Technical Analysis of Established Blockchain Systems

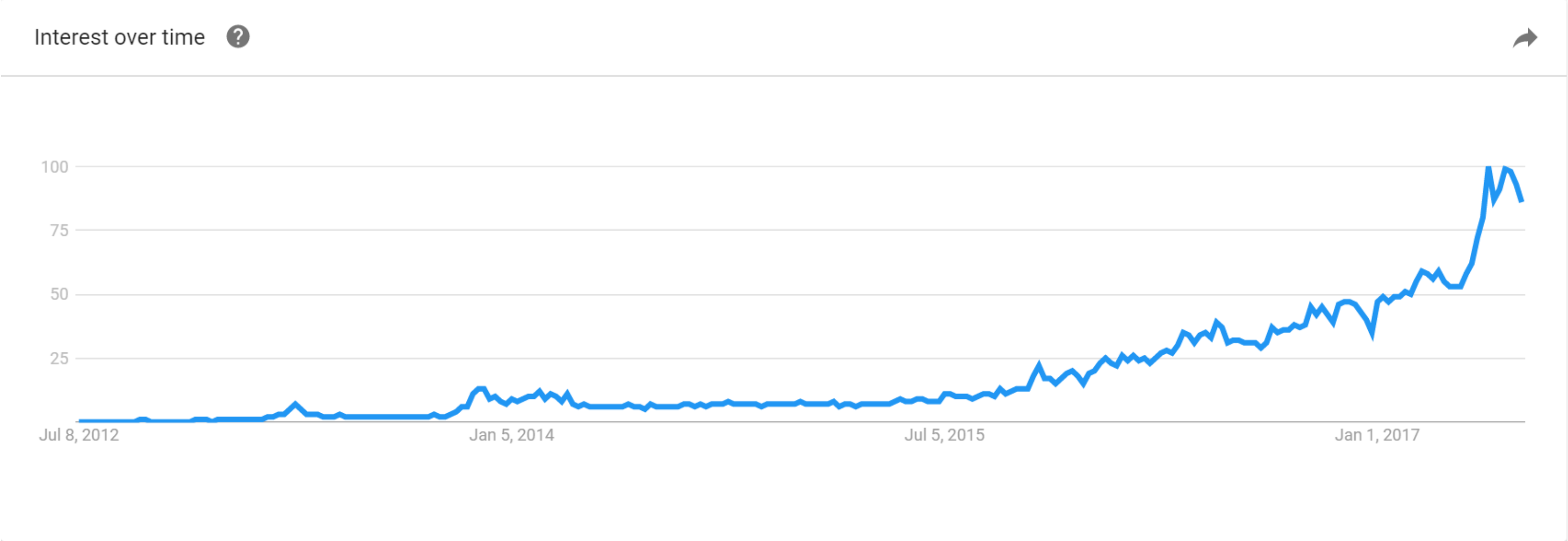
Florian Haffke, 10.07.2017, Munich

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

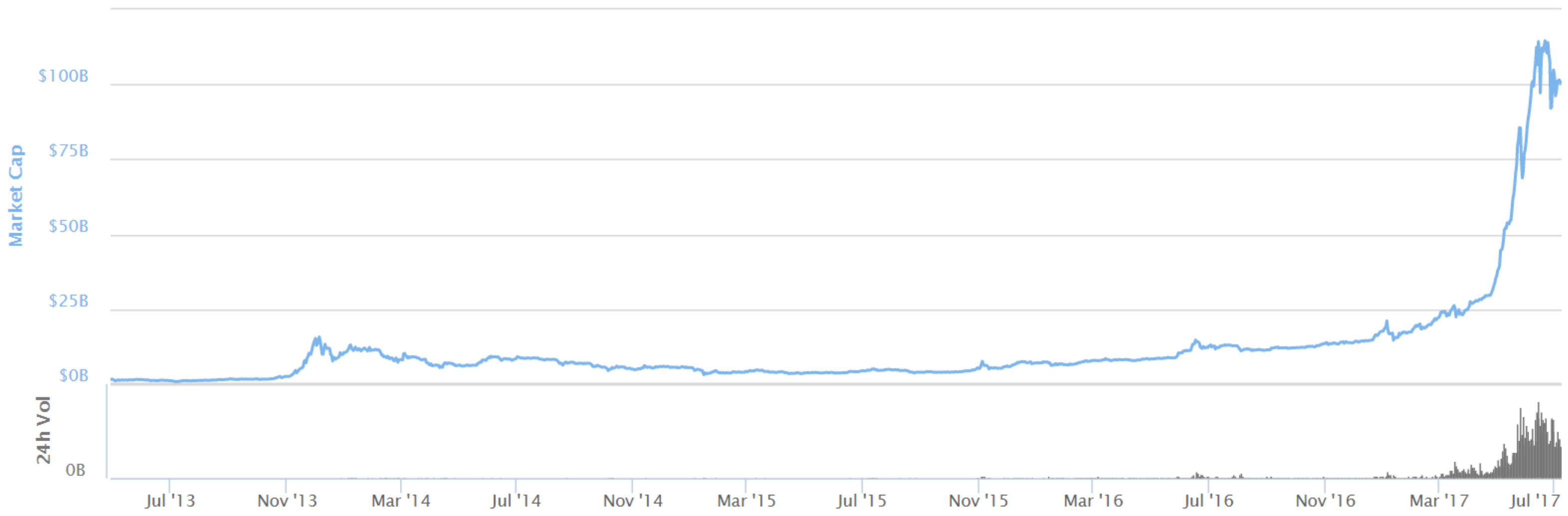
Outline

1. Motivation
2. Research Approach
3. Established Blockchain Systems
4. Research Questions & Timeline
5. Example Analysis

Motivation



GoogleSearch
Blockchain



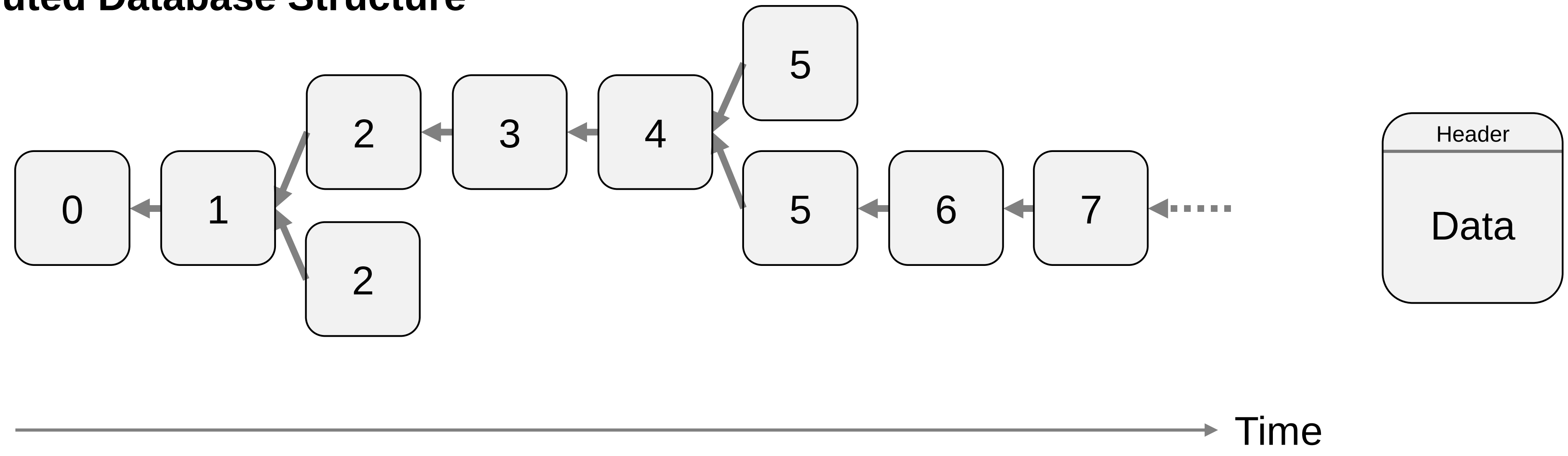
Total Market-Cap
Blockchains' Cryptocurrencies

bitcoin

Motivation

How to define the term Blockchain?

