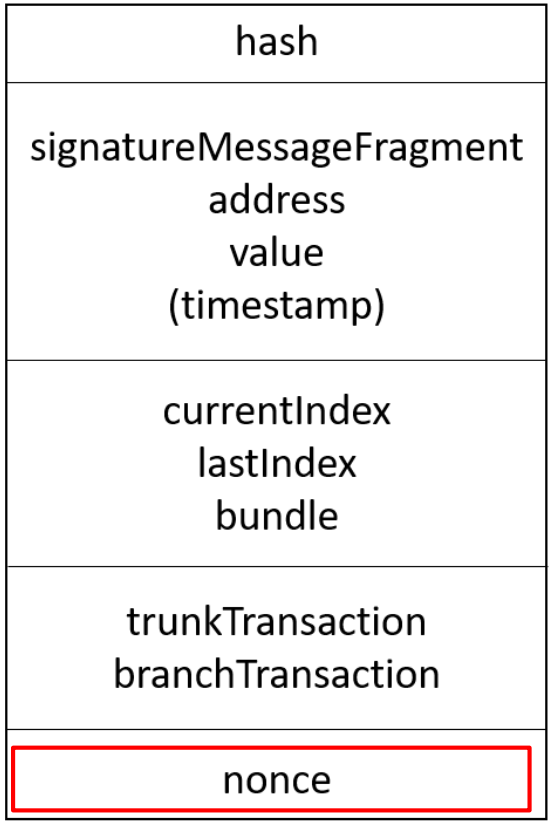
The Tangle

4. PoW

Hashcash

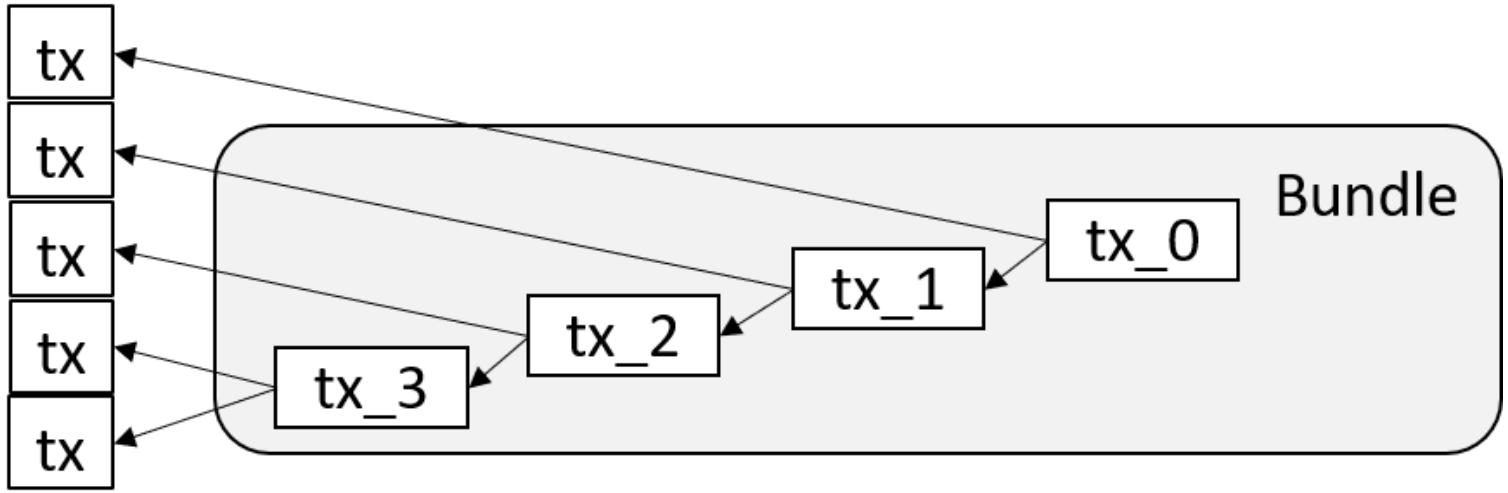
- ✓ DDOS-protection
- ✓ Immutability
- ✓ Protection against double-spending

