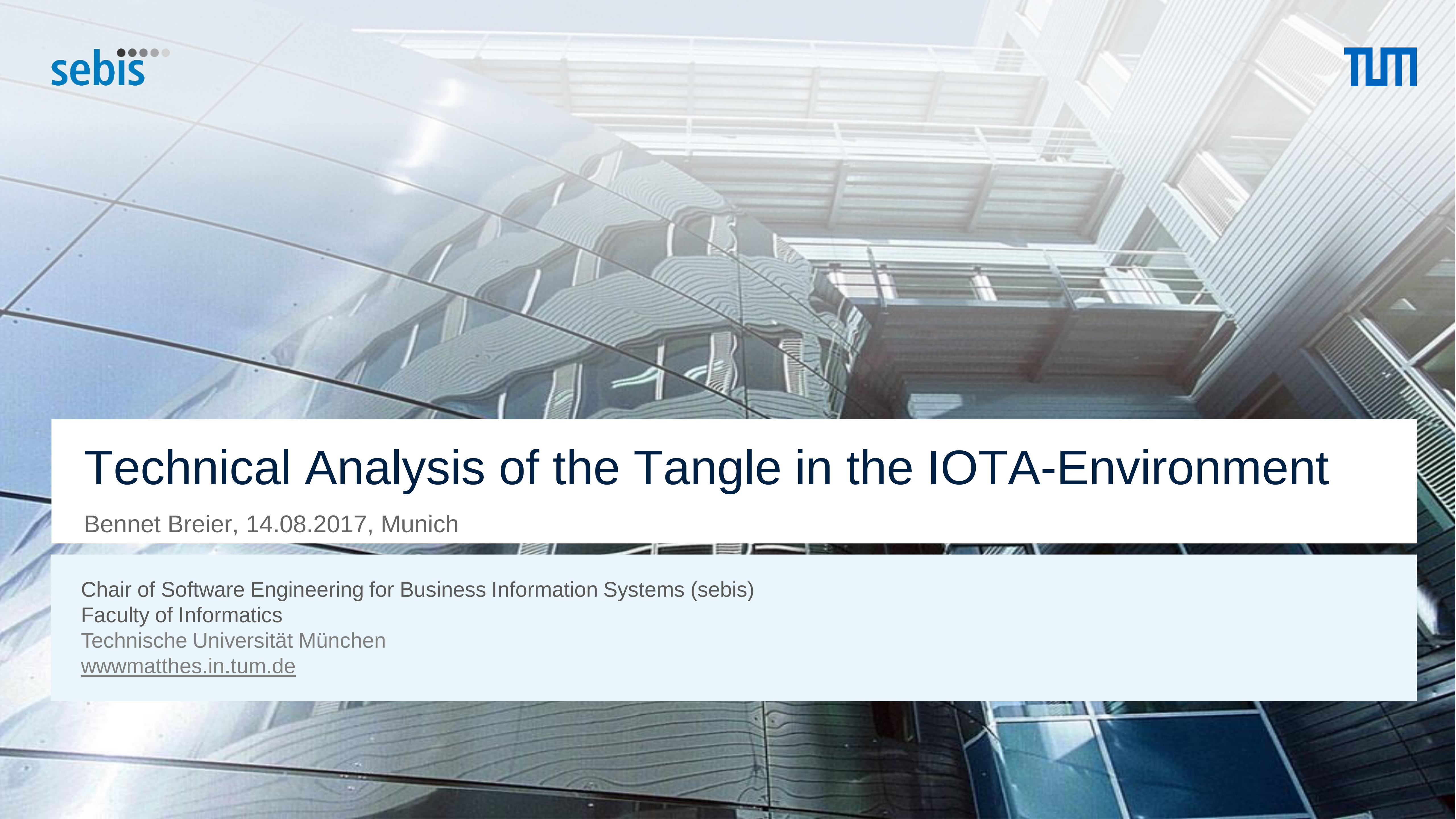


Technical Analysis of the Tangle in the IOTA-Environment

Bennet Breier, 14.08.2017, 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 & Approach
3. Timeline
4. Example Analysis

