

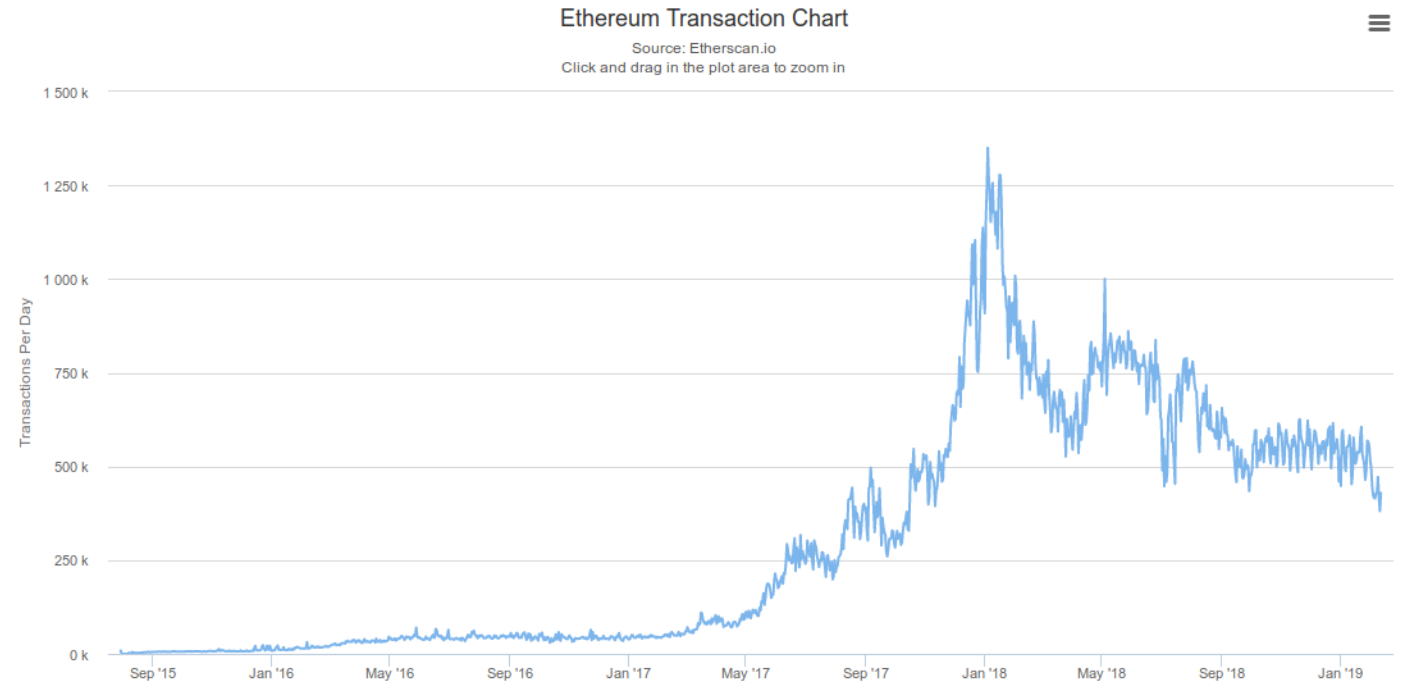
A Conceptual Model for Ethereum Blockchain Analytics

Alexander Hefele, 18th February 2019, Advanced Seminar

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

Ethereum

- Proposed in 2014
- Higher complexity than Bitcoin
- Introduced smart contracts
- \$12bn market capitalization
- 500k transactions per day
- 50k „verified contracts“ on Etherscan



My contribution

- Model the system with Software Engineering techniques
- Goal: bring structure to the system to facilitate data analysis
- Practical implementation of blockchain data analysis

RQ1

- How are the different parts of the Ethereum system correlated with each other?

RQ2

- What data can be extracted from the blockchain for analysis and how can this be done efficiently?