Structure of a transaction



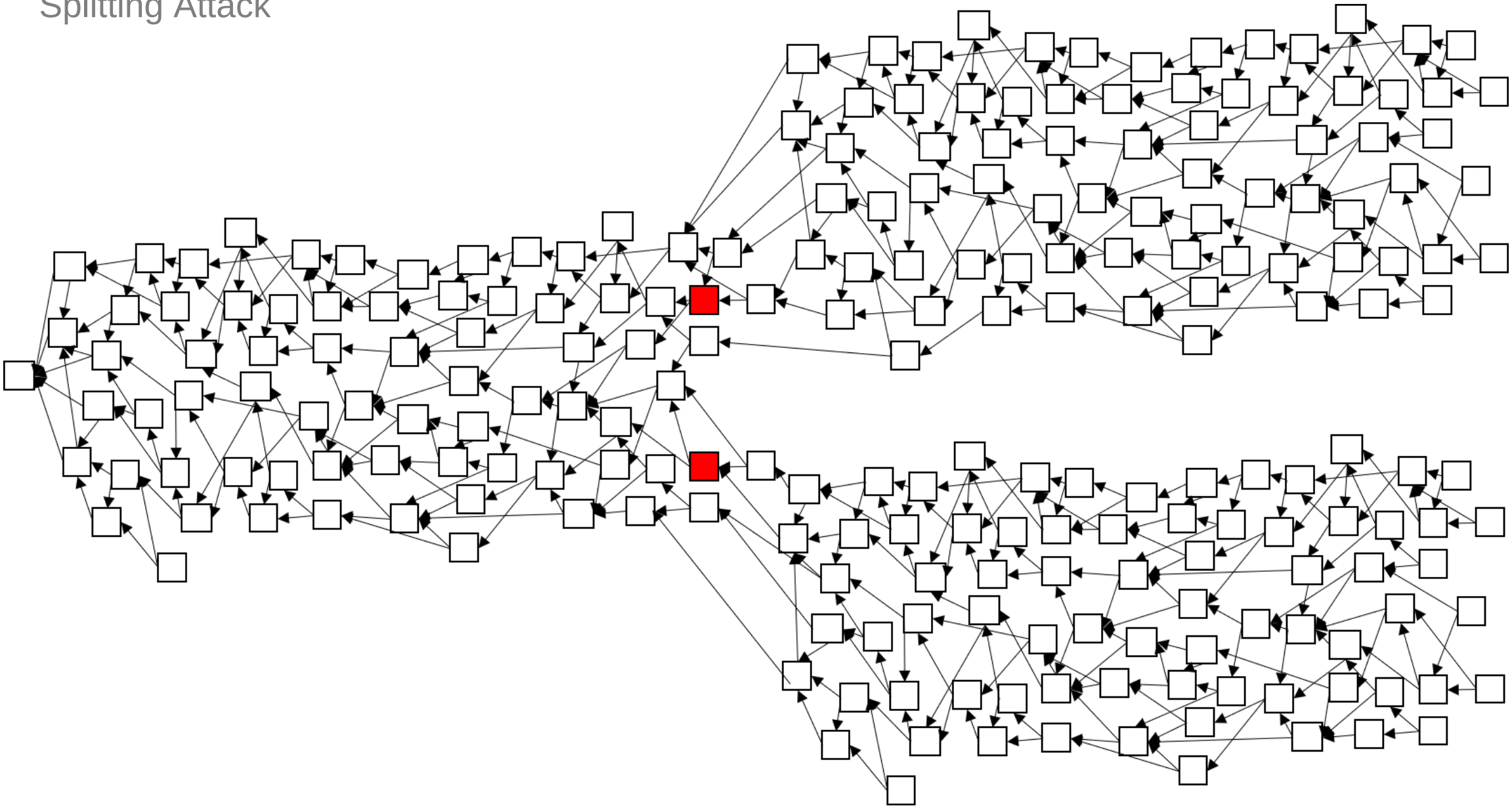
The Tangle

5. Publishing



The Tangle

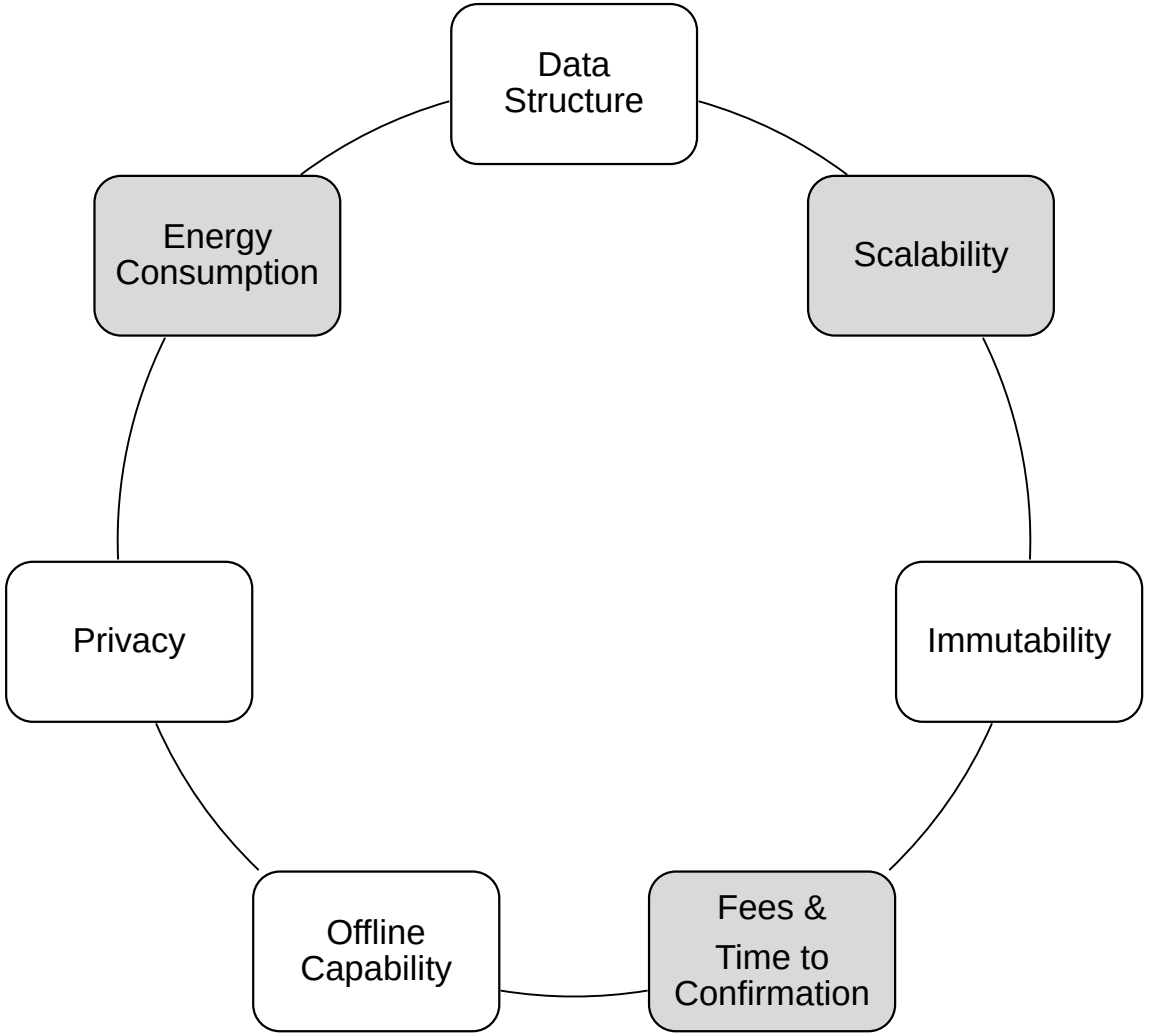
