Technical Analysis of Established Blockchain Systems

Florian Haffke, 20.11.2017, Munich

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

Outline

1. Research Questions
2. Blockchain Basics
3. Wrap-up Bitcoin, Ethereum and Ripple
4. Analysis Extract – High-level and Design Space

Research Questions

1. **Which** are established Blockchain Systems?

2. What is the respective **Setup** of established Blockchain Systems?

3. How do established Blockchain Systems **differ**?

4. What are **crucial** Components and Characteristics of all established Blockchain Systems?

5. How can a **Design Space** of Blockchain Systems be defined?

Research Questions

1. **Which** are established Blockchain Systems?

2. What is the respective **Setup** of established Blockchain Systems?

3. How do established Blockchain Systems **differ**?

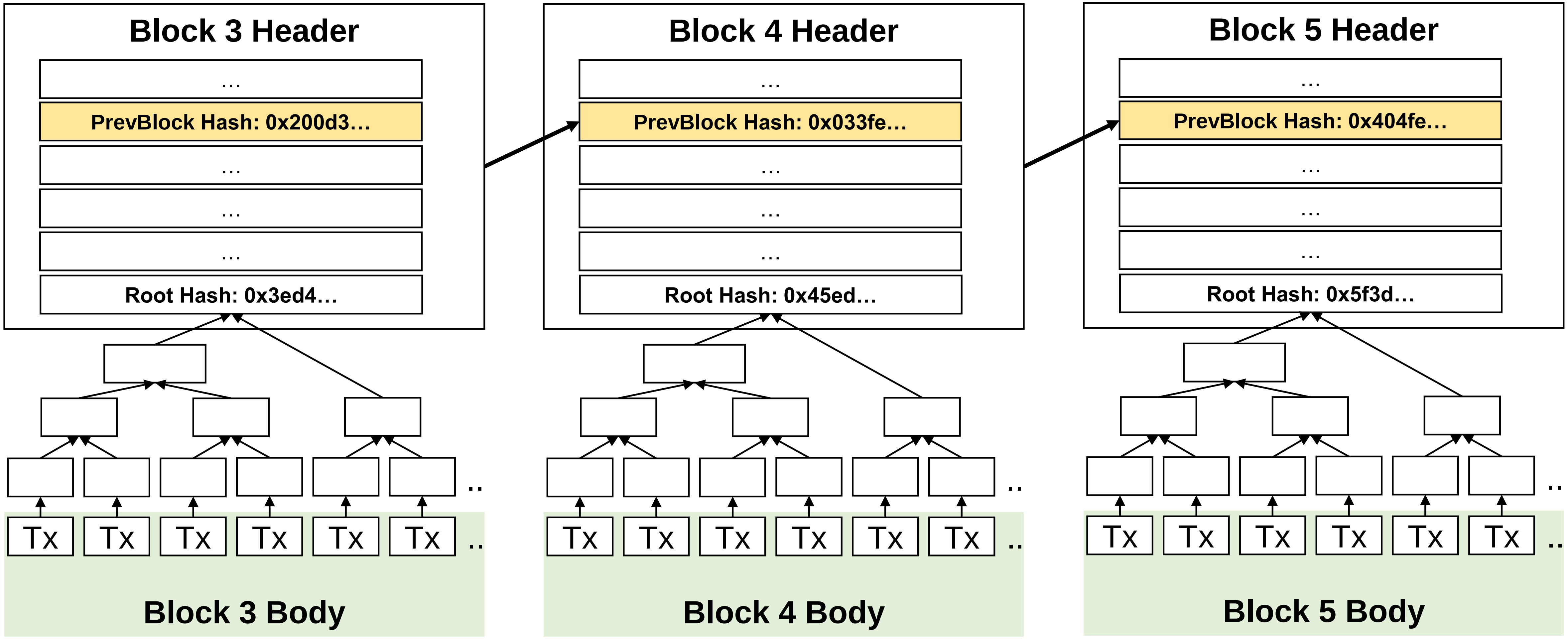
4. What are **crucial** Components and Characteristics of all established Blockchain Systems?

5. How can a **Design Space** of Blockchain Systems be defined?

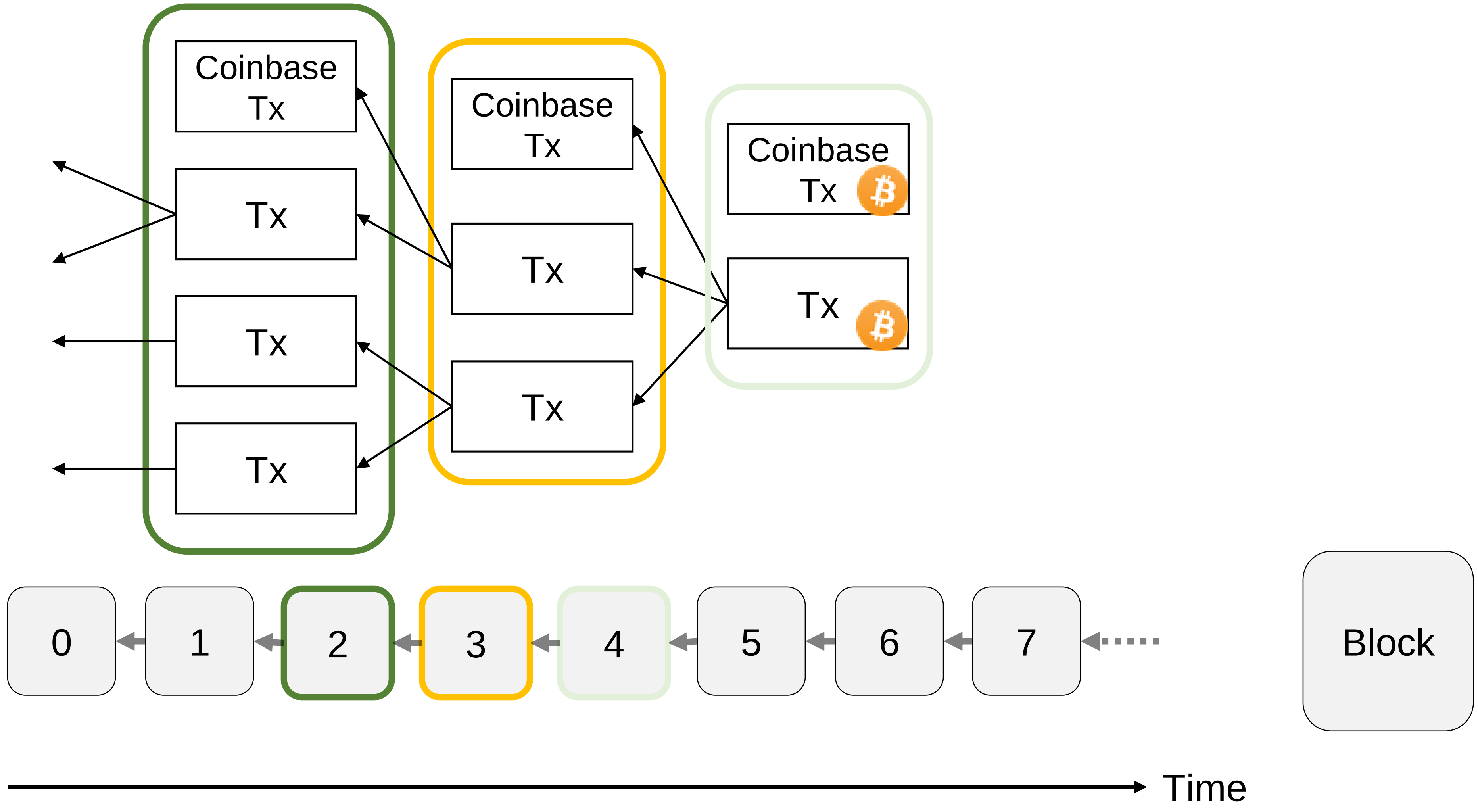
Outline

1. Research Questions
2. Blockchain Basics
3. Wrap-up Bitcoin, Ethereum and Ripple
4. Analysis Extract – High-level and Design Space