RQ3

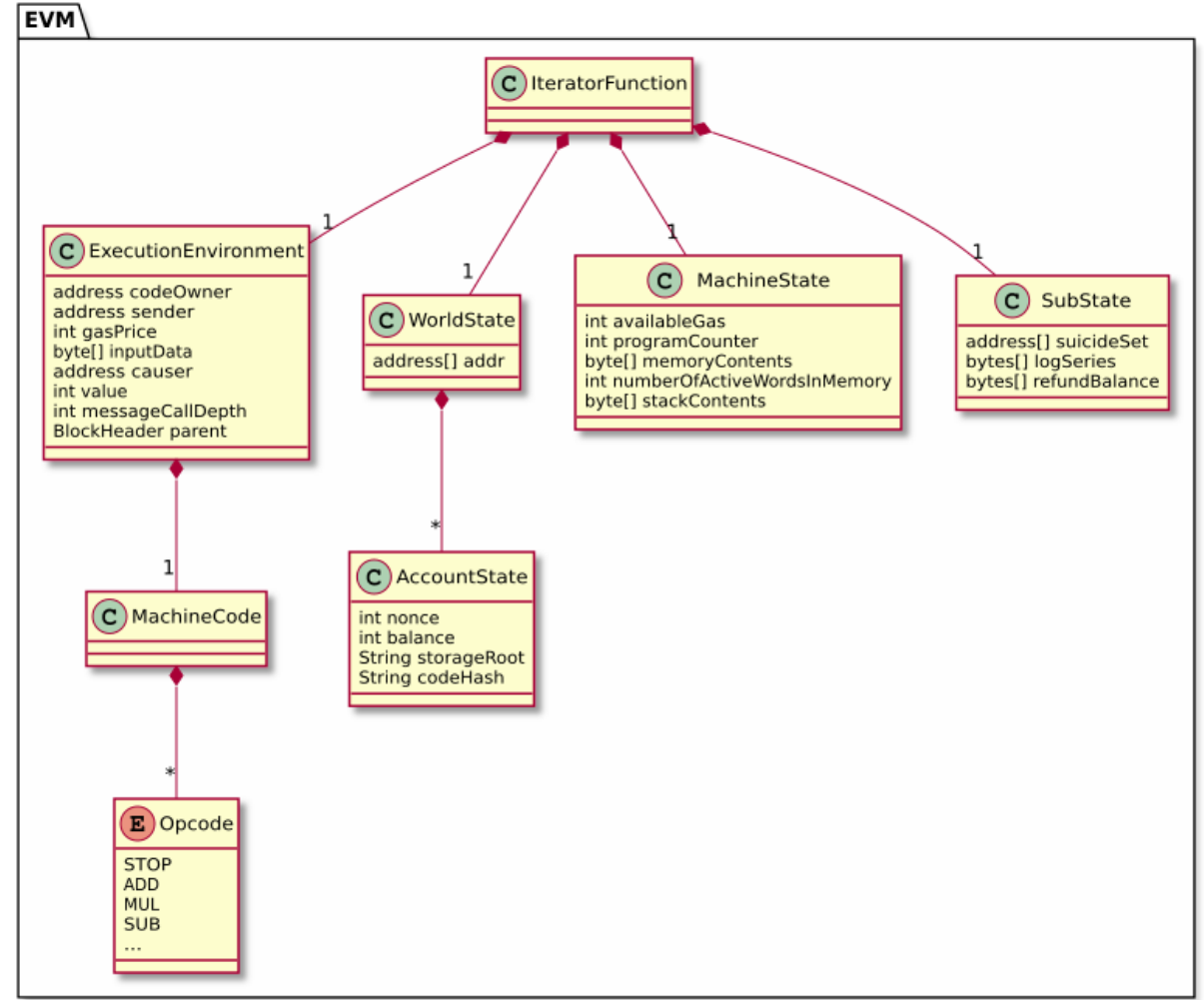
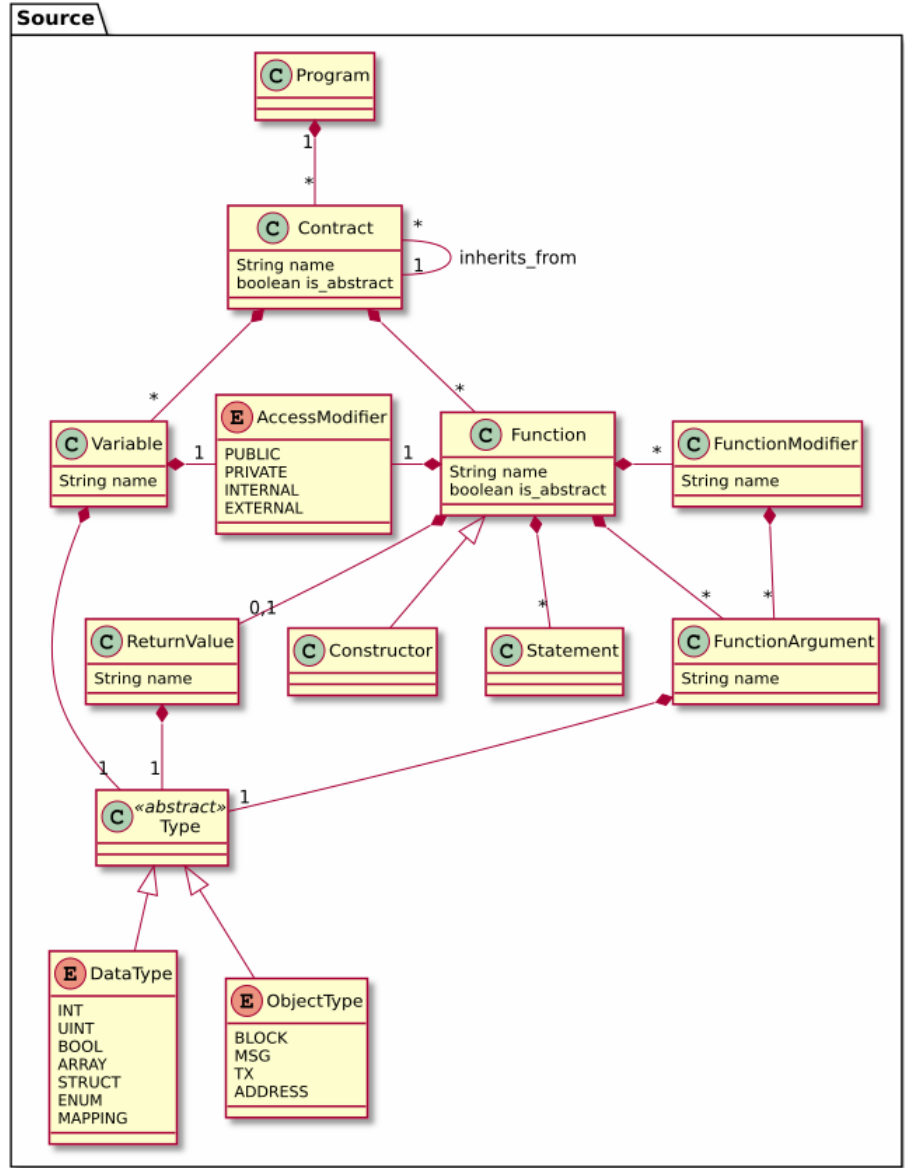
- What does metadata tell us about the network?