Splitting Attack



Outline

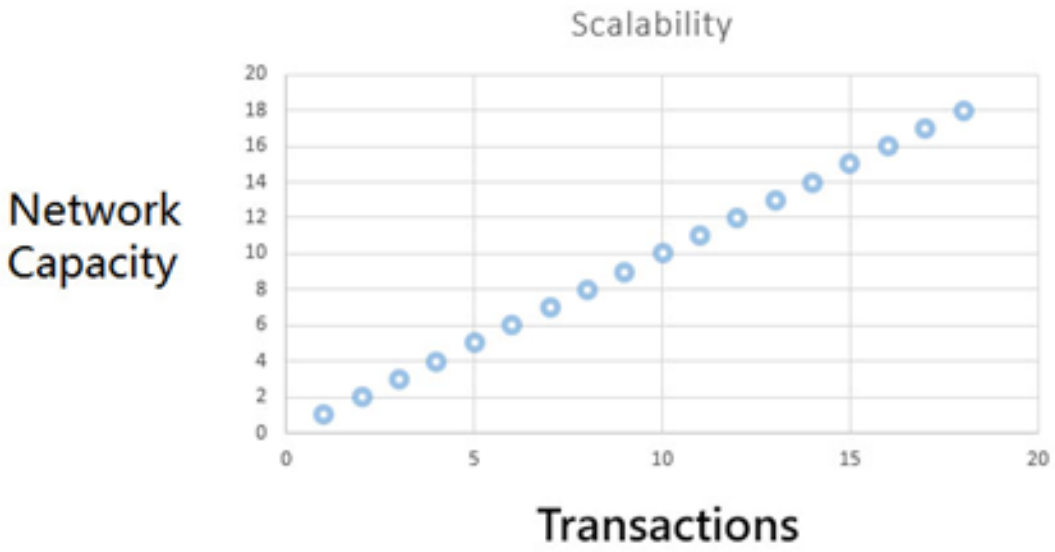
1. Motivation
2. Research Questions
3. Research Approach
4. Findings
    1. Analysis of the Tangle
    2. Comparison of Tangle & Blockchain
    3. The Tangle in the IOTA-environment
5. Conclusion & Outlook