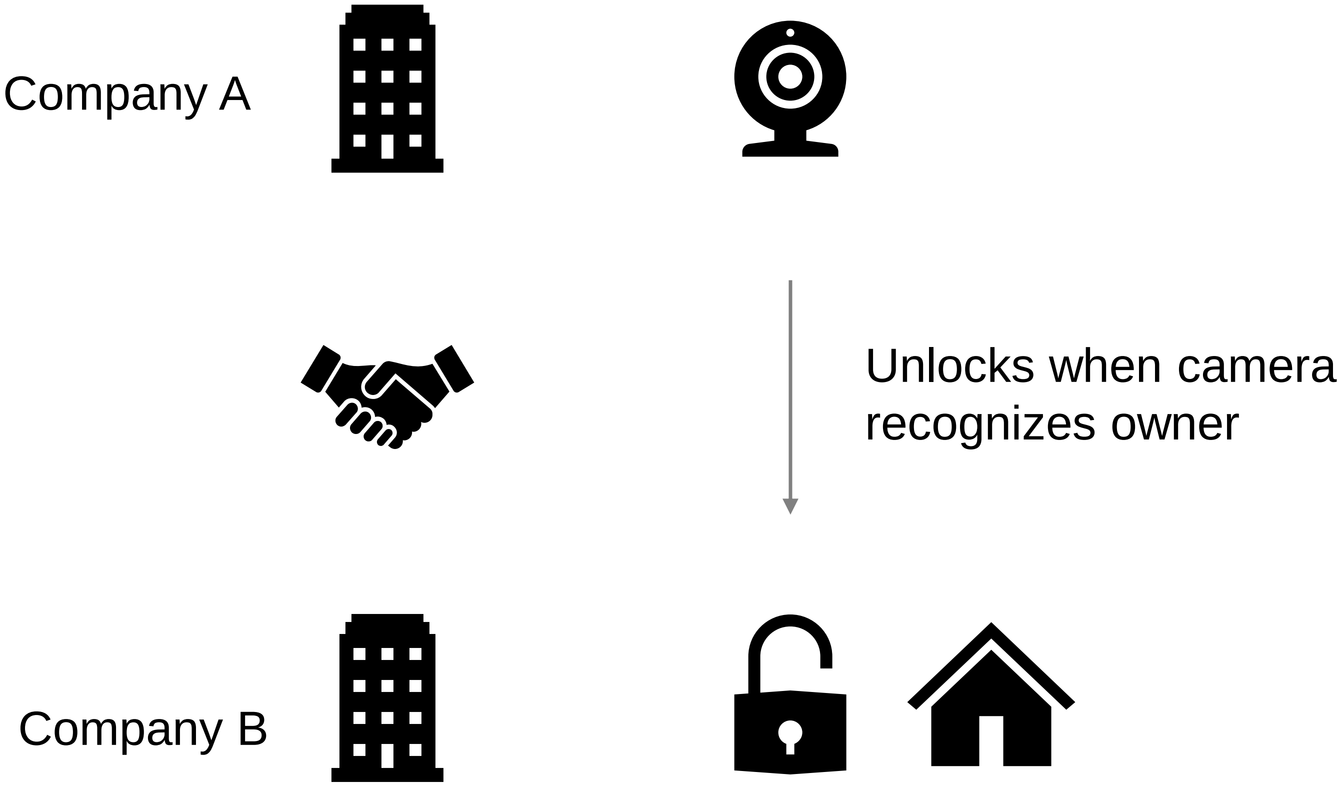
Motivation – Simple Example

Distributed Ledger Technology:

✓ Smart devices can communicate

✓ The ledger is legally binding

✓ And immutable



Company A

Unlocks when camera recognizes owner

Company B

Motivation

IOTA

- ✓ no fees
- ✓ scalable
- ✓ fast (700 txs/sec, gets faster with more users)
- ✓ works offline
- ✓ quantum secure

➡ Better suited for IoT use-cases

ethereum

- ❖ 0.25 € per tx (transaction)
- ❖ Scalability issues not resolved
- ❖ 25 txs/sec
- ❖ needs internet connection
- ❖ RSA, ECC not quantum secure

Setup of this Bachelor’s Thesis

Title: Technical Analysis of the Tangle in the IOTA-Environment

Author: Bennet Breier (bennet.breier@tum.de)