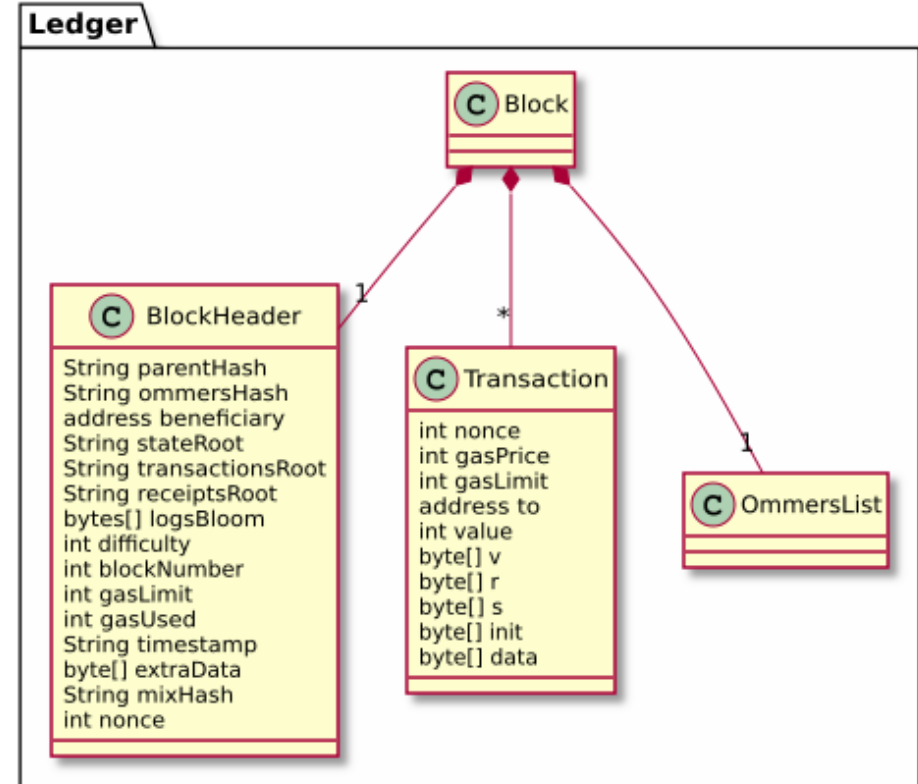
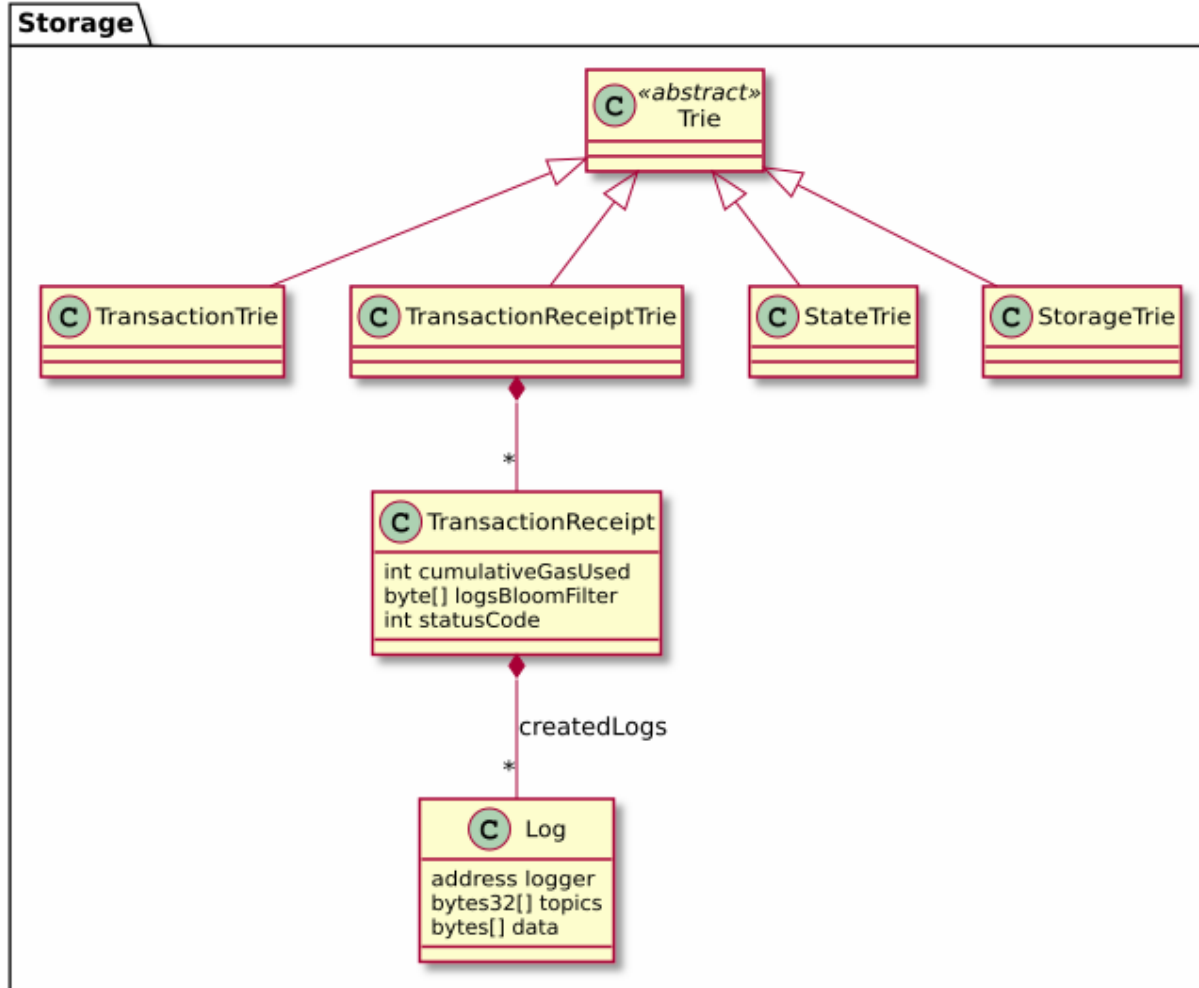
RQ4