Chaining of Blocks



Transactions Graph



Outline

1. Research Questions
2. Blockchain Basics
3. Wrap-up Bitcoin, Ethereum and Ripple
4. Analysis Extract – High-level and Design Space

Goals

Bitcoin

Trustless and anonymous peer-to-peer electronic cash system

Ethereum

General-purpose platform for building transaction-based state machines

Ripple

One global connected payment network for cheaper and faster settlements

Blockchains

Tamper-resistant blocks with non-reversible transactions

1. Setup: State Data

Set of Unspent-Transactions-Outputs (*UTXOs*)

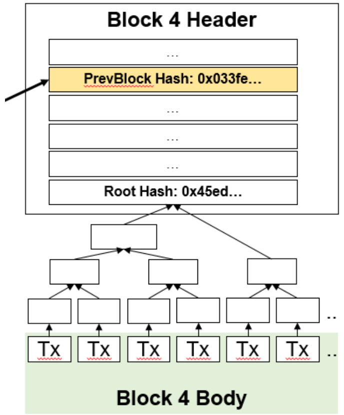
Mapping of *account* objects comprising balance and key-value storage to addresses

Concatenation of single *account* ledgers comprising balance and address

2. Setup: Consensus and Transitions

Proof of Work mining race

Stack-based script execution binding transactions



Proof of Work mining race

Smart contract execution in Ethereum Virtual Machine

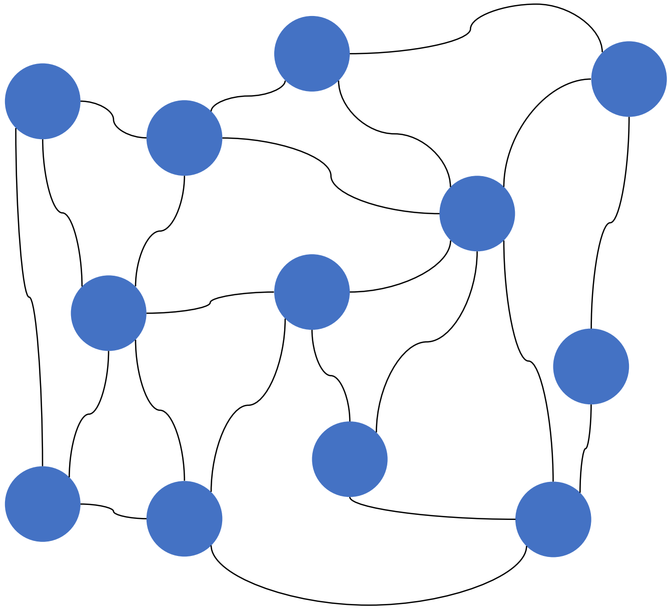
Proof of Correctness without mining rewards

Trivially updating account ledger value

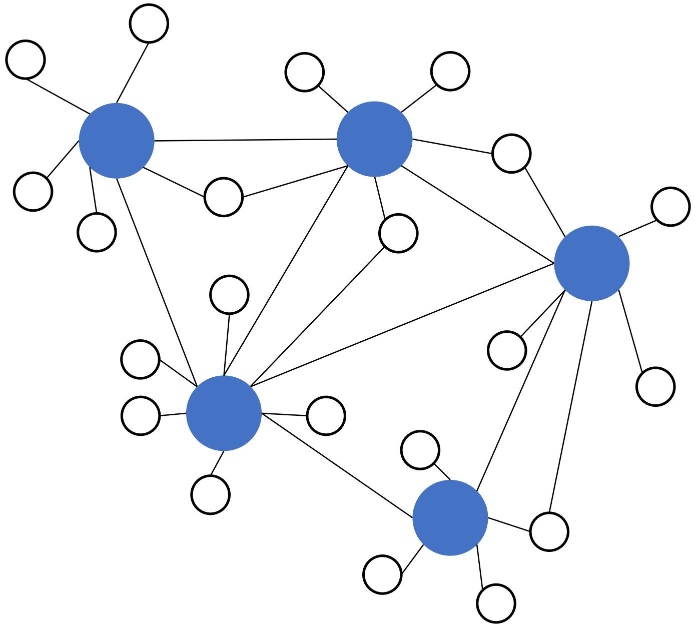
State transitions are triggered by transactions and finalized in a new block under distributed consensus.

Every valid block alters the state deterministically.