Advisor: Patrick Holl (patrick.holl@tum.de)

Start: 15 August 2017

End: 15 November 2017

Outline

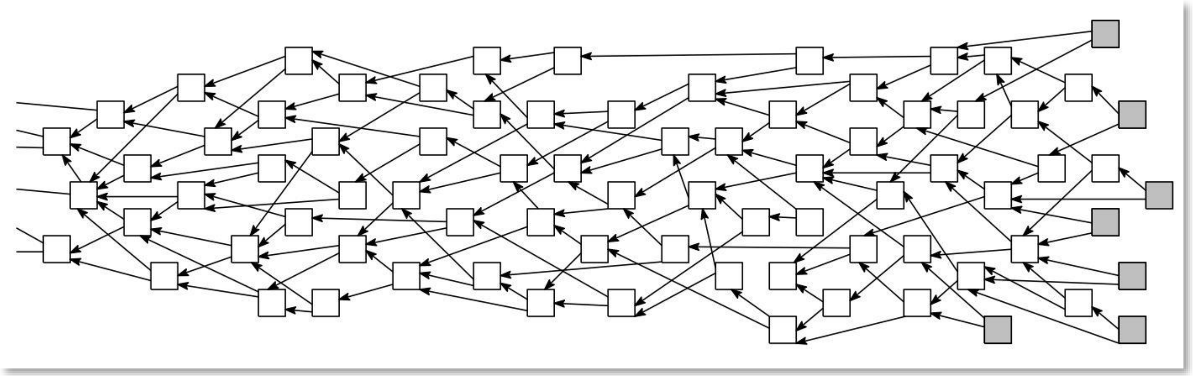
1. Motivation
2. Research Questions & Approach
3. Timeline
4. Example Analysis

Research Questions and Approach

1. What is the theoretical foundation of the tangle?

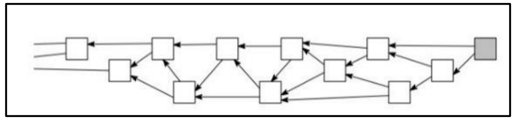
- Processing of Transactions
- Tip selection
- Byzantine Fault Tolerance
- Proof-of-Work
- Hashing (Curl & Kerl) & cryptography
- Scalability
- Privacy
- Quantum resistance

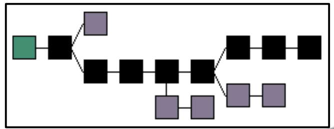
- Conditions for a secure & stable system
- Attack vectors (Sybil Attack, Parasite Chain Attack, Splitting Attack, 300% Attack)



Research Questions and Approach

2. What are the key differences between tangle vs. blockchain?





Comparable characteristics: (argued along a comprehensive use-case)

- Data structure
- Scalability, Transactions per second
- Fee structure
- Time to confirmation
- Privacy
- Security

Research Questions and Approach

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

- Facts about IOTA Foundation (business relations, adoption/advantages of their technology, …)
- IOTA-Implementation (deviations from theory)
- Coordinator
- peer discovery

Approach

Research questions

R1

- Theory behind the tangle

R2

- Tangle vs. Blockchain

R3

- IOTA environment

Research Approach

✓ Literature & online research (google scholar, ….)