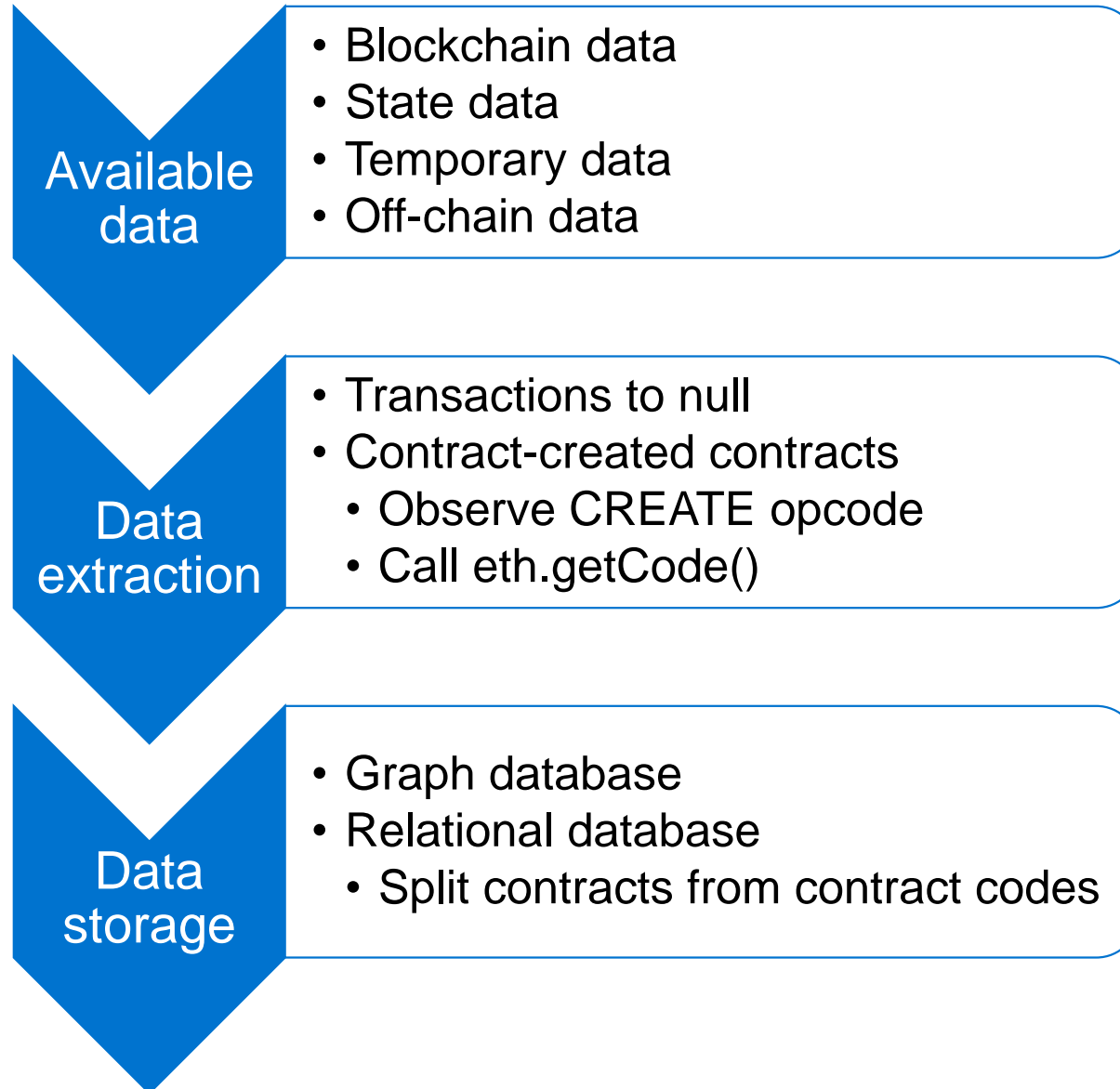
- What are different areas of application of the Ethereum blockchain?

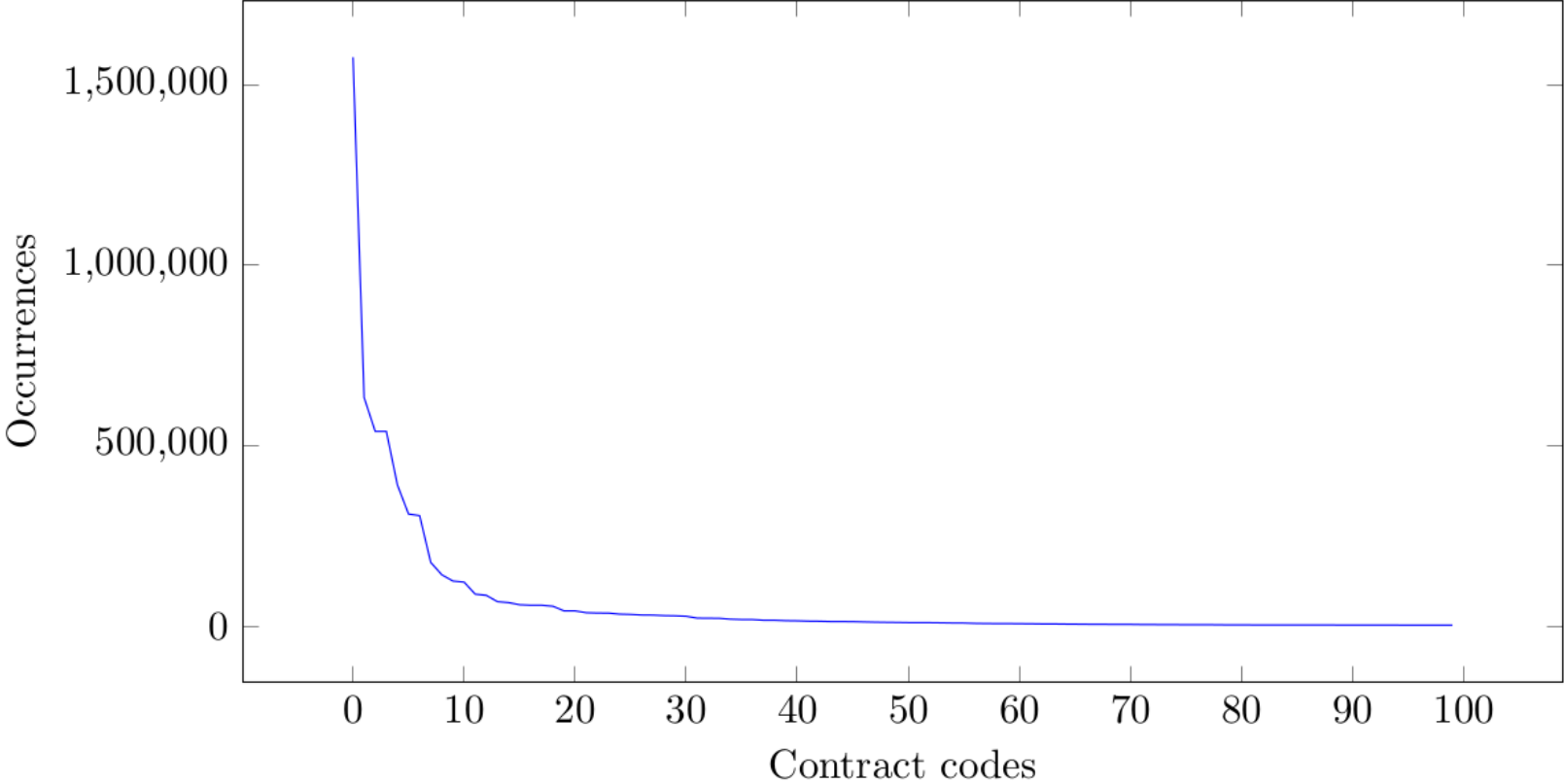
RQ5

- Which anomalies can be observed in the network?