3. Setup: Peer-to-Peer Network



Distributed



Decentralized

● Full Node/Validator

○ Client Node

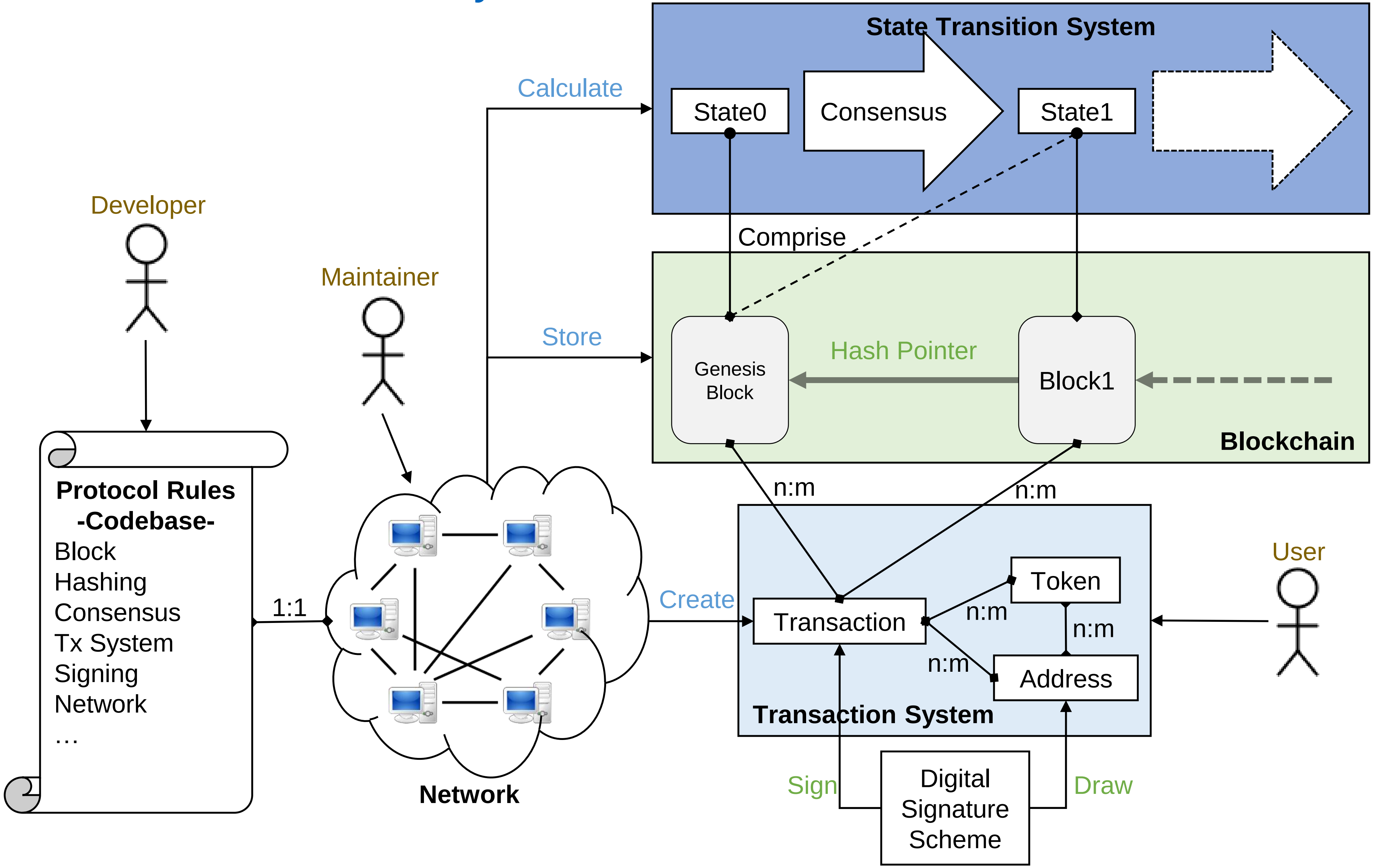
— UNL Connection

∫ Semi-random Connection

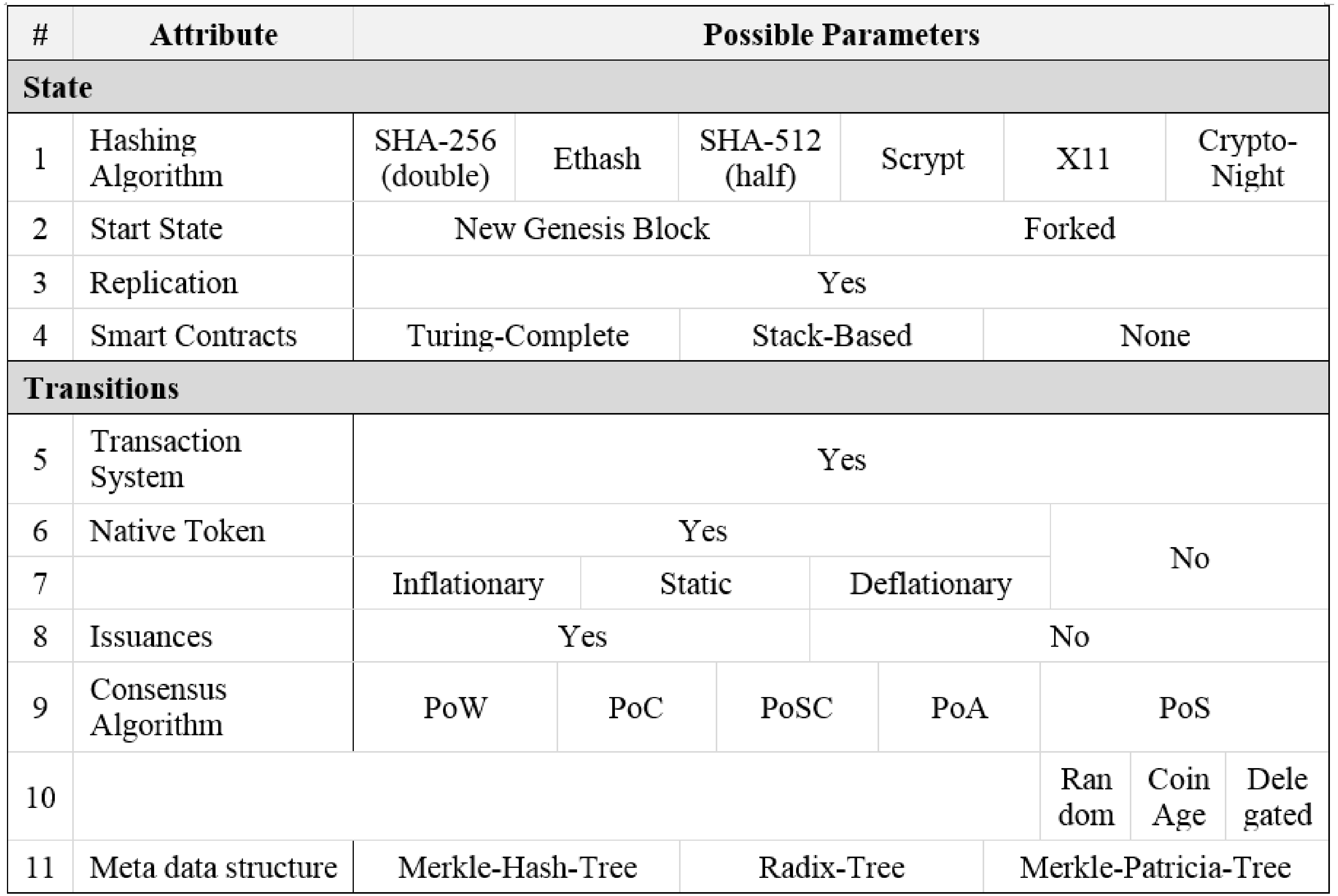
Outline

1. Research Questions
2. Blockchain Basics
3. Wrap-up Bitcoin, Ethereum and Ripple
4. Analysis Extract – High-level and Design Space