Distributed Database Structure



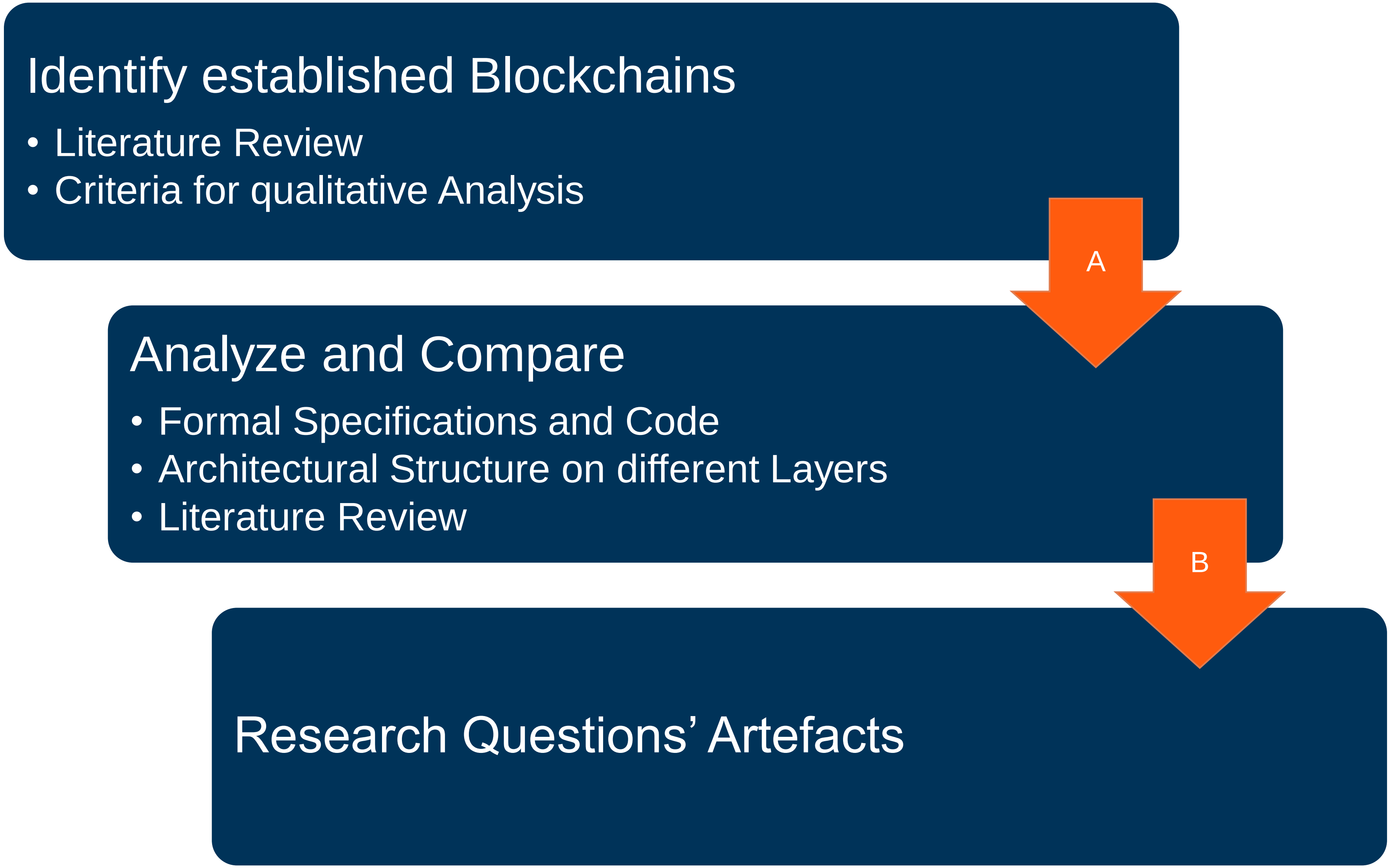
vs. The System

Coded Protocol on *P2P Network* specifying Layers’ communication

Outline

1. Motivation
2. Research Approach
3. Established Blockchain Systems
4. Research Questions & Timeline
5. Example Analysis

Research Approach



Identify established Blockchains

- Literature Review
- Criteria for qualitative Analysis

Analyze and Compare

- Formal Specifications and Code
- Architectural Structure on different Layers
- Literature Review

Research Questions’ Artefacts

Outline

1. Motivation
2. Research Approach
3. Established Blockchain Systems
4. Research Questions & Timeline
5. Example Analysis

Established Blockchain Systems

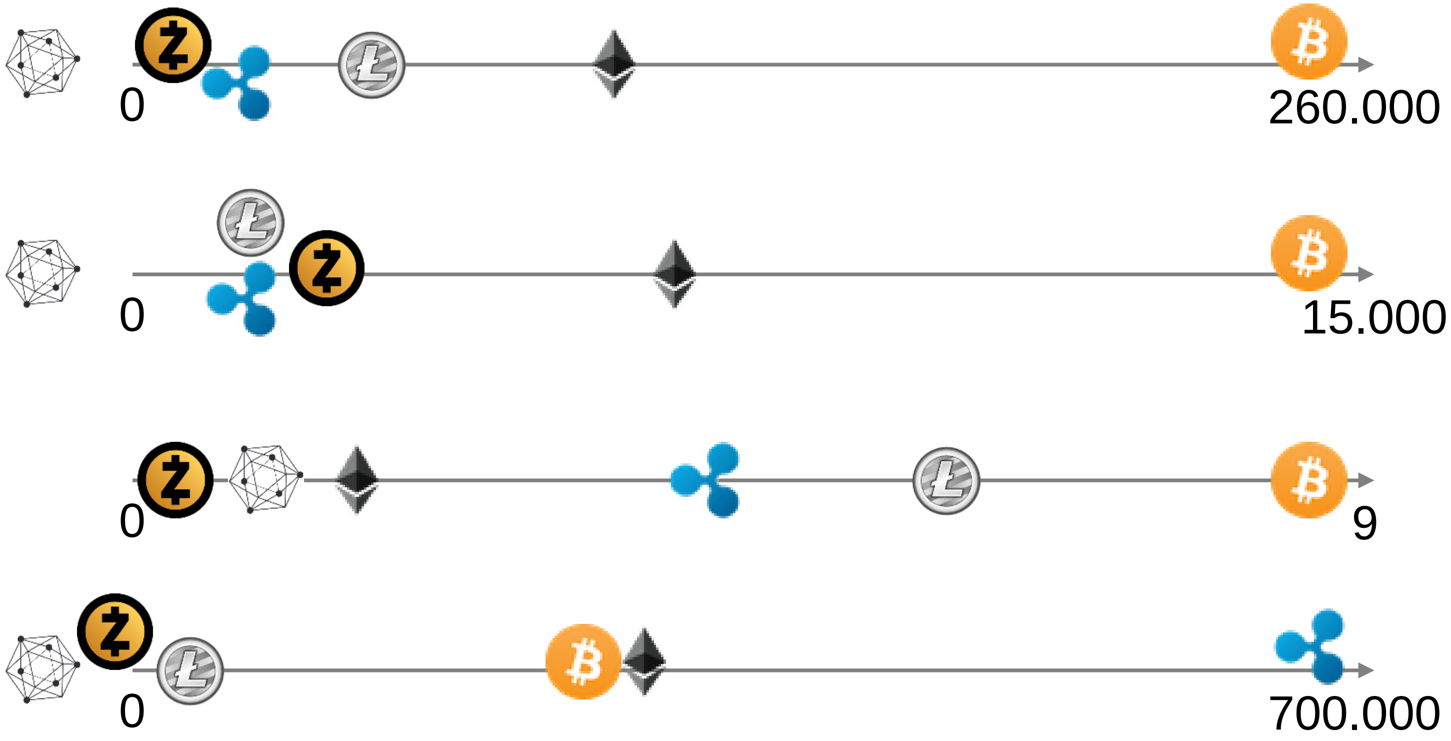
How to identify the most established Blockchains?