6.90M
blocks

2.18M
user-created contracts

4.80M
contract-created contracts

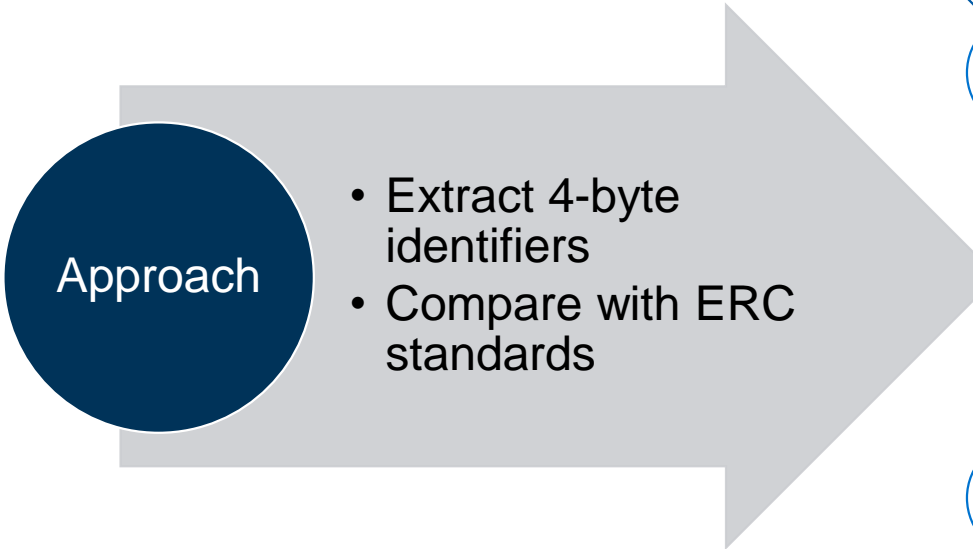
190k
contract codes

Front-running

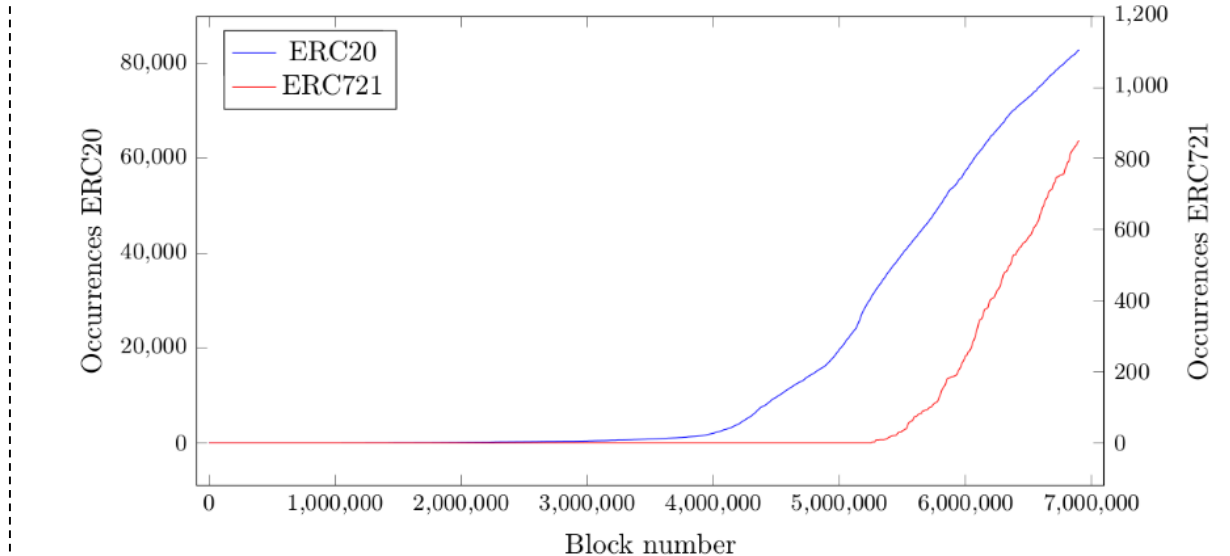
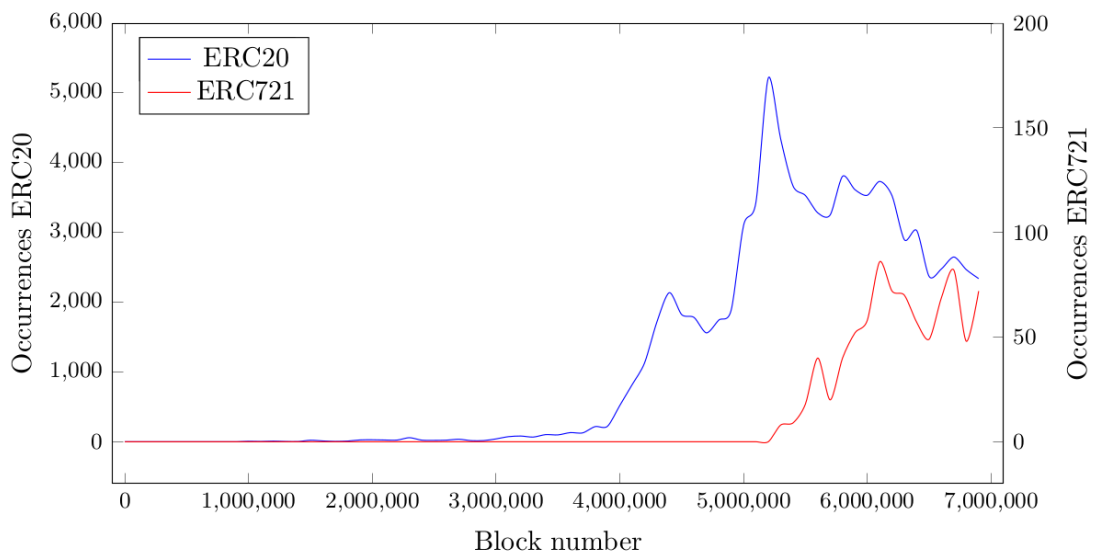
- Conditions:
 - Same recipient
 - Same function call
 - 50% higher gas price
 - Issued ≥ 3 seconds later
- Detected during launch of a blockchain card game

Self-destructing constructors

- 43 detected contracts
- Reasons:
 - Obfuscation
 - Programming error



- 89k ERC20 tokens
- 900 ERC721 tokens
- 1.3% of contracts
- 27% of contract codes