A Generic View of Blockchain Systems

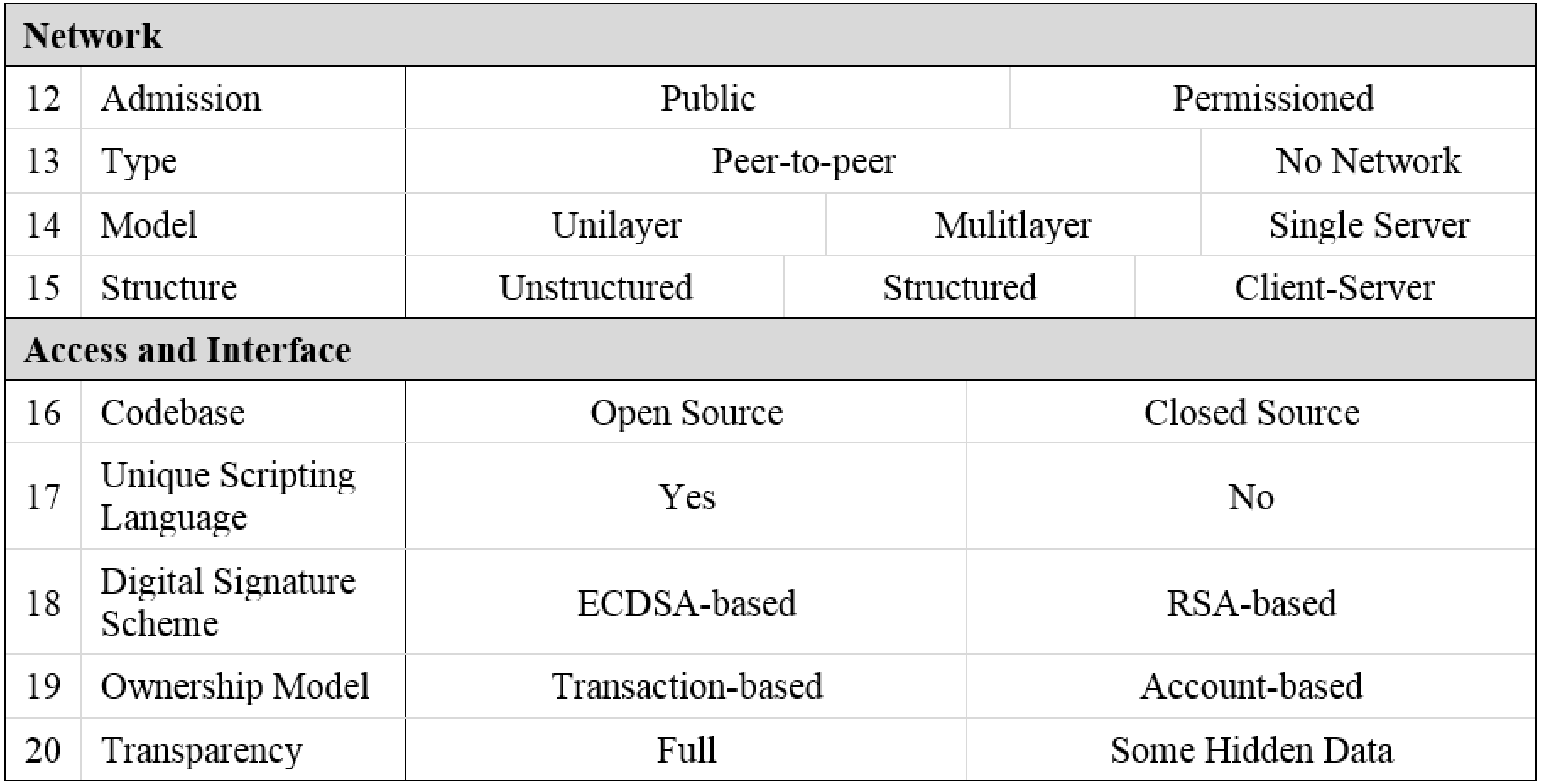


Morphology Part 1



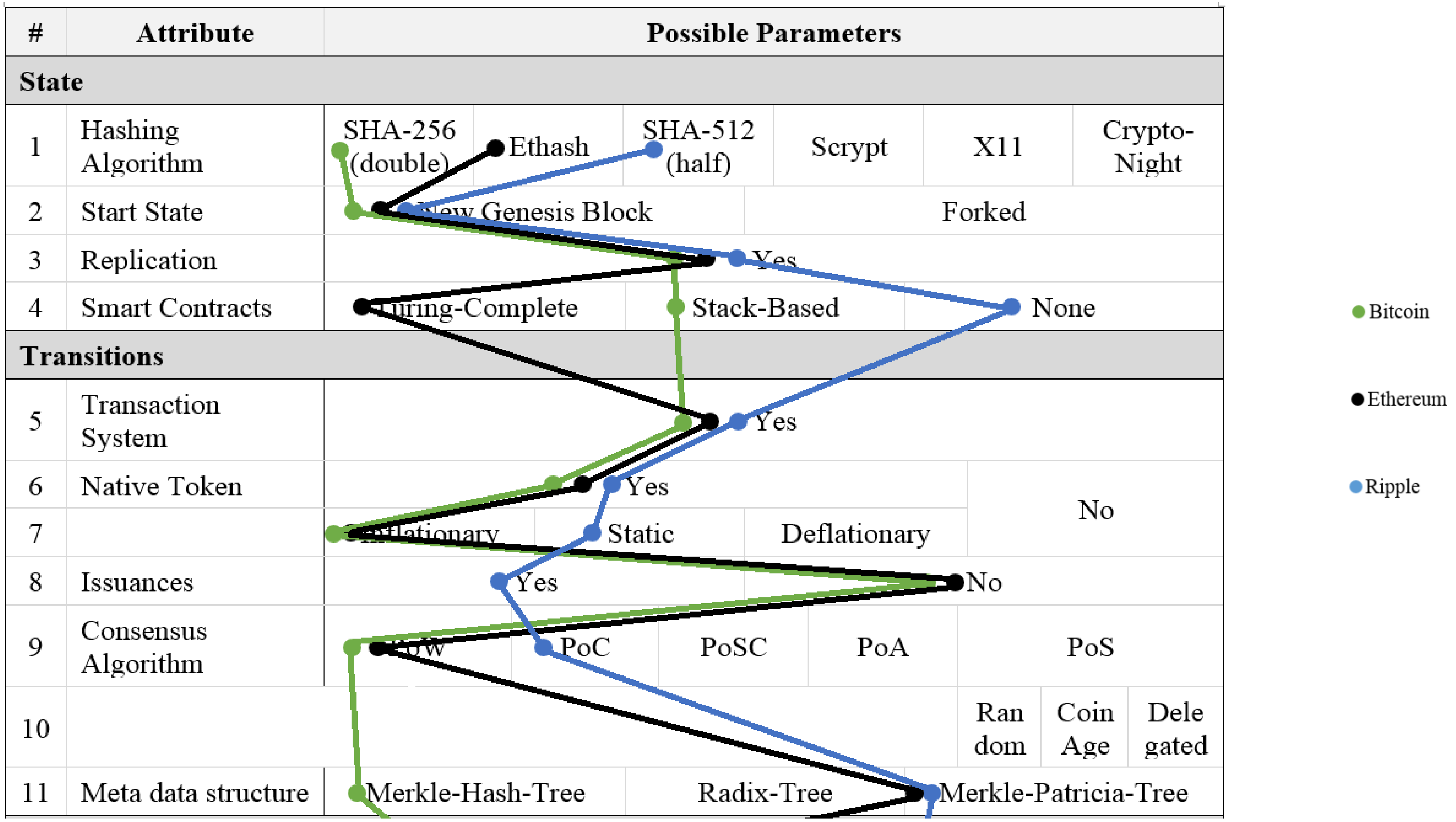
<table>
<tr><th>#</th><th>Attribute</th><th colspan="16">Possible Parameters</th></tr>
<tr><td colspan="18"><b>State</b></td></tr>
<tr><td>1</td><td>Hashing Algorithm</td><td>SHA-256 (double)</td><td colspan="3">Ethash</td><td colspan="3">SHA-512 (half)</td><td colspan="3">Scrypt</td><td colspan="4">X11</td><td colspan="2">Crypto-Night</td></tr>
<tr><td>2</td><td>Start State</td><td colspan="6">New Genesis Block</td><td colspan="10">Forked</td></tr>
<tr><td>3</td><td>Replication</td><td colspan="16">Yes</td></tr>
<tr><td>4</td><td>Smart Contracts</td><td colspan="4">Turing-Complete</td><td colspan="5">Stack-Based</td><td colspan="7">None</td></tr>
<tr><td colspan="18"><b>Transitions</b></td></tr>
<tr><td>5</td><td>Transaction System</td><td colspan="16">Yes</td></tr>
<tr><td>6</td><td>Native Token</td><td colspan="12">Yes</td><td colspan="4" rowspan="2">No</td></tr>
<tr><td>7</td><td></td><td colspan="3">Inflationary</td><td colspan="3">Static</td><td colspan="6">Deflationary</td></tr>
<tr><td>8</td><td>Issuances</td><td colspan="6">Yes</td><td colspan="10">No</td></tr>
<tr><td>9</td><td>Consensus Algorithm</td><td colspan="2">PoW</td><td colspan="3">PoC</td><td colspan="3">PoSC</td><td colspan="3">PoA</td><td colspan="5">PoS</td></tr>
<tr><td>10</td><td colspan="12"></td><td colspan="2">Random</td><td colspan="2">Coin Age</td><td>Delegated</td></tr>
<tr><td>11</td><td>Meta data structure</td><td colspan="4">Merkle-Hash-Tree</td><td colspan="5">Radix-Tree</td><td colspan="7">Merkle-Patricia-Tree</td></tr>
</table>