Criteria	Metric [Unit]
Supporting Community	*Reddit Subscribers [#]*
Development Support	*Activity in Public Source Code Repos [#]*
Longevity	*Age since Initial Release Date [Years]*
Network Activity	*Transactions [# per Day]*
Investor Evaluation	*Market cap of native currency [Bn$]*
Public Awareness and Interest	*Alexa Rank [#]*
Technical Uniqueness of Protocol	*Ordered Attribute Scale [1..5]*
Application Ecosystem	*Ordered Attribute Scale [1..5]*

Established Blockchain Systems

Relative Comparison

Criteria	Metric [Unit]
Supporting Community	*Reddit Subscribers [#]*
Development Support	*Activity in Public Source Code Repos [#]*
Longevity	*Age since Initial Release Date [Years]*
Network Activity	*Transactions [# per Day]*



Bitcoin

Ethereum

Ripple

Litecoin

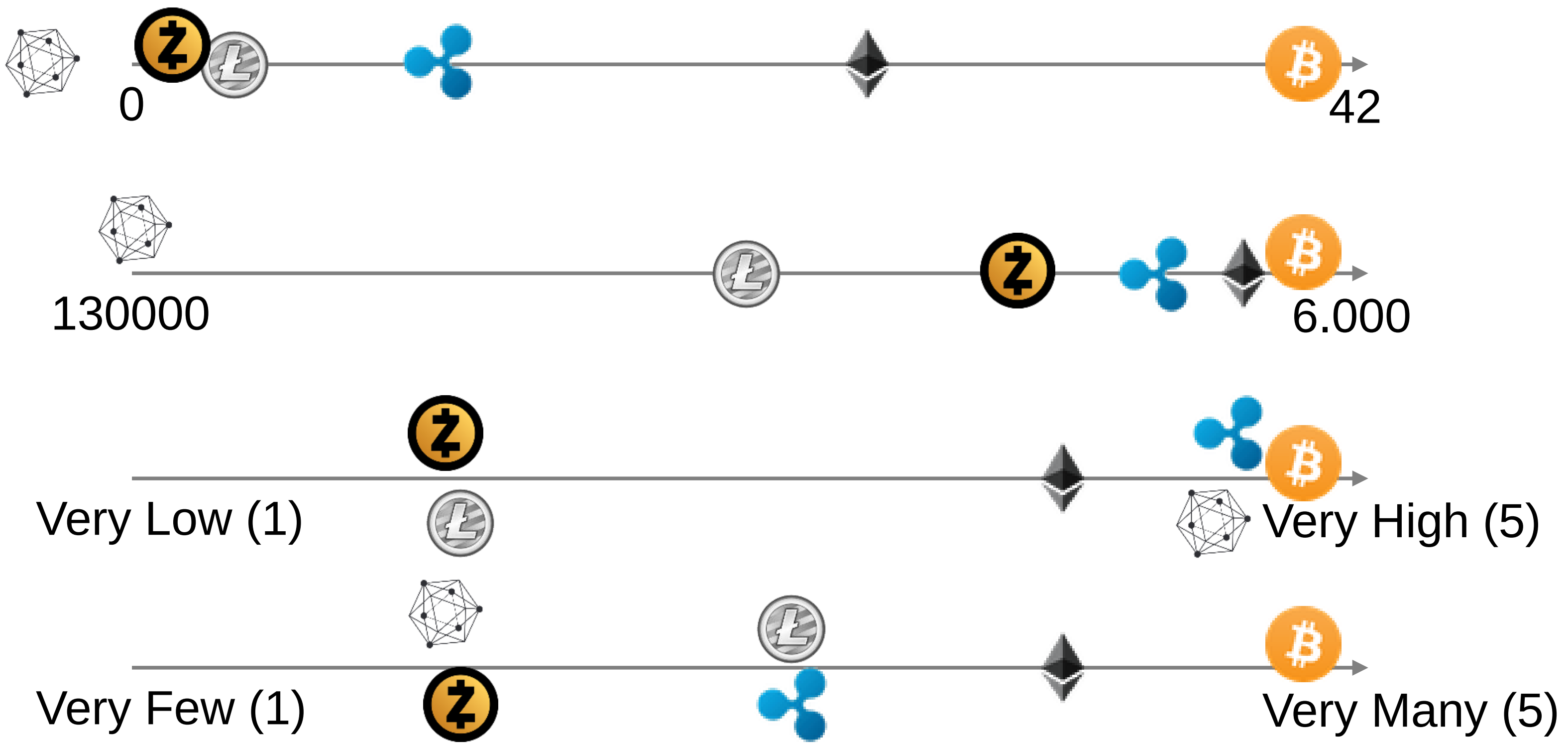
Hyperledger Project

Zcash

Established Blockchain Systems

Relative Comparison

Criteria	Metric [Unit]
Investor Evaluation	*Market cap of native currency [Bn$]*
Public Awareness and Interest	*Alexa Rank [#]*
Technical Uniqueness of Protocol	*Ordered Attribute Scale [1..5]*
Application Ecosystem	*Ordered Attribute Scale [1..5]*



Bitcoin Ethereum Ripple

Litecoin Hyperledger Project Zcash

Established Blockchain Systems

Further minor established Blockchains with unique Concepts

DASH

- Tiered P2P Network with **Masternodes**

Onmi Layer, Counterparty

- Bitcoin Extension Protocols

Monero

- Complete Privacy & Intransparency with **Ring Signatures**

Steemit

- Social Media Platform with **DPoS**

BitShares

- Asset Decentralisation with DPoS

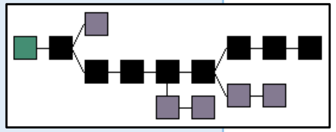
Outline

1. Motivation
2. Research Approach
3. Established Blockchain Systems
4. Research Questions & Timeline
5. Example Analysis

Research Questions and Approach

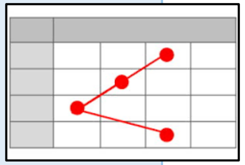
1. What are crucial Elements and Characteristics of all established Blockchains?