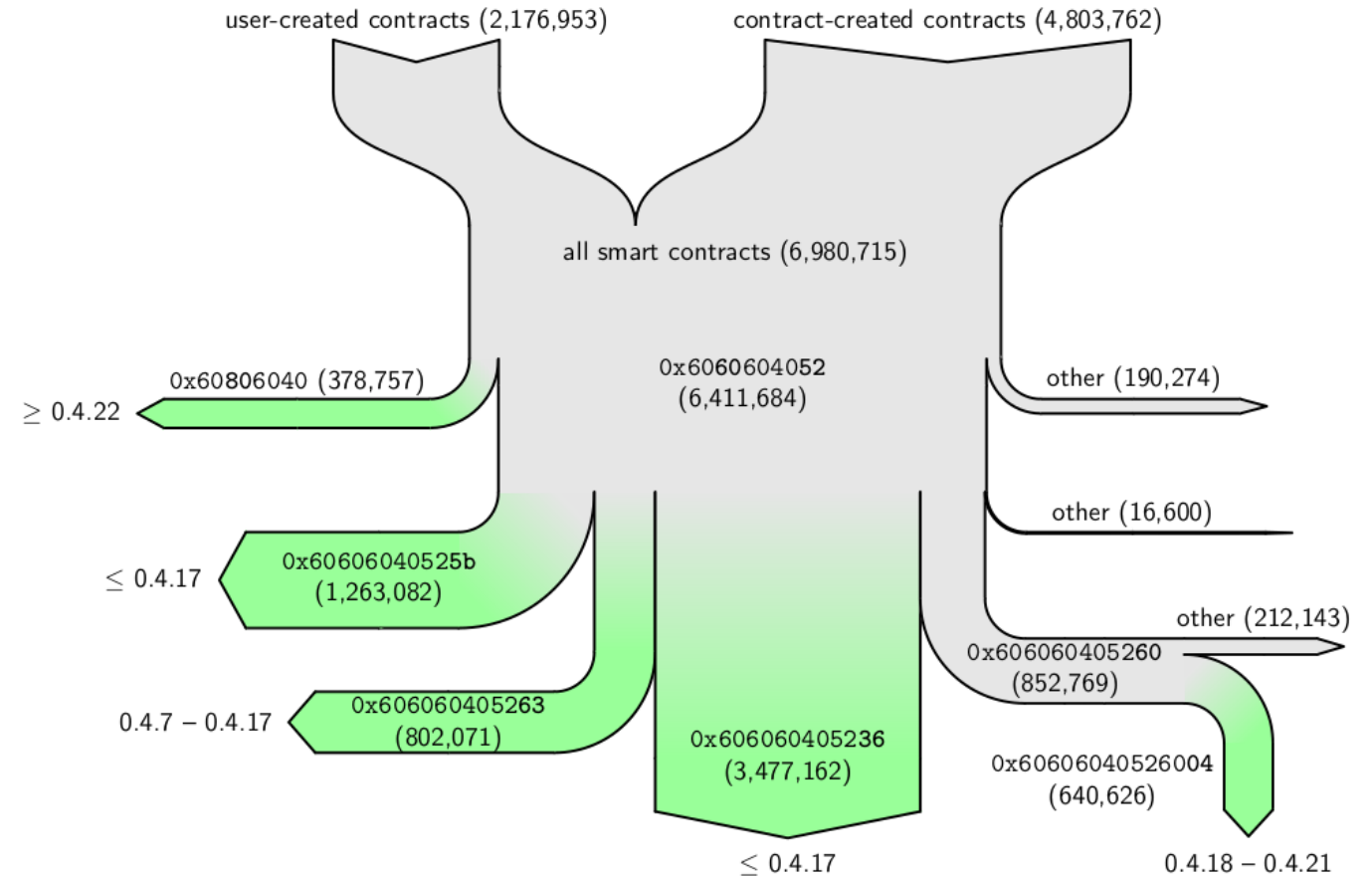


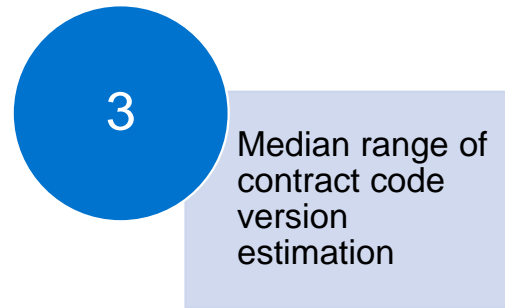
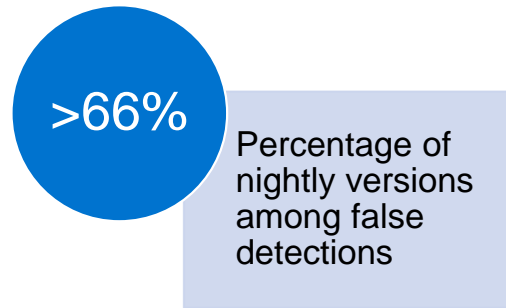
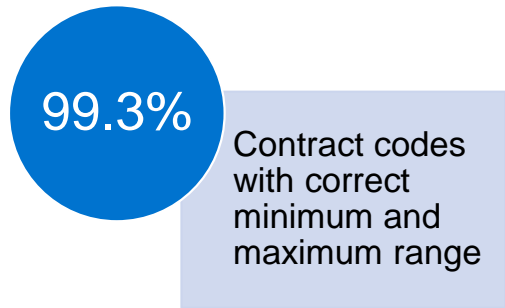
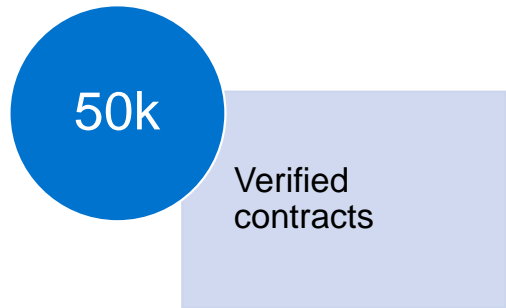
Heuristics