Morphology Part 2



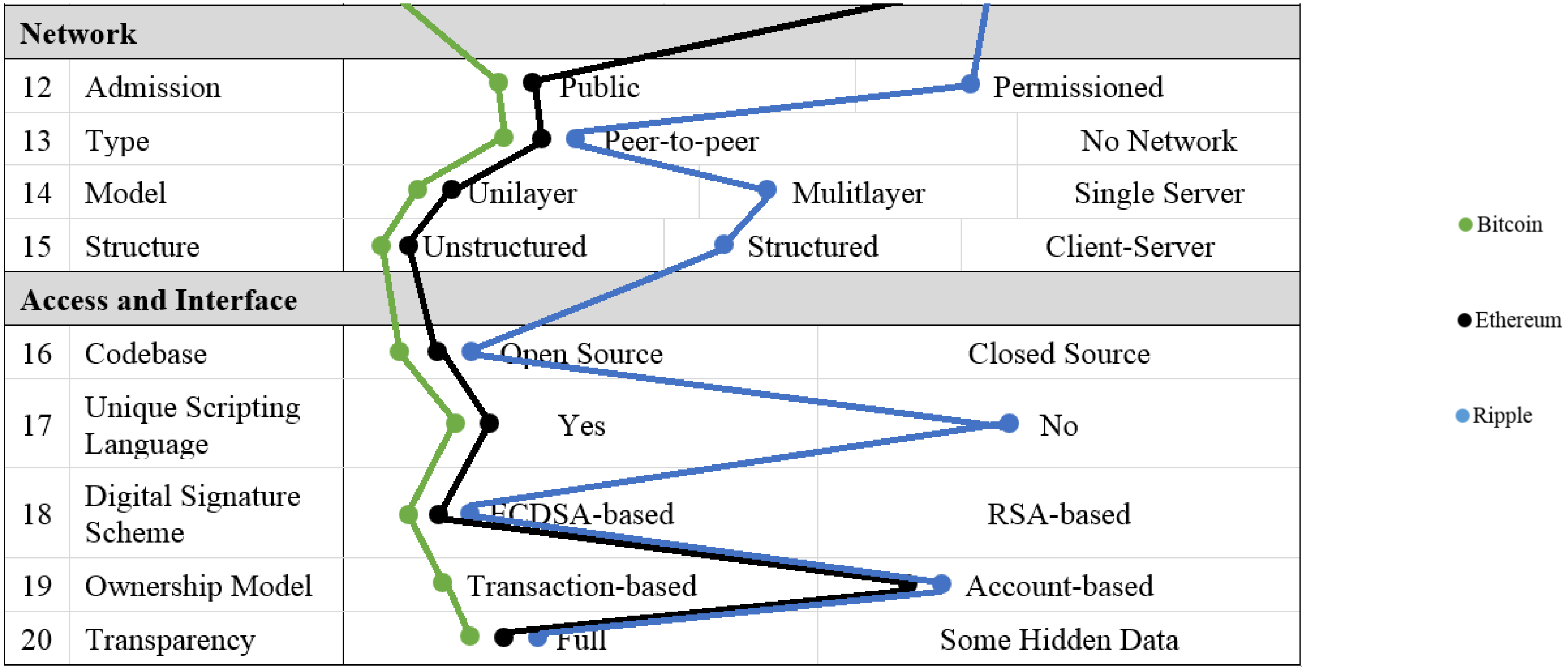
Network				
12	Admission	Public	Permissioned	
13	Type	Peer-to-peer	No Network	
14	Model	Unilayer	Mulitlayer	Single Server
15	Structure	Unstructured	Structured	Client-Server
Access and Interface				
16	Codebase	Open Source	Closed Source	
17	Unique Scripting Language	Yes	No	
18	Digital Signature Scheme	ECDSA-based	RSA-based	
19	Ownership Model	Transaction-based	Account-based	
20	Transparency	Full	Some Hidden Data	

Classification Part 1



#	Attribute	Possible Parameters						
State								
1	Hashing Algorithm	SHA-256 (double)	Ethash	SHA-512 (half)	Scrypt	X11	Crypto-Night	
2	Start State	New Genesis Block			Forked			
3	Replication	Yes						
4	Smart Contracts	Turing-Complete		Stack-Based		None		
Transitions								
5	Transaction System	Yes						
6	Native Token	Yes				No		
7		Inflationary	Static	Deflationary				
8	Issuances	Yes			No			
9	Consensus Algorithm	PoW	PoC	PoSC	PoA	PoS		
10						Ran dom	Coin Age	Dele gated
11	Meta data structure	Merkle-Hash-Tree		Radix-Tree		Merkle-Patricia-Tree		