Comparison of Tangle & Blockchain

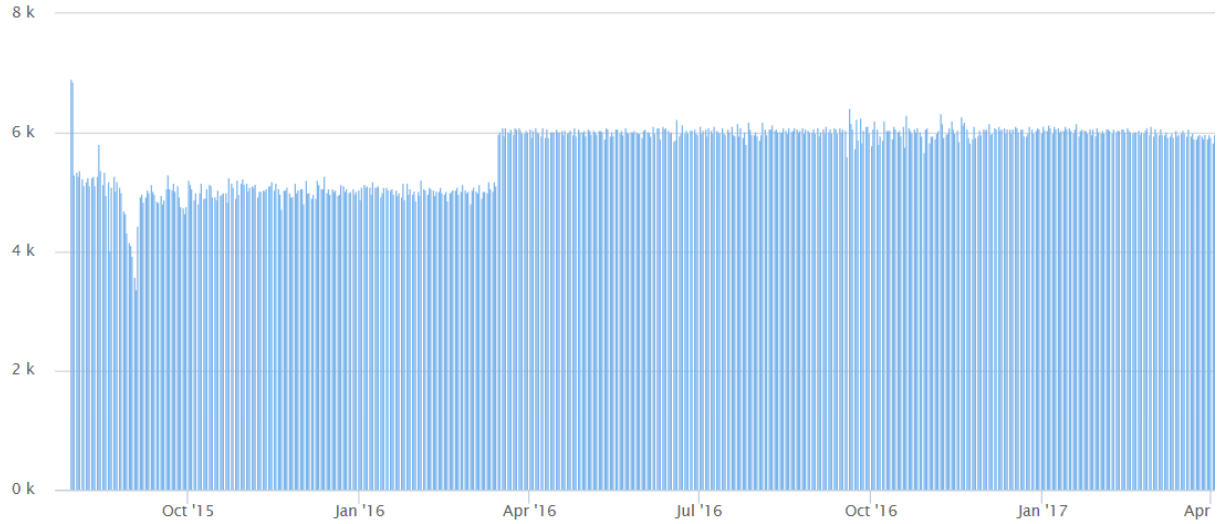


Comparison

Scalability



Blocks per day



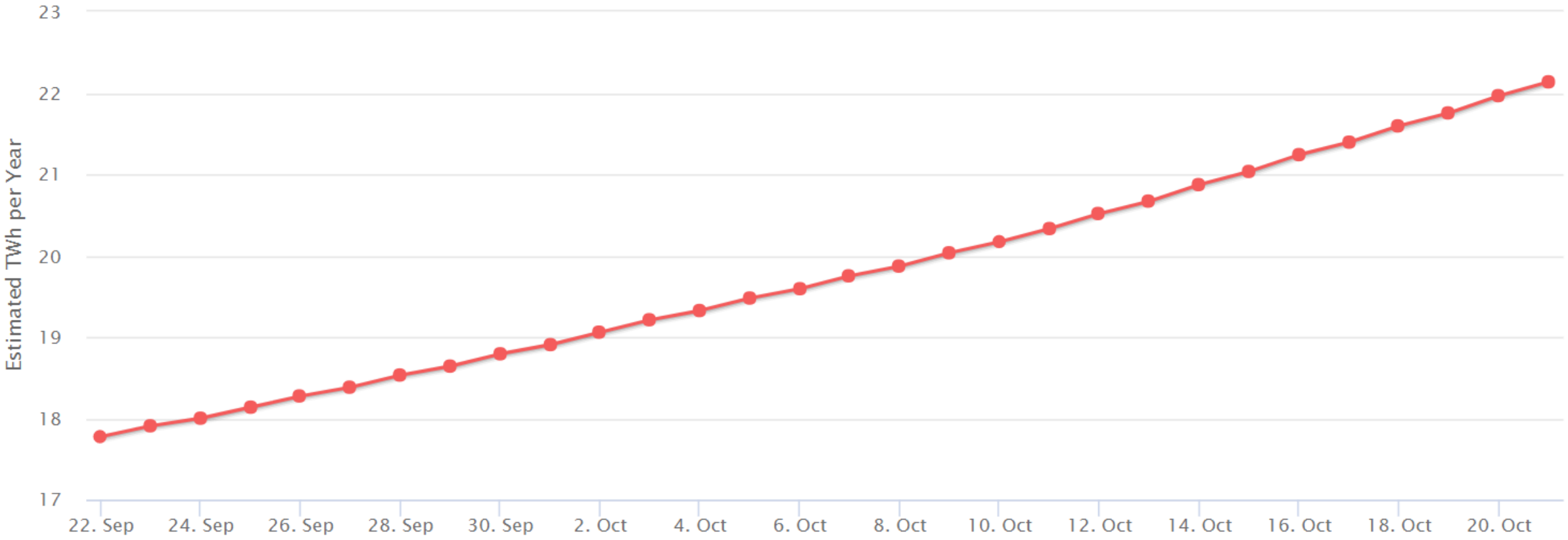
Comparison

Fees & Time to Confirmation

	Buyer	Merchant
Tangle	PoW ↑ ⟹ Propagation ↑	Specific percentage of consensus.
Blockchain	Fee ↑ ⟹ Mined ↑	Specific number of blocks building on top of this block.