- Contract creation date
- Header analysis

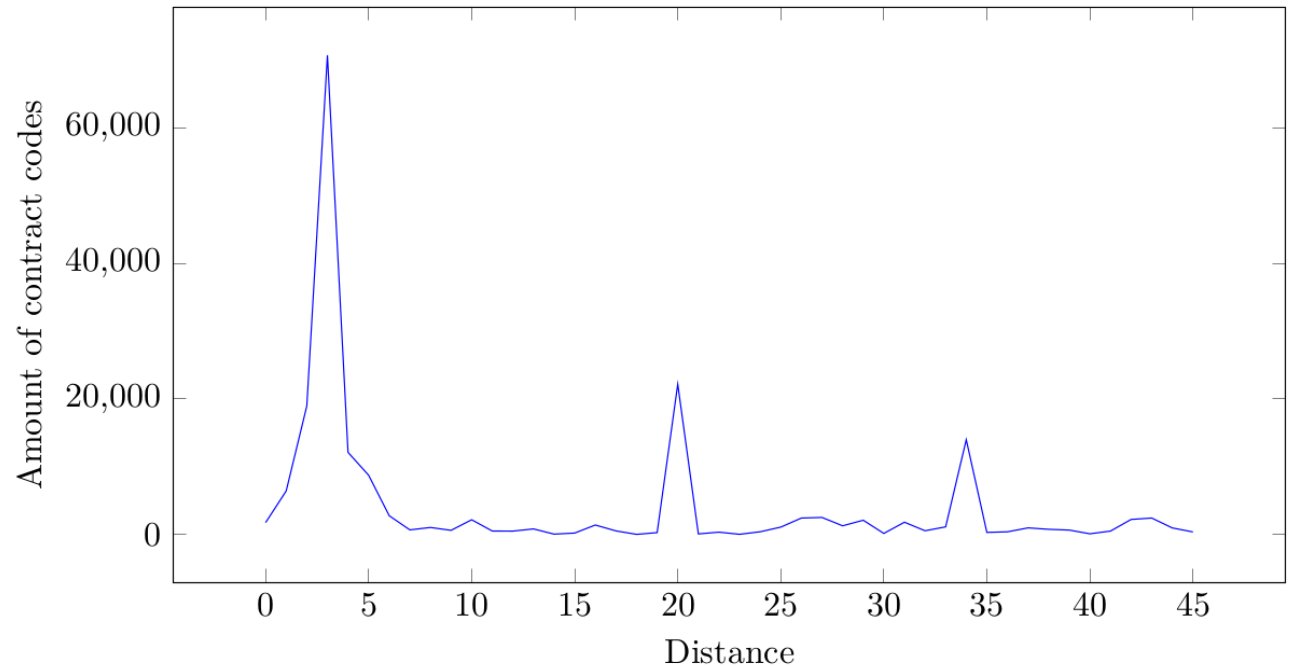
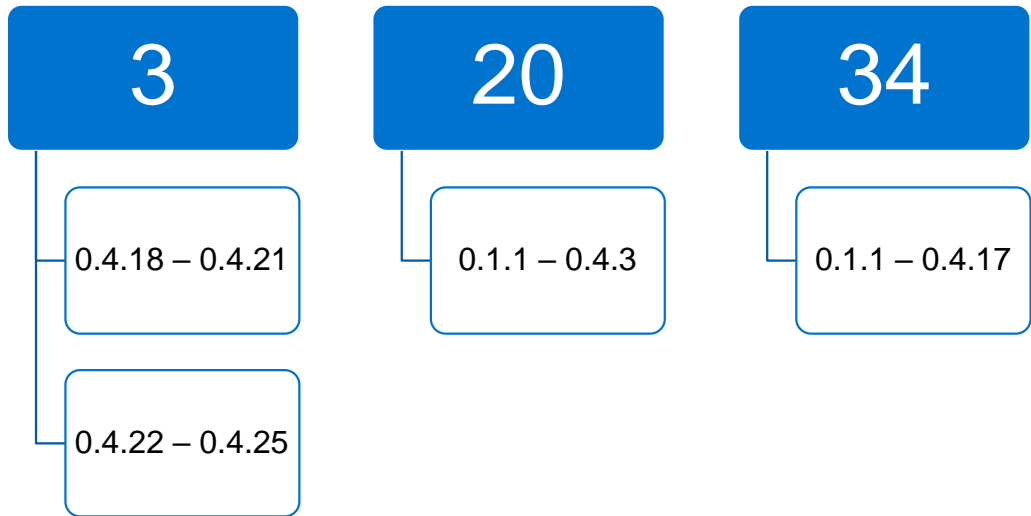
Goal

- Set minimum and maximum version
- Version estimation range as small as possible