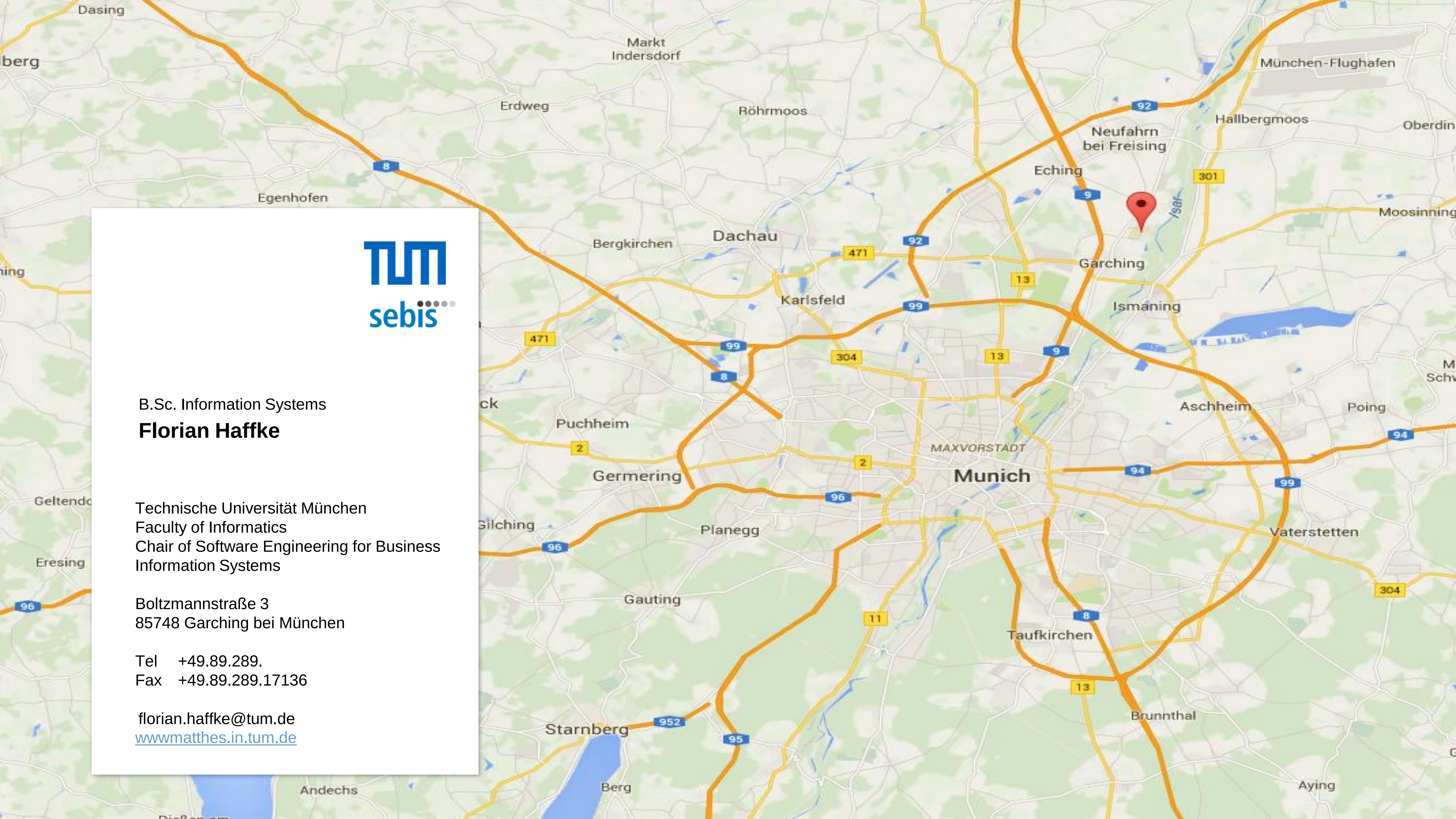
Classification Part 2



Network				
12	Admission	Public	Permissioned	
13	Type	Peer-to-peer		No Network
14	Model	Unilayer	Mulitlayer	Single Server
15	Structure	Unstructured	Structured	Client-Server
Access and Interface				
16	Codebase	Open Source	Closed Source	
17	Unique Scripting Language	Yes	No	
18	Digital Signature Scheme	ECDSA-based	RSA-based	
19	Ownership Model	Transaction-based	Account-based	
20	Transparency	Full	Some Hidden Data	

Questions and Feedback

Thank you for your Attention ☺



B.Sc. Information Systems

Florian Haffke

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

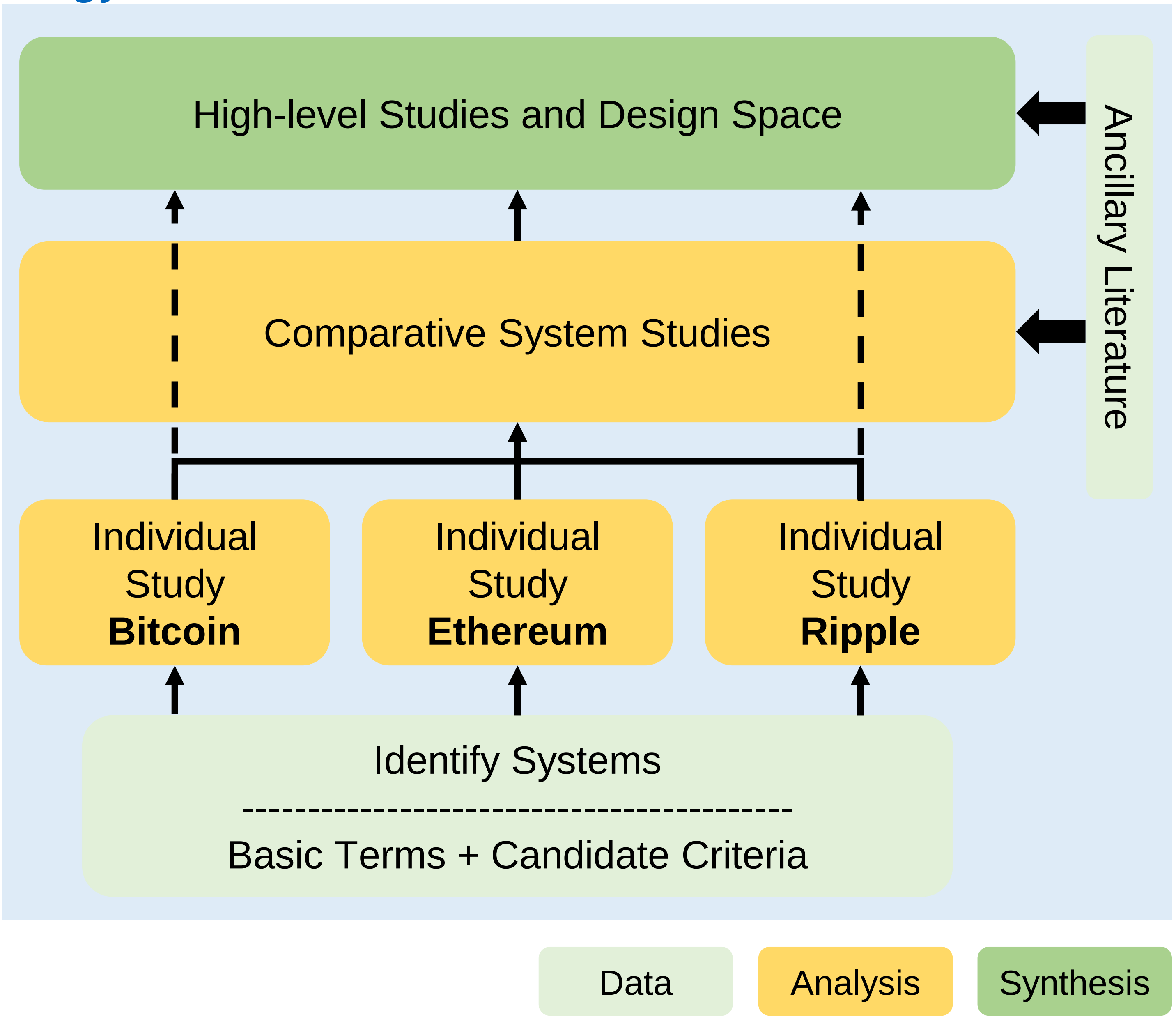
Boltzmannstraße 3
85748 Garching bei München

Tel +49.89.289.
Fax +49.89.289.17136

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

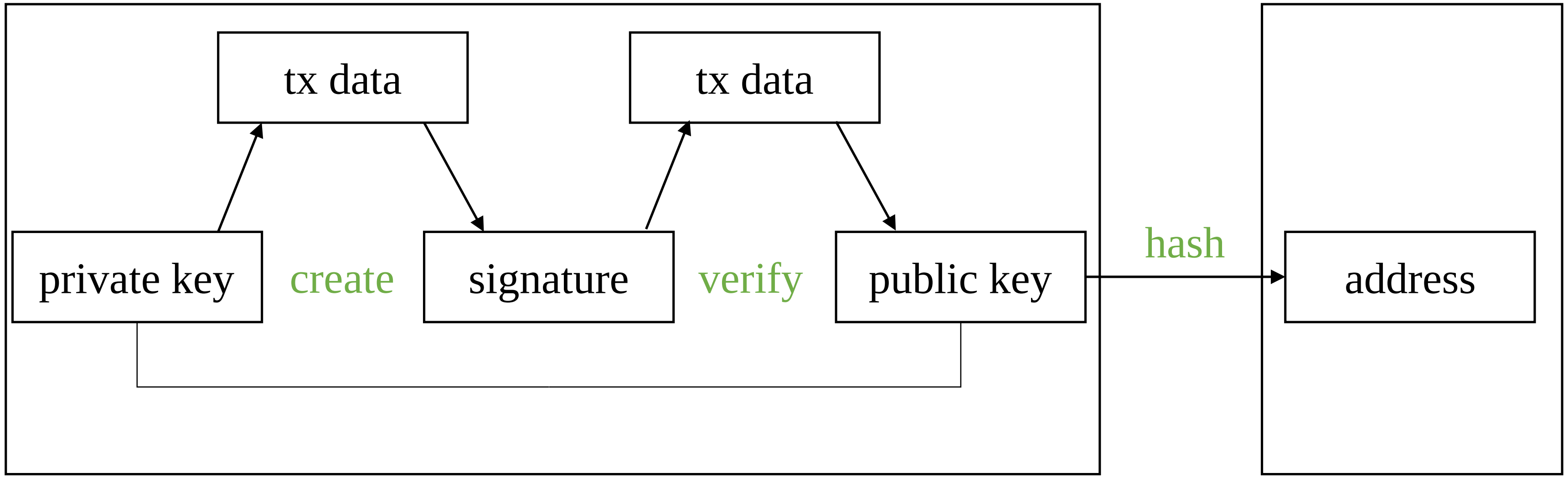
Appendix

Research Strategy


High-level Studies and Design Space
Comparative System Studies
Ancillary Literature
Individual Study **Bitcoin**
Individual Study **Ethereum**
Individual Study **Ripple**
Identify Systems