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

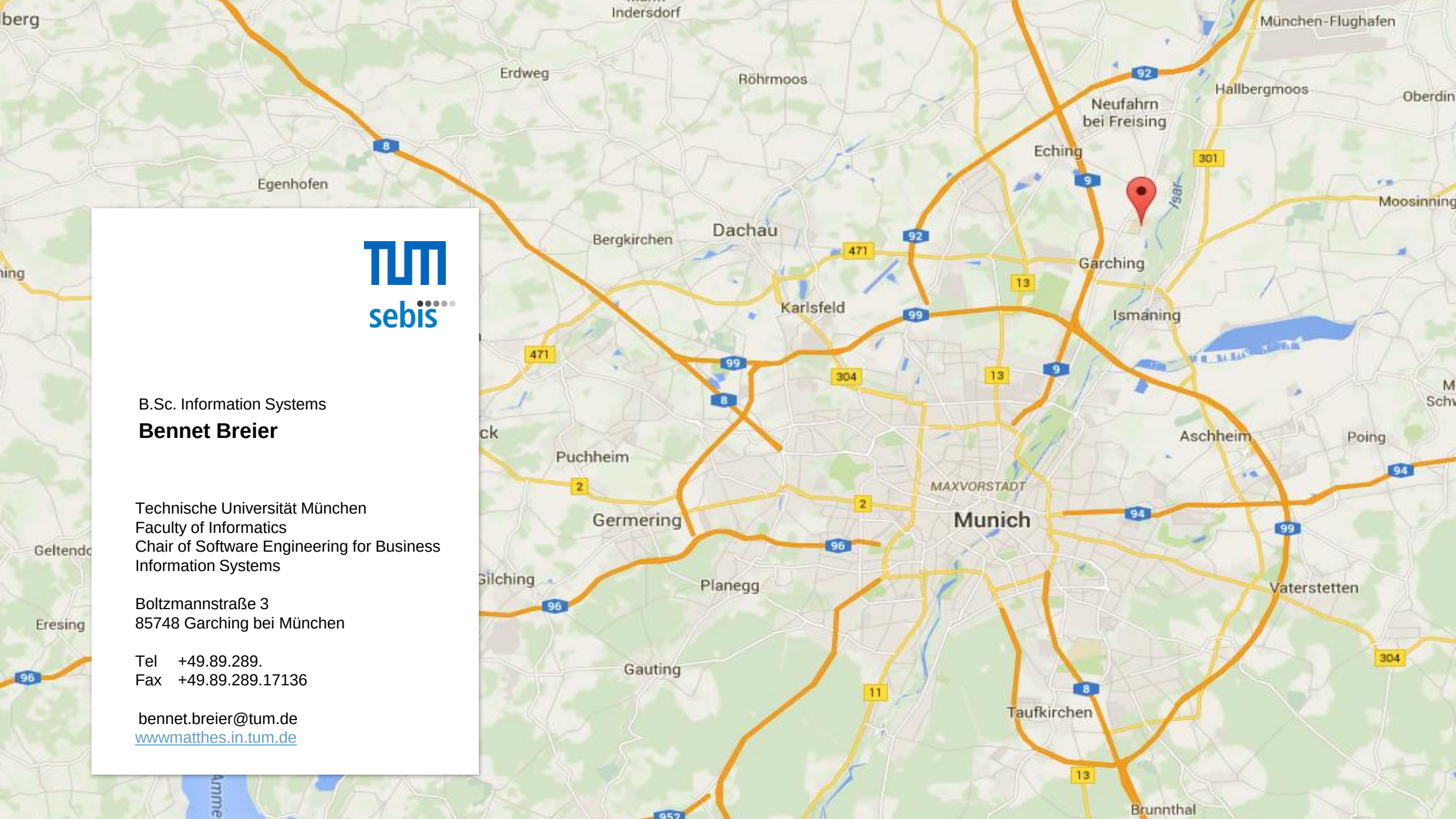
Energy consumption

Cryptographic security & the coordinator

Concrete use-cases

Thank you for your attention

Further questions?



B.Sc. 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
wwwmatthes.in.tum.de

Backup

```
[
    {
        "address":
            "ZHITHKLKRZEY9HJCWH9DBLIHZLWB9OUMSKZHNAEQVMPSMQYWYJHUJRZHIJI
             GJBUSHLXLWETVWNFWLPZAL",
        "balance": "50000000"
    },
    {
        "address":
            "DWVNBUBSTUTSEB9KZPATIKHDJPZGEEFATMIGZFKQZTAYVZ99GNQAMQVNRBS
             UATBNVDOPOLPUYBQUXWHUO",
        "balance": "200000000000"
    },
    ...
]
```