✓ Online-communities

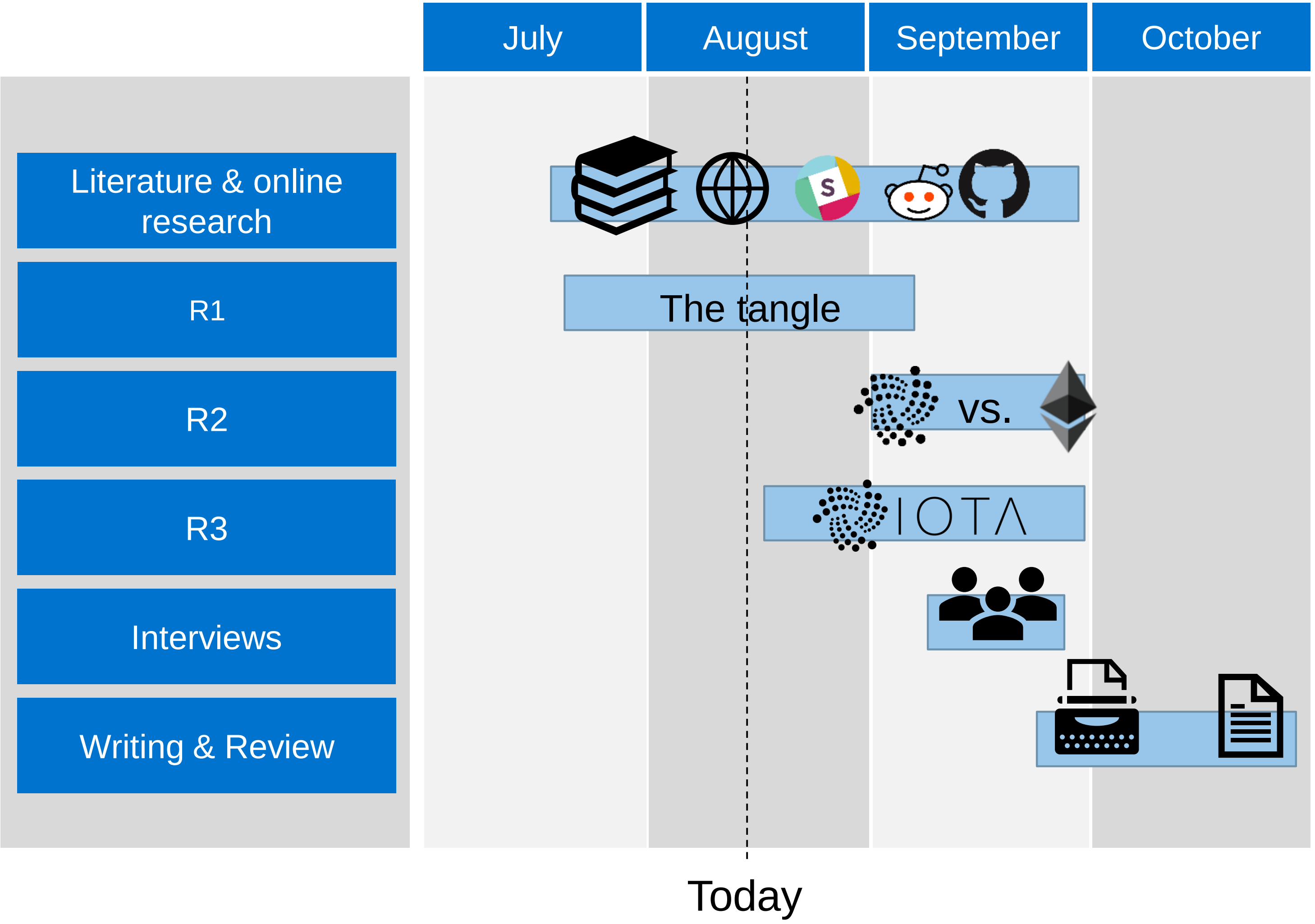
- Slack team
- forum.iota.org
- reddit
- Github (+ code review)
- Stackoverflow (coming soon)

