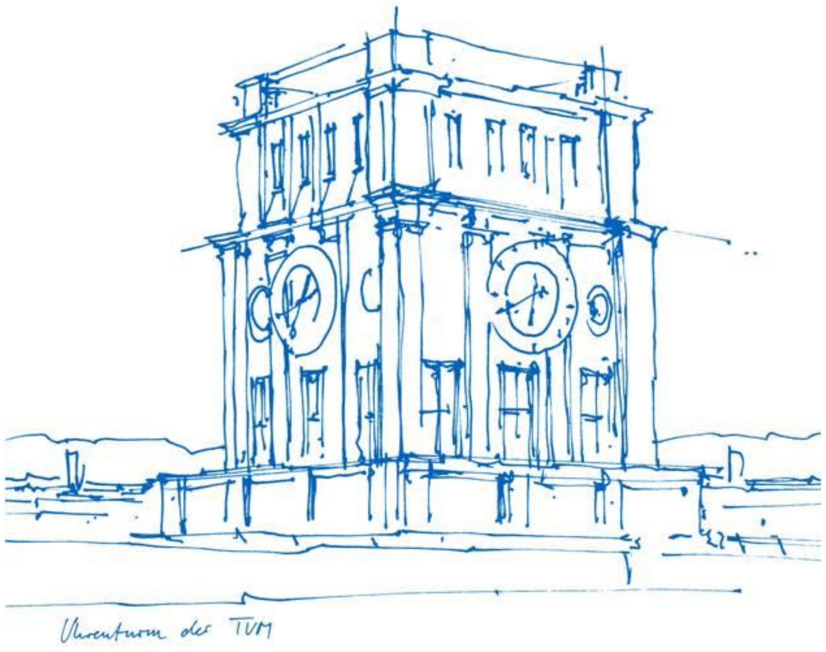
Chair of Network Architectures and Services
Department of Computer Engineering
TUM School of Computation, Information, and Technology
Technical University of Munich

METHODA: **M**ultilayer **E**nvironment and **T**oolchain for **H**olistic NetwO**r**k **D**esign and **A**nalysis

Authors:
Filip Rezabek, Kilian Glas, Richard von Seck, Achraf Aroua, Tizian Leonhardt, Georg Carle
rezabek@net.in.tum.de



Outline

1. Motivation
   - What open challenges we try to solve
   - Considered scenarios
2. Methodology overview
   - Problem analysis
   - Considered parameters and metrics
3. Design details
   - Considered solutions based on requirements
4. Validation of our approach
   - Certain results & capabilities
5. Future work
   - Several of our ideas & open to your input ☺

Introduction

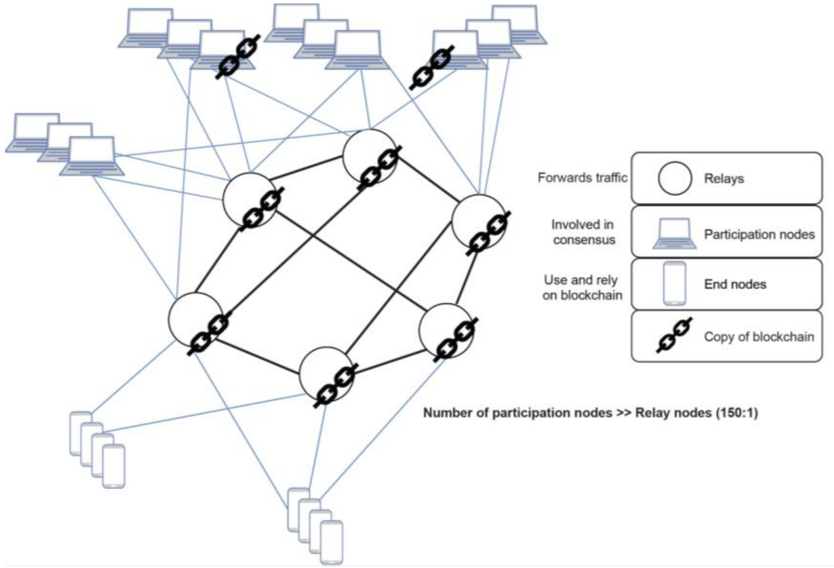
Motivation

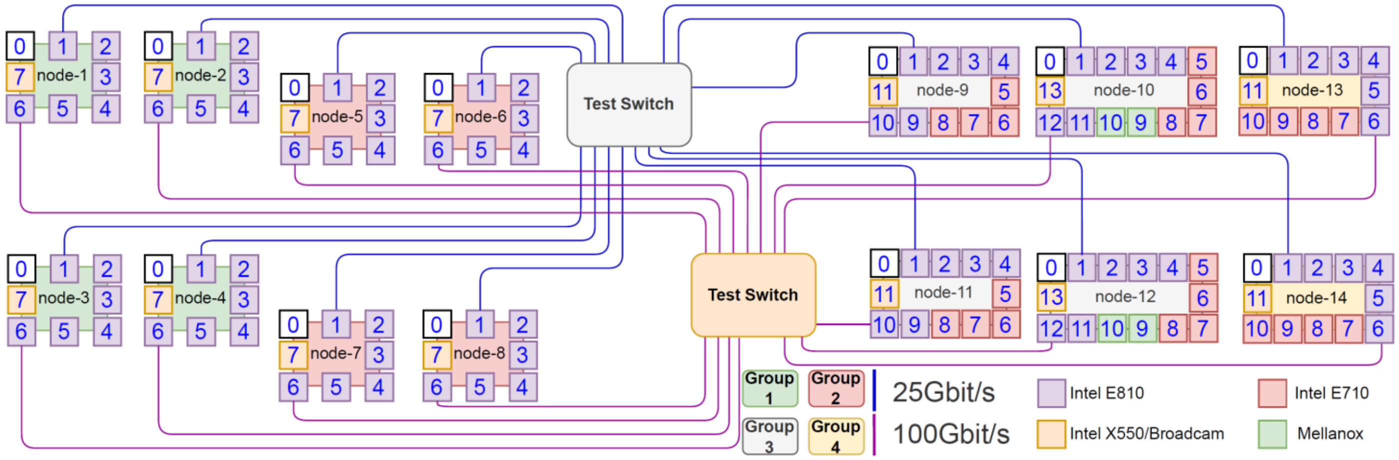
>> 100 of nodes

Globally distributed

Many configuration parameters

Various building blocks





Introduction
Motivation 1/2

1. Various L1/L2 solutions with different properties

- TPS
- Latency
- Finality, …

2. Several technologies discussed to make the system more robust and introduce new features

3. Each protocol has additional configuration parameters, but often no structured approach why such params are selected and undergoes regular updates

Introduction

Motivation 1/2

1. Various L1/L2 solutions with different properties

2. Several technologies discussed to make the system more robust and introduce new features

- Encrypted mempools
- Private compute on permissionless blockchains
- Rollups
- Privacy preserving P2P solutions, …

3. Each protocol has additional configuration parameters, but often no structured approach why such