- Elements & Properties
- Conceptual High Level Model



2. How can a Design Space of Blockchains be defined?

- Morphological Analysis
- Common Patterns



Research Questions and Approach

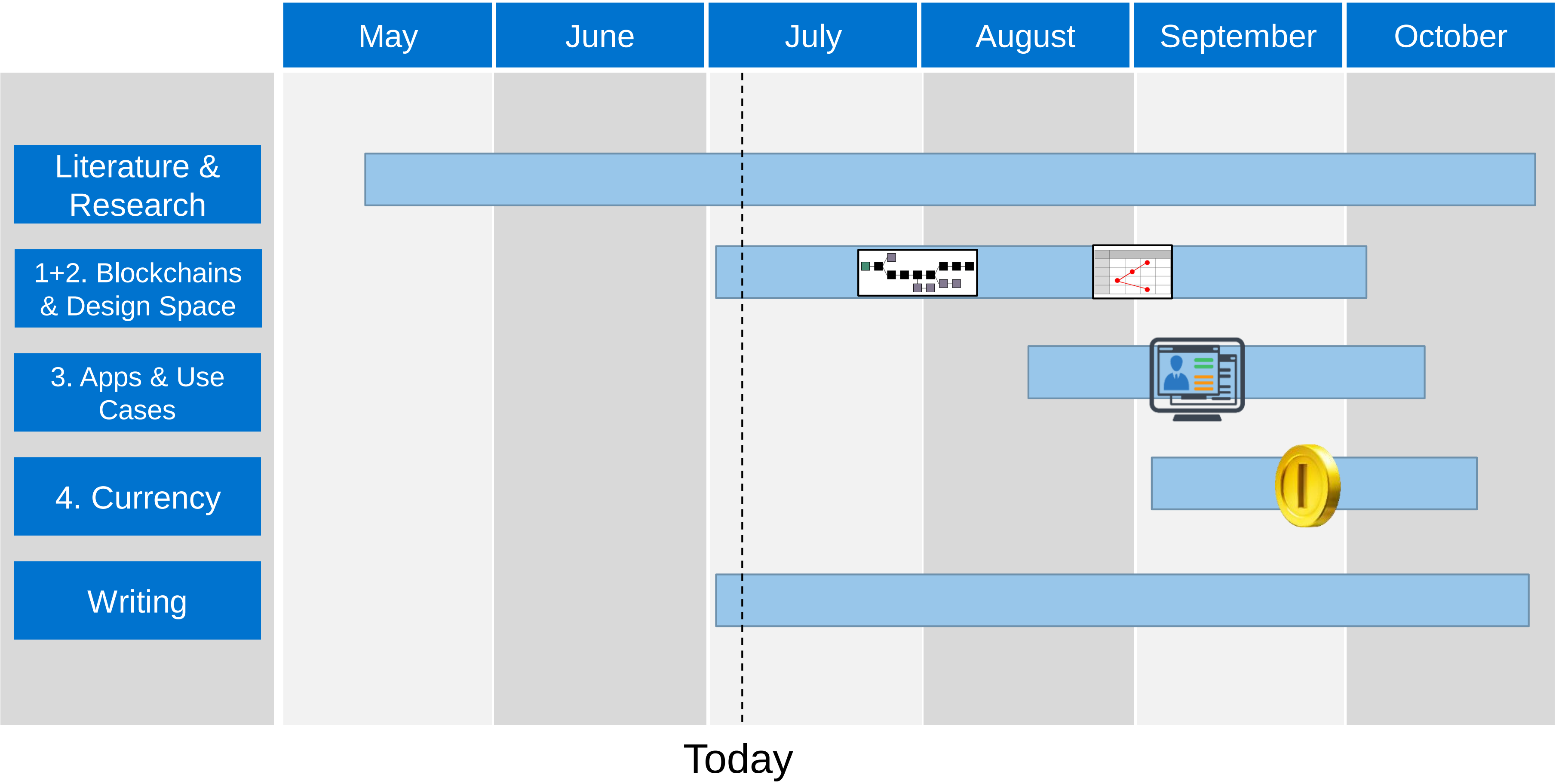
3. What are suitable Applications and Use Cases for Blockchain Systems?

- Archievements of Blockchains
- Requirements of Applications & Use Cases
- Disruptiveness of Blockchain
- Business Models

4. What Role does a native Currency have for its Blockchain?

- Game theoretical Analysis
- Implications for the Absence of a native Currency

Timeline



Official Start Date: 15.5.2017

Official End Date: 15.11.2017

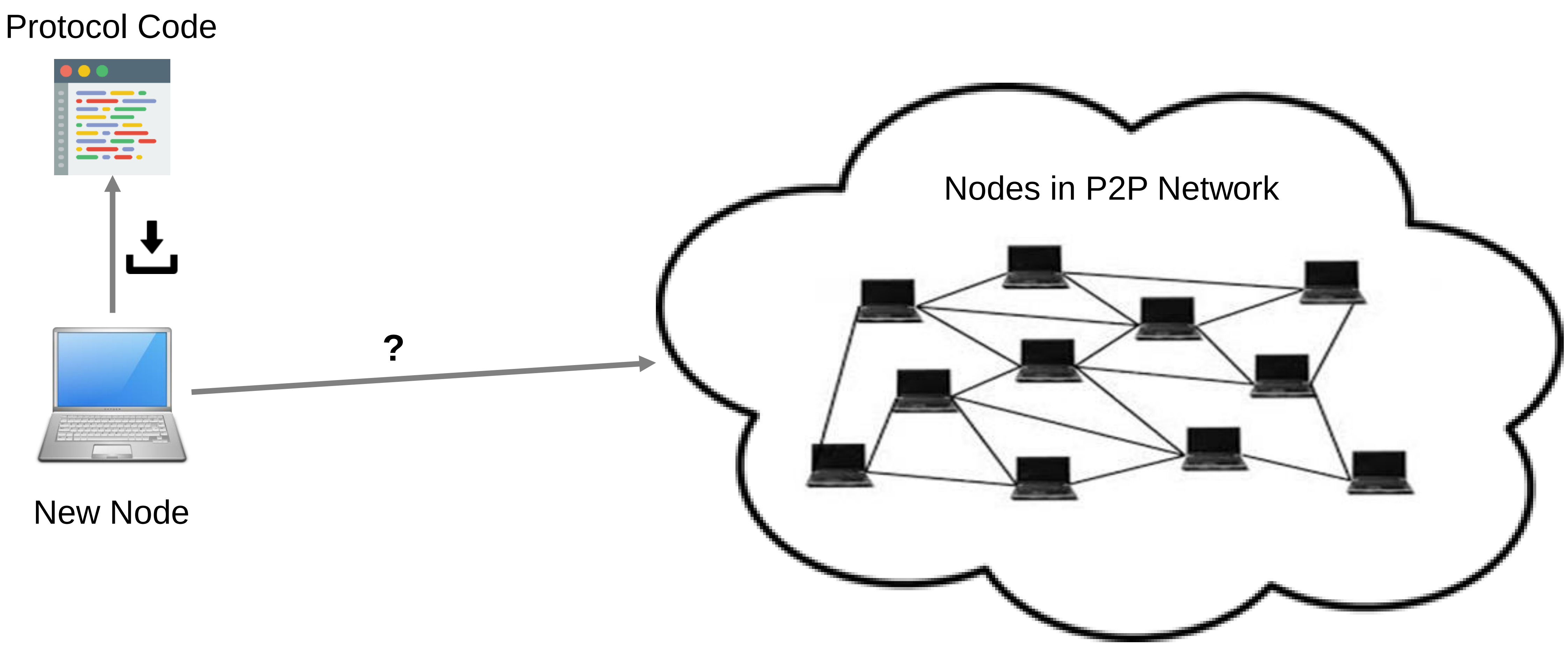
Supervisor: Patrick Holl

Outline

1. Motivation
2. Research Approach
3. Established Blockchain Systems
4. Research Questions & Timeline
5. Example Analysis

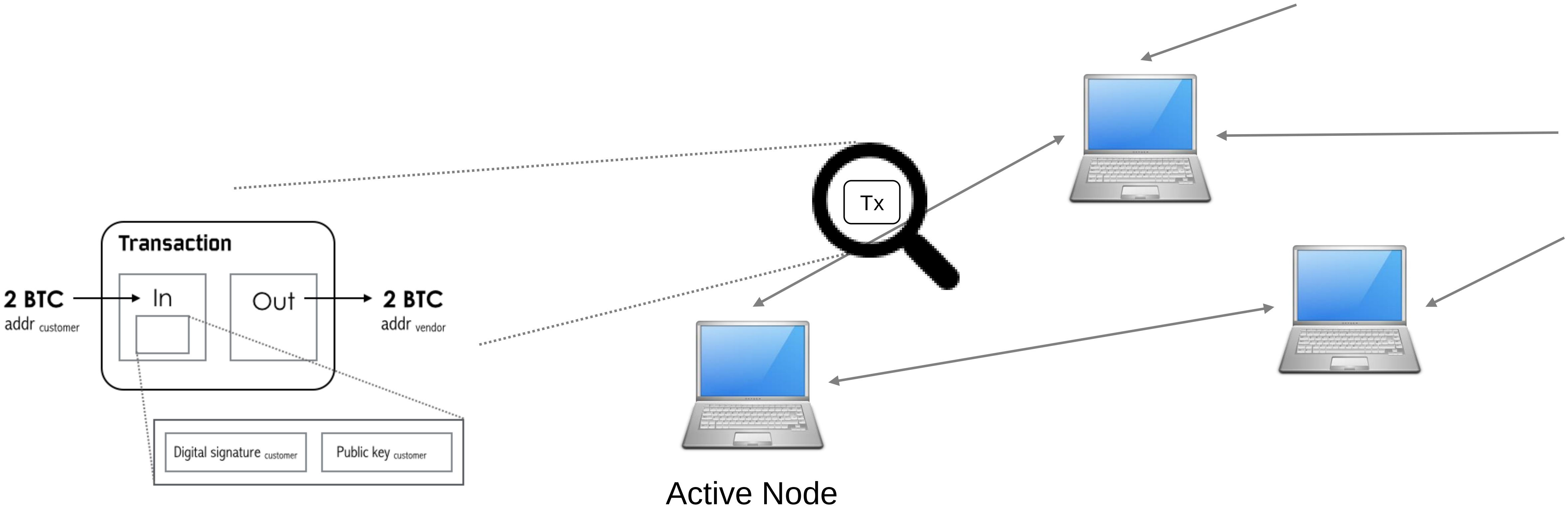
Example Analysis Process

The Bitcoin Protocol in 3 Slides – Joining and Leaving the Network



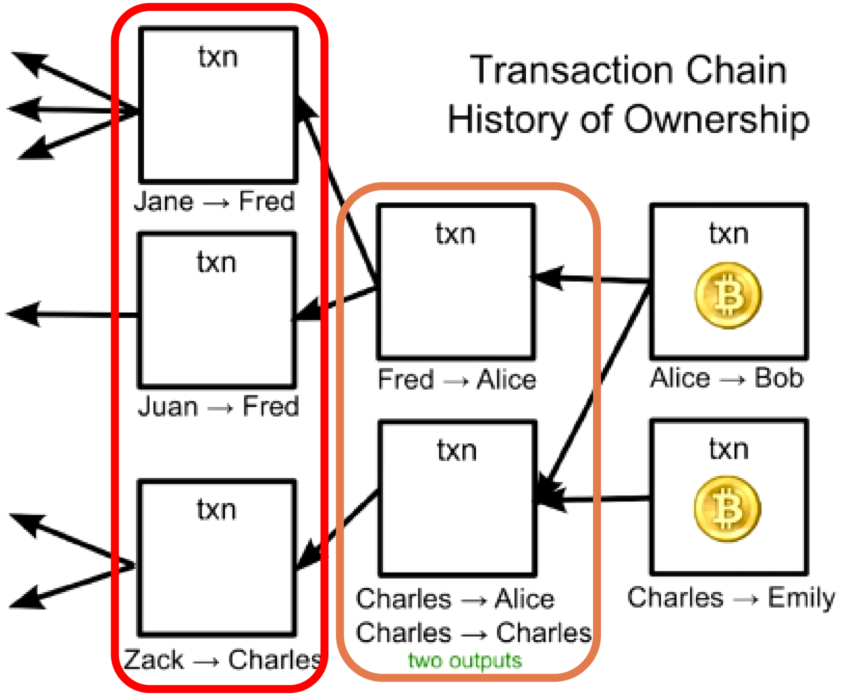
Example Analysis Process

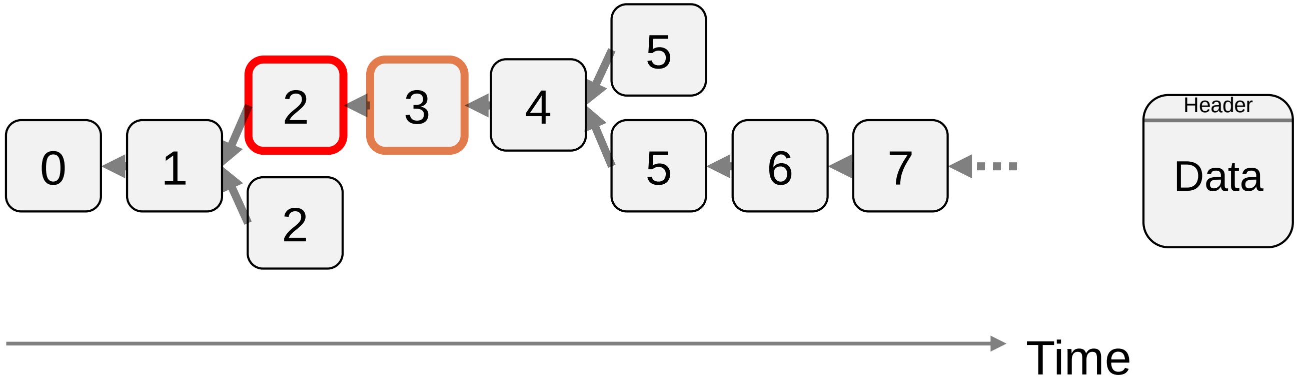
The Bitcoin Protocol in 3 Slides – Data Propagation



Example Analysis Process

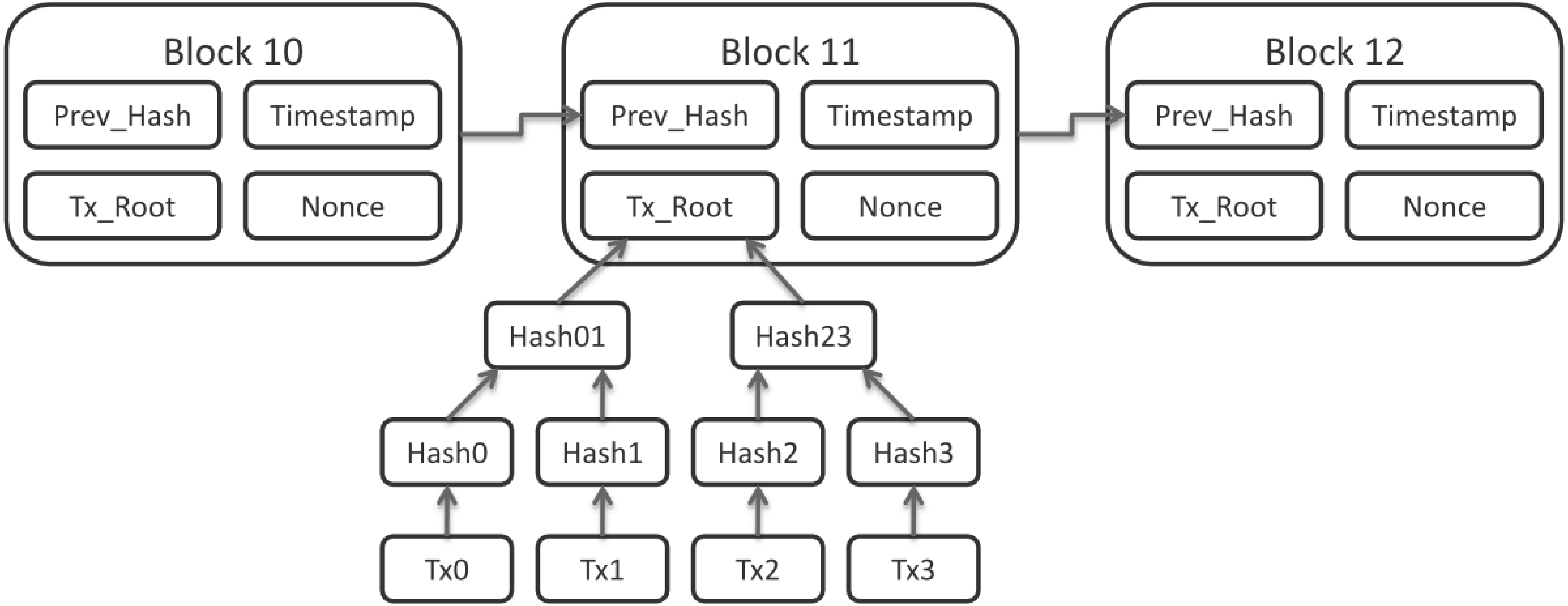
The Bitcoin Protocol in 3 Slides – Transaction Graph





Example Analysis Process

The Bitcoin Protocol in 3 Slides – Consensus Algorithm: Proof of Work



Example Analysis Process

The Ripple Consensus Algorithm (RPCA) vs. Bitcoins’ PoW

RPCA main Differences to PoW

10s Round based

- 2s Window to compare List of collected Txn = Candidate Set
- *Repeat if* **>80%** of Nodes have same Candidate Set
  - *then* finalize Consensus and create Block
  - *else* add missing Txn to Candidate Set

P2P Network permissioned with **Whitelist** of Banks and Gateways

Trustlines with Balance-based IOU Assets, like $ or €

Problem Cases

Without Consensus the Protocol falls into infinity loop

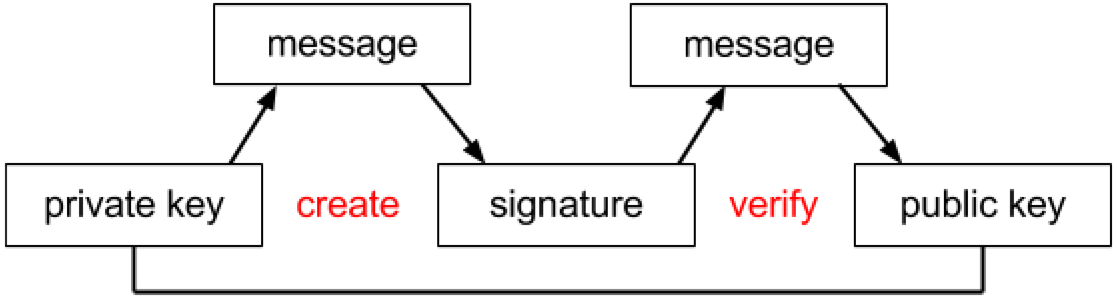
Bitcoins’ PoW would fork the chain with different Consensuses

Example Analysis Process

Bitcoins’ Address System vs. Ethereums’ Account Balances

Bitcoins’ Address System

- Trapdoor Function
- Elliptic Curve Digital Signature Algorithm
- Human used
- Public Key serves as Address



Example *Private* Key: L1aW4aubDFB7yfras2S1mN3bqg9nwySY8nkoLmJebSLD5BWv3ENZ

Corresponding *Public* Key: 1HgiEYL6fsKrfh8wuMhAGfvSc6PY5ZXJdv

Ethereums’ Account Balances

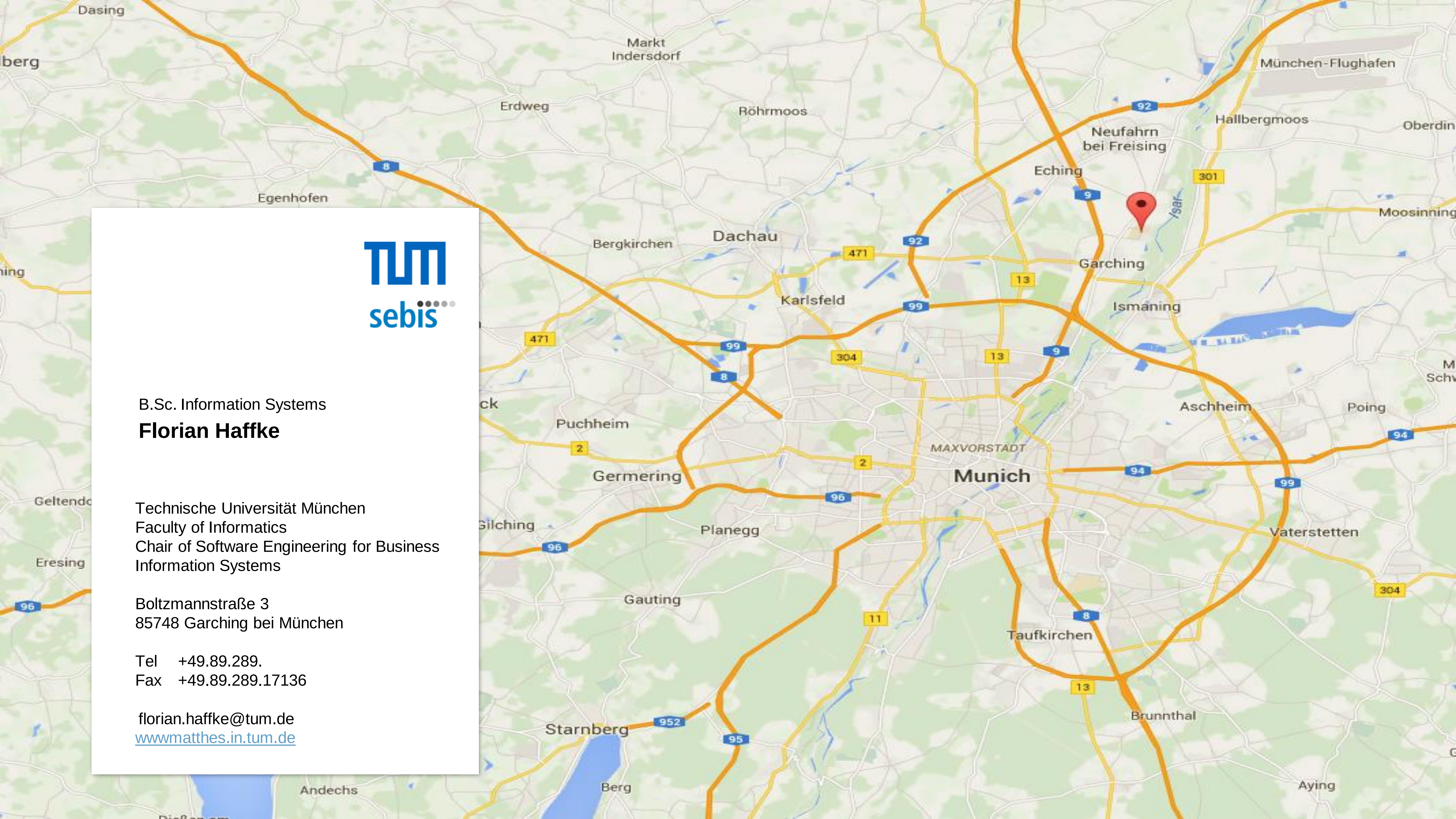
- Similar to Bitcoin, but *Account Objects* are stored in Blockchain
- Either Human used
- Or Smart Contracts
  - Persistent Variables in Key/Value Store
- Quasi Turing Complete instead of Stack-based

Account

• Address
• Ether Balance
? Contract Code
? Storage
• Nonce

Thanks for your Attention

Please provide Input and Feedback! ☺



B.Sc. Information Systems

Florian Haffke

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

florian.haffke@tum.de
wwwmatthes.in.tum.de

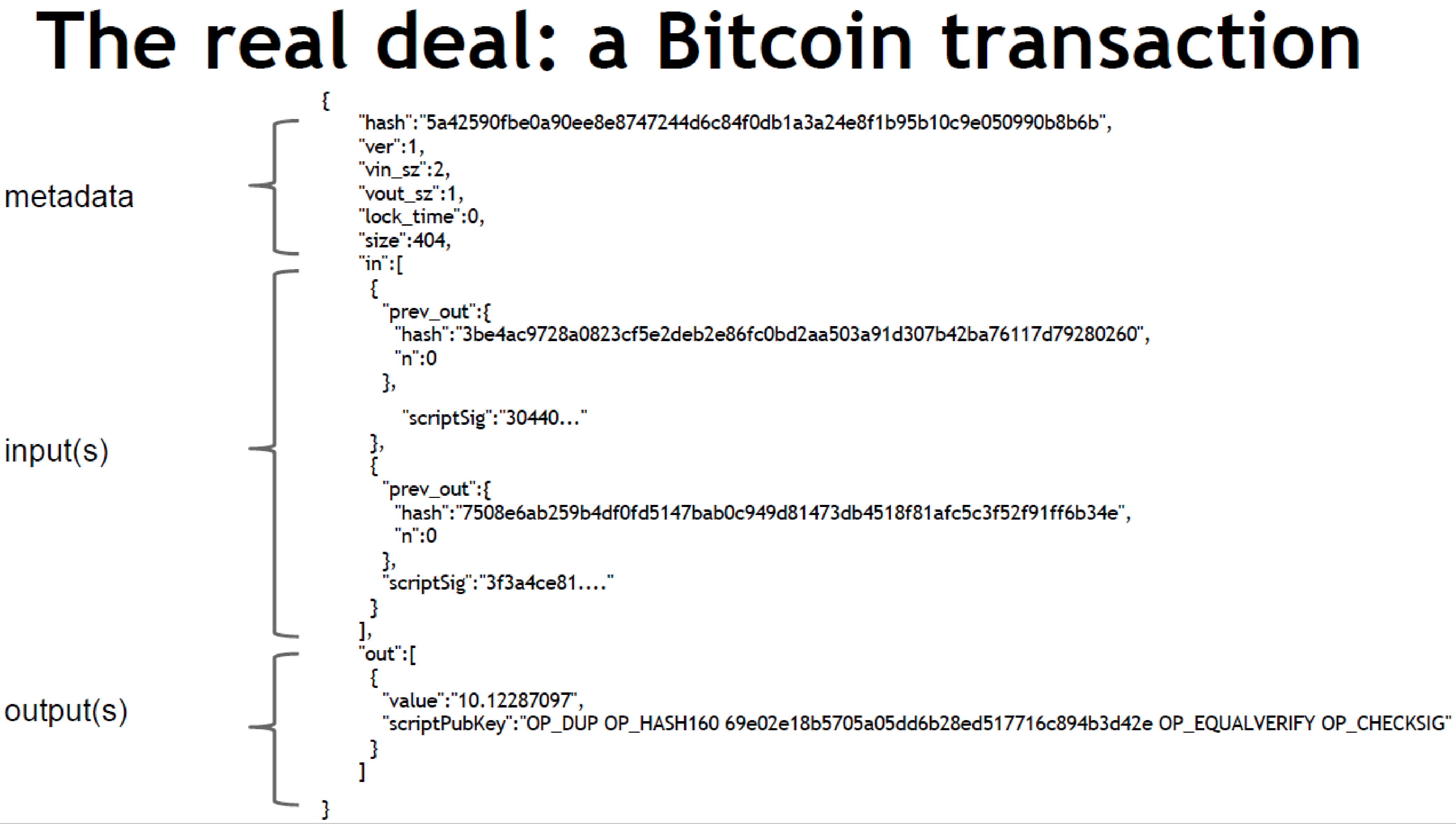
Appendix

Established Blockchain Systems

How to identify the most established Blockchains? – Data Snapshot

Criteria	Metric [Unit]	Bitcoin	Litecoin	Ethereum	Hyperledger Project	Ripple	Zcash
Supporting Community	*Reddit Subscribers [#]*	255.744	39.602	85.636	--- Linux Foundation, IBM	14.882	3459
Development Support	*Activity in Public Source Code Repos [#]*	14.090	1.484	5.671	--- Linux Foundation, IBM	1.428	2556
Longevity	*Age since Initial Release Date [Years]*	01-200 (8,5)	10-2011 (6)	07-2015 (2)	12-2015 (1,5)	10-2012 (4,5)	10-2016 (1)
Network Activity	*Transactions [# per Day]*	212.140	17.300	248.060	---	665.304	---
Investor Evaluation	*Market cap of native currency [Bn$]*	42	2,5	25	---	10	0,4
Public Awareness and Interest	*Alexa Rank [#]*	6.880	62.478	7.156	128.476	12.697	20.214
Technical	*Ordered*	Very High,	Low,	High, Parts of	Very High,	Very High,	Low,

Transaction Structure



The real deal: a Bitcoin transaction

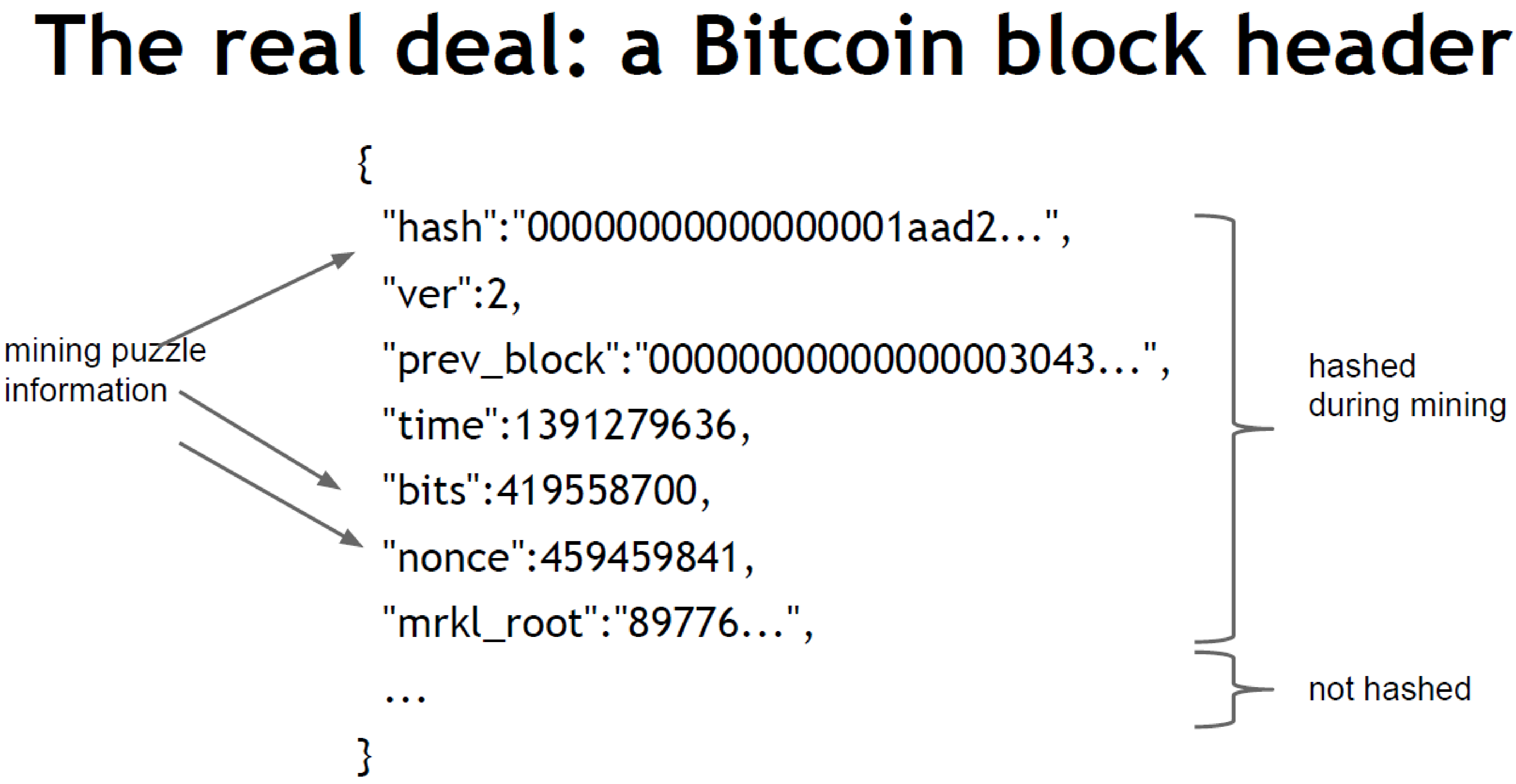
metadata

input(s)

output(s)

```
{
    "hash":"5a42590fbe0a90ee8e8747244d6c84f0db1a3a24e8f1b95b10c9e050990b8b6b",
    "ver":1,
    "vin_sz":2,
    "vout_sz":1,
    "lock_time":0,
    "size":404,
    "in":[
     {
       "prev_out":{
         "hash":"3be4ac9728a0823cf5e2deb2e86fc0bd2aa503a91d307b42ba76117d79280260",
         "n":0
       },
         "scriptSig":"30440..."
     },
     {
       "prev_out":{
         "hash":"7508e6ab259b4df0fd5147bab0c949d81473db4518f81afc5c3f52f91ff6b34e",
         "n":0
       },
       "scriptSig":"3f3a4ce81...."
     }
    ],
    "out":[
     {
       "value":"10.12287097",
       "scriptPubKey":"OP_DUP OP_HASH160 69e02e18b5705a05dd6b28ed517716c894b3d42e OP_EQUALVERIFY OP_CHECKSIG"
     }
    ]
}
```

Block Header Structure



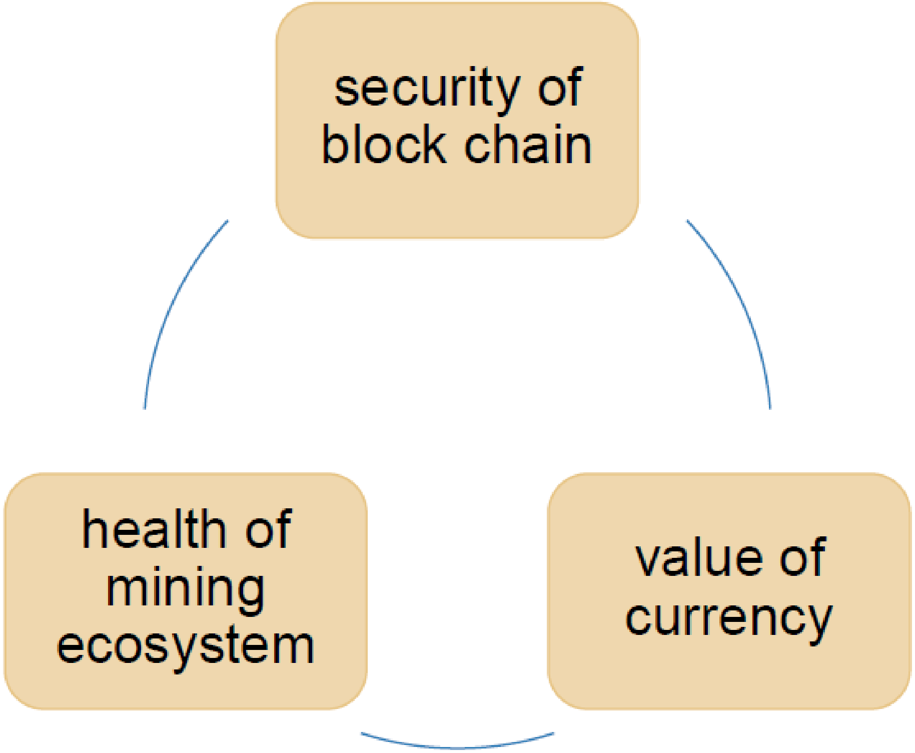
The real deal: a Bitcoin block header

```
{
  "hash":"0000000000000001aad2...",
  "ver":2,
  "prev_block":"0000000000000003043...",
  "time":1391279636,
  "bits":419558700,
  "nonce":459459841,
  "mrkl_root":"89776...",
  ...
}
```

mining puzzle information
hashed during mining
not hashed

Block Header Structure

Bitcoin is bootstrapped



security of block chain

value of currency

health of mining ecosystem