✓ 2 – 4 Interviews with members of IOTA

Outline

1. Motivation
2. Research Questions & Approach
3. Timeline
4. Example Analysis

Timeline



Official Start Date: 15.08.2017

Official End Date: 15.12.2017

Supervisor: Patrick Holl

Outline

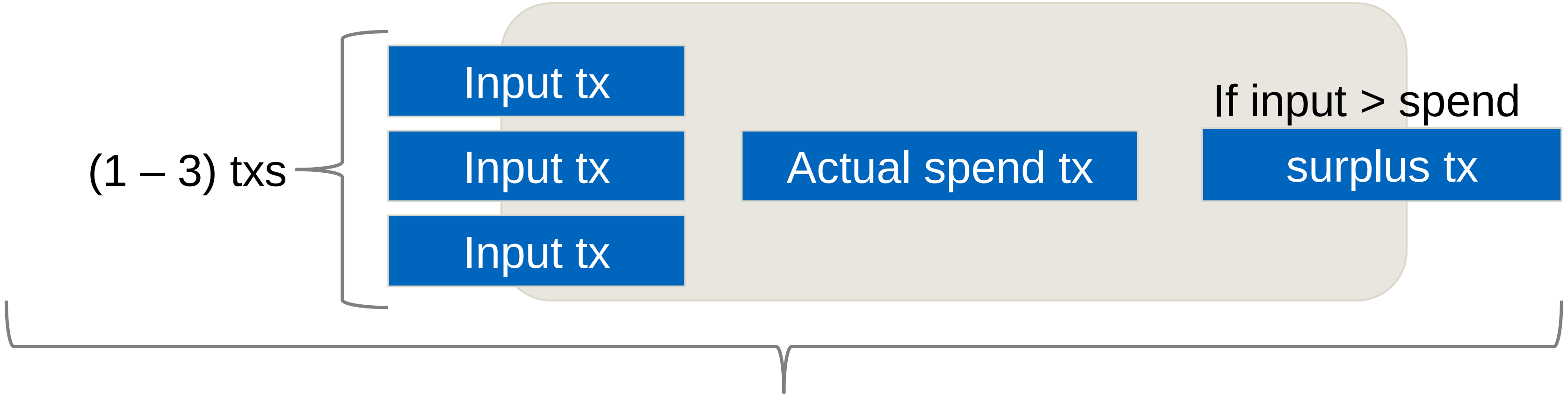
1. Motivation
2. Research Questions & Approach
3. Timeline
4. Example Analysis

Example Analysis Process

Processing of Transactions

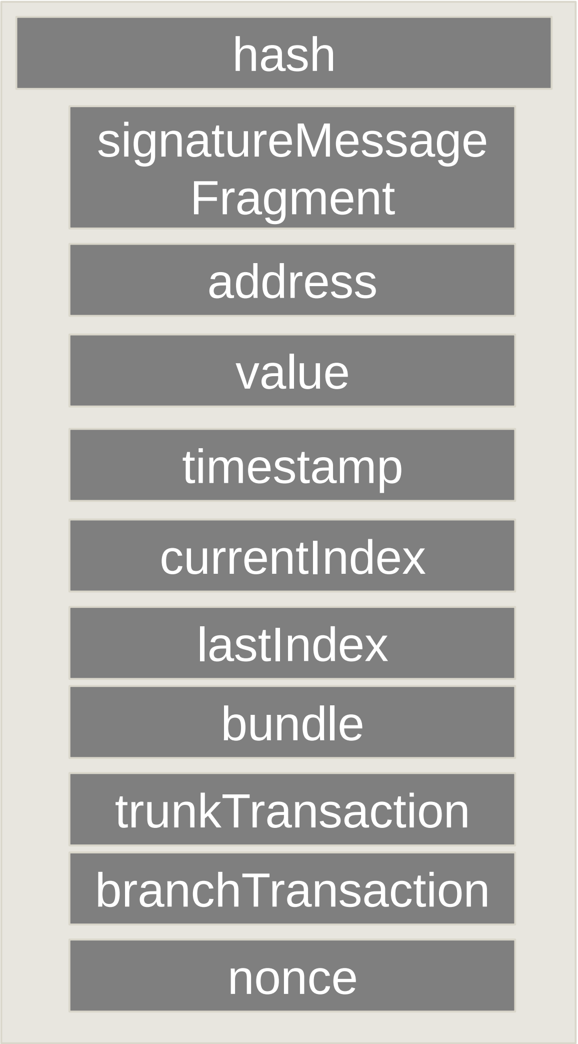
1. Constructing the bundle and signing of inputs
2. Tip selection
3. Proof of Work