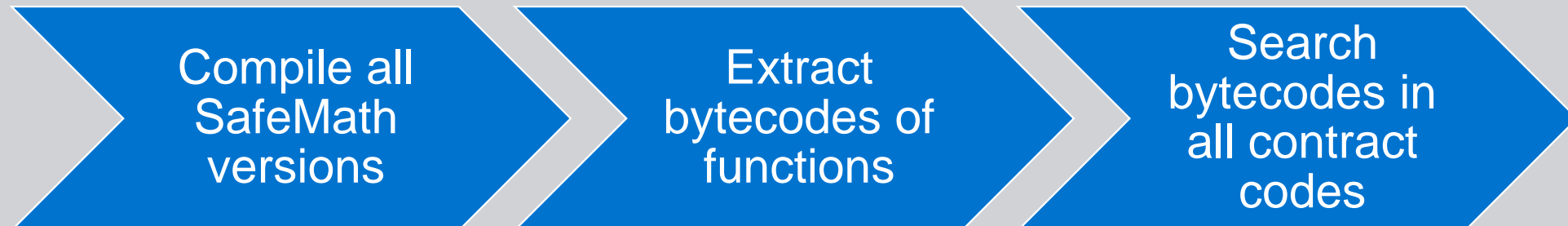


Distances between minimum and maximum compiler version



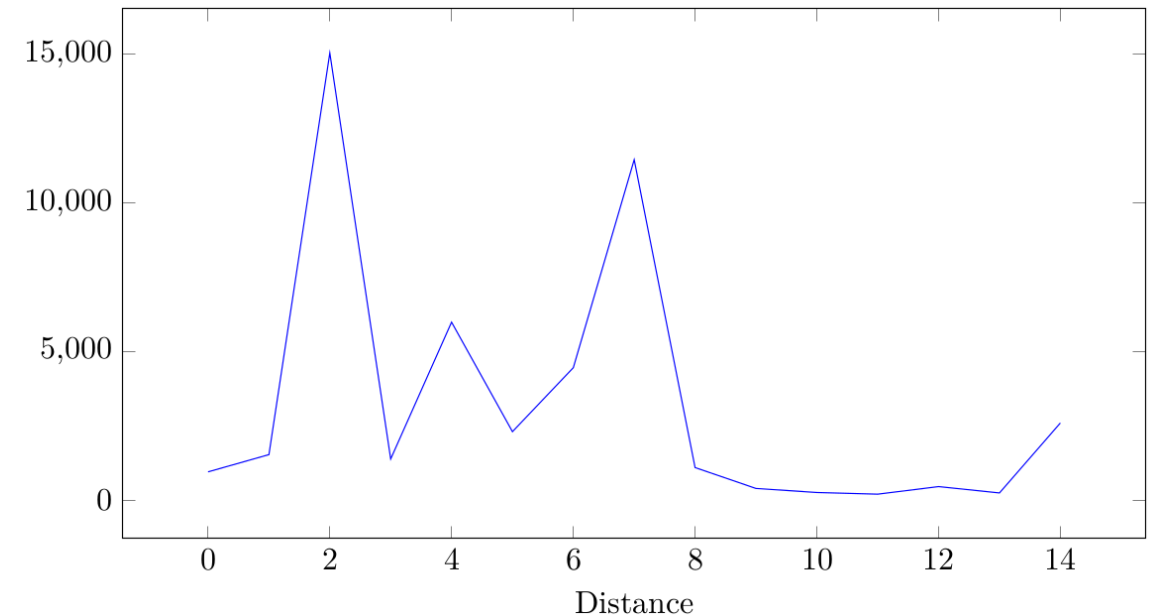
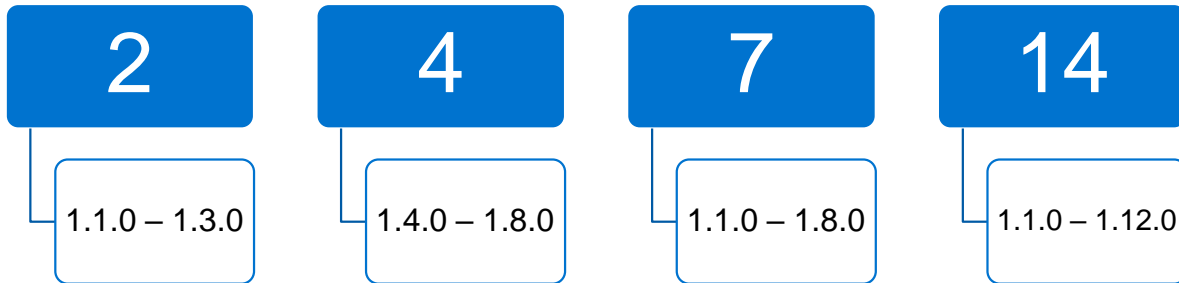
SafeMath library

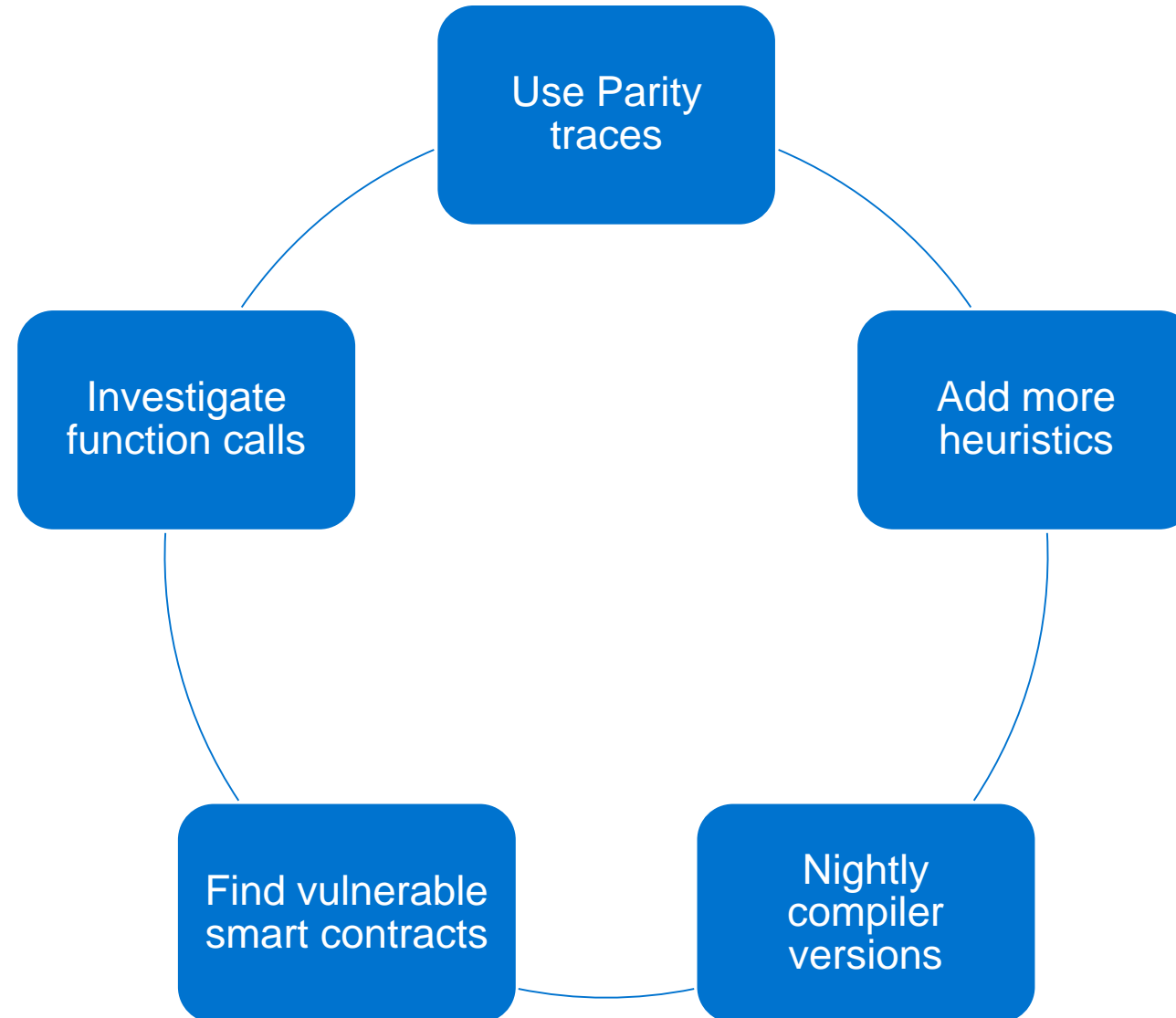
- Most popular Solidity library
- Arithmetic operations without over- and underflows
- All functions are internal
- Approach:



	Source code uses SafeMath	Does not use SafeMath
Detected SafeMath in bytecode	21,375 true positives	27 false positives
Did not detect SafeMath	8,978 false negatives	20,053 true negatives

Distances between minimum and maximum SafeMath version







Alexander Hefele

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

a.hefele@tum.de
www.matthes.in.tum.de