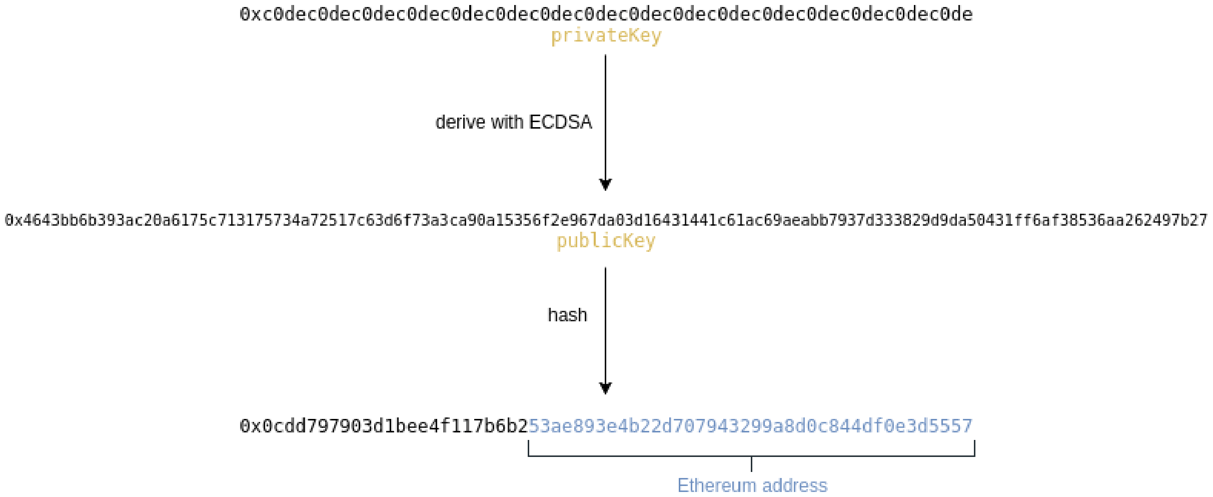
Basic Terms + Candidate Criteria
Data
Analysis
Synthesis

Digital Signature Scheme and Addresses



ECDSA

Example Ethereum

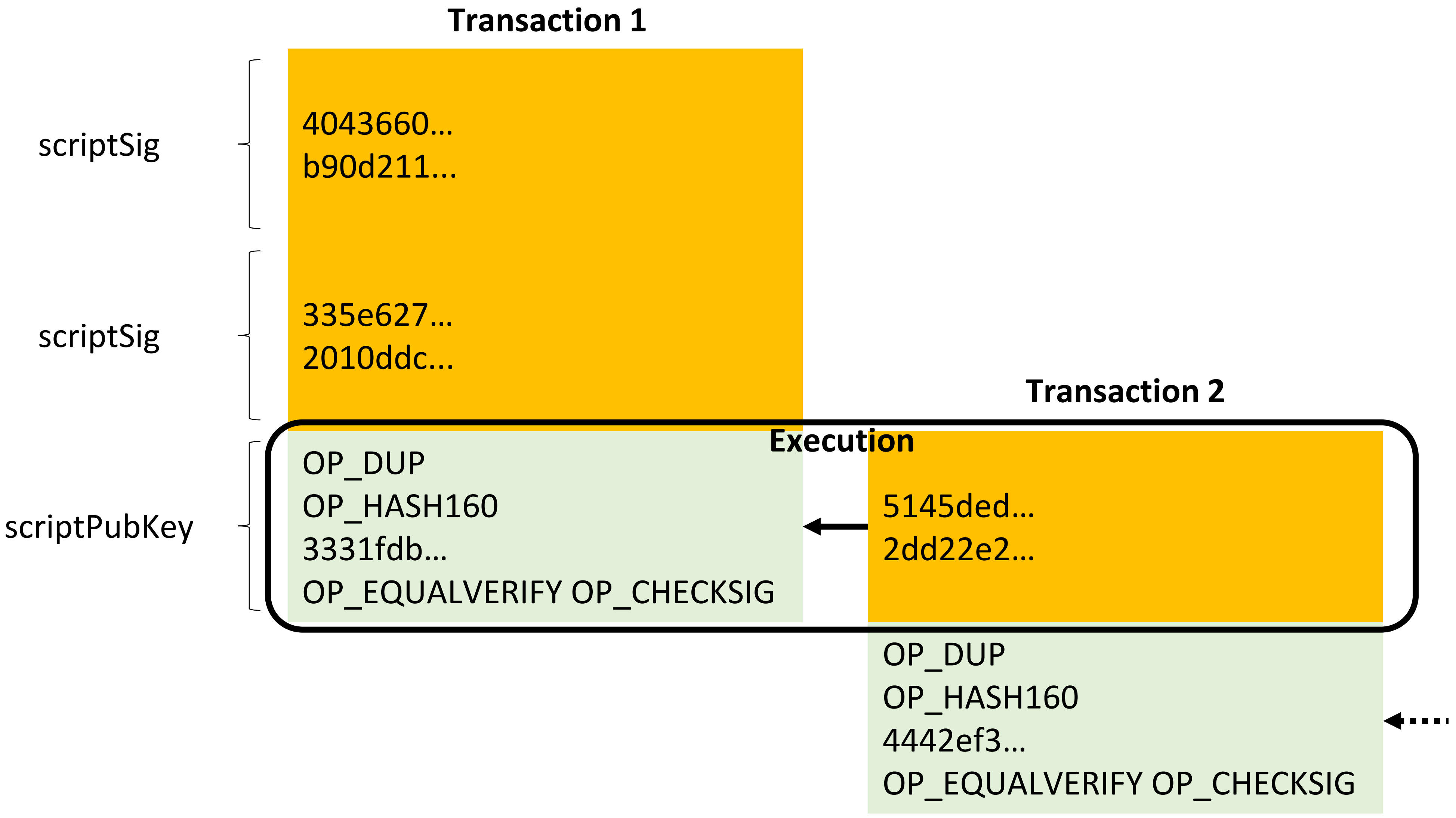


0xc0dec0dec0dec0dec0dec0dec0dec0dec0dec0dec0dec0dec0dec0dec0dec0de
privateKey

0x4643bb6b393ac20a6175c713175734a72517c63d6f73a3ca90a15356f2e967da03d16431441c61ac69aeabb7937d333829d9da50431ff6af38536aa262497b27
publicKey

0x0cdd797903d1bee4f117b6b253ae893e4b22d707943299a8d0c844df0e3d5557

Bitcoin Script Execution



Transaction 1

scriptSig

4043660…
b90d211...

scriptSig

335e627…
2010ddc...