1. Constructing the bundle and signing of inputs



1 bundle = (2 – 5) txs

Structure of a transaction



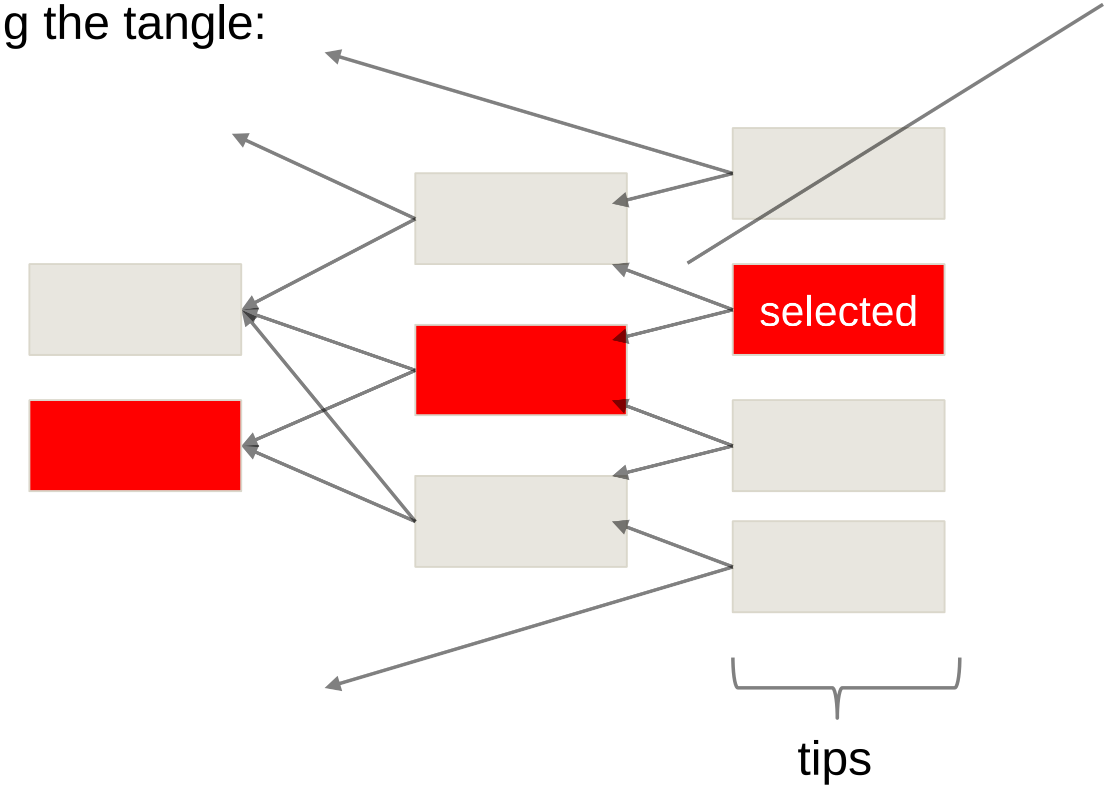
Example Analysis Process

Processing of Transactions

2. Select 2 tips according to a tip selection strategy

- Random tip selection
- **Markov Chain Monte Carlo:**

Perform multiple random-walks along the tangle:



the transition-probability is proportional to the **cumulative weight** of the tx

cumulative weight =
own weight of tx + sum of weights of all approving txs

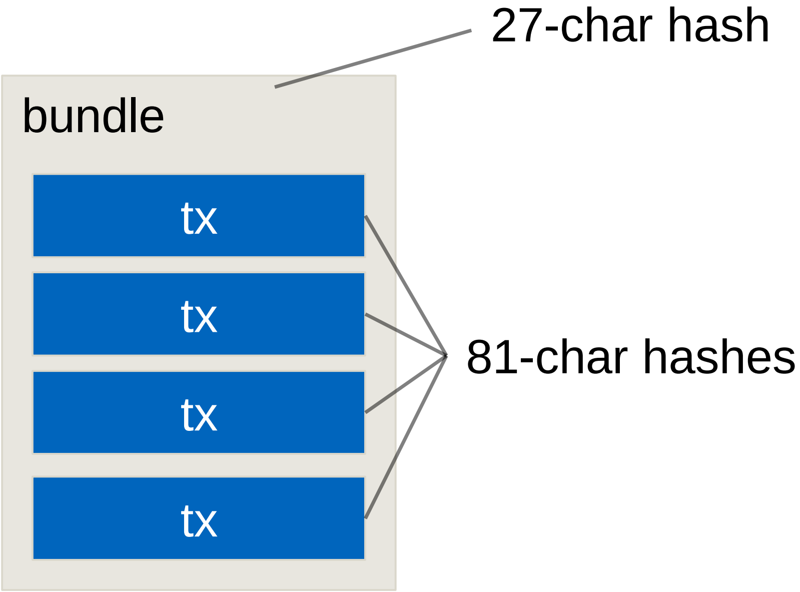
own weight of a tx is proportional to the amount of work put into it