scriptPubKey

OP_DUP
OP_HASH160
3331fdb…
OP_EQUALVERIFY OP_CHECKSIG

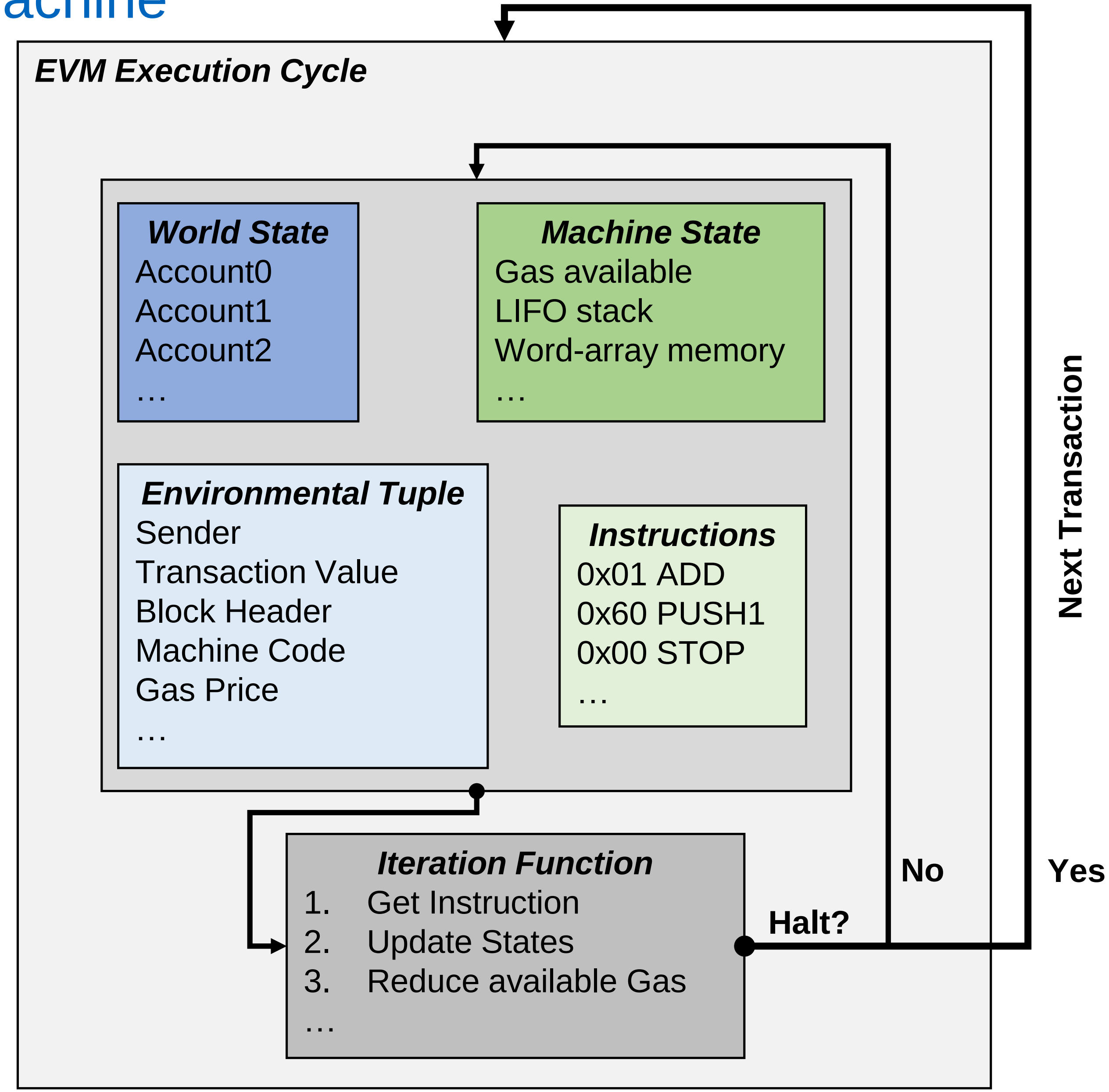
Transaction 2

Execution

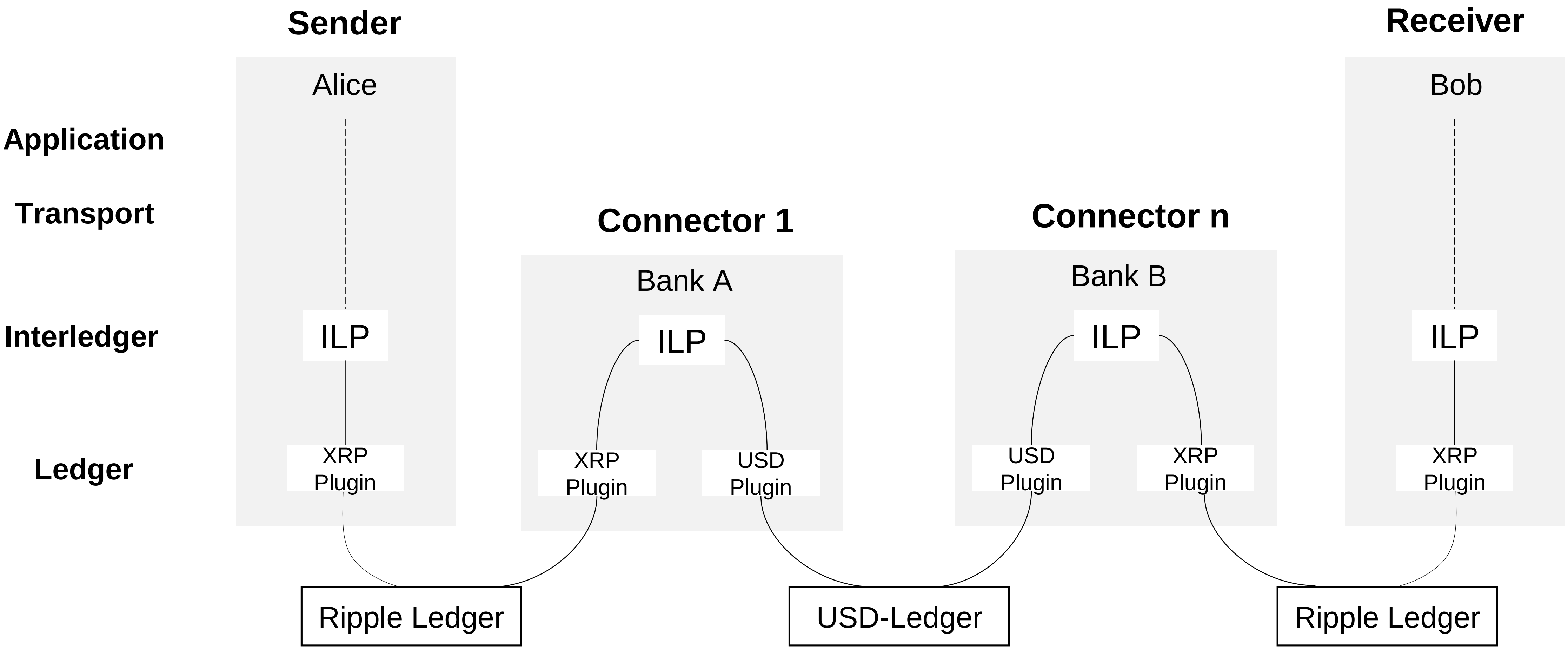
5145ded…
2dd22e2…

OP_DUP
OP_HASH160
4442ef3…
OP_EQUALVERIFY OP_CHECKSIG

Ethereum Virtual Machine



Ripple Issuance Transfers with Interledger


Sender
Receiver
Alice
Bob
Application
Transport
Connector 1
Connector n
Bank A
Bank B
Interledger
ILP
ILP
ILP
ILP
Ledger
XRP Plugin
XRP Plugin
USD Plugin
USD Plugin
XRP Plugin
XRP Plugin
Ripple Ledger
USD-Ledger
Ripple Ledger