Example Analysis Process

Processing of Transactions

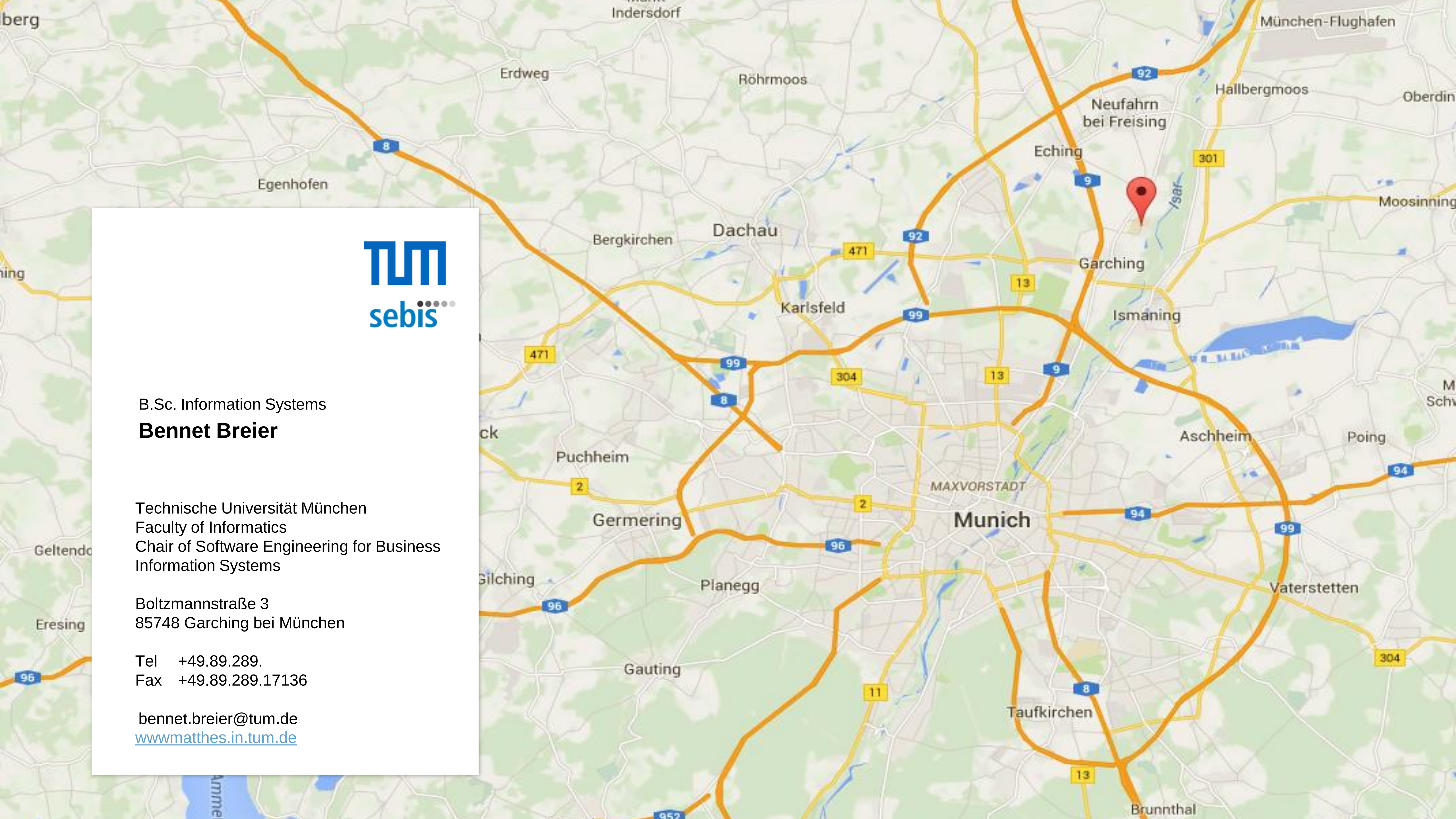
3. Proof of Work

Principle:	**Hashcash**
Hash function:	**Curl** (from the sponge family hash functions)



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

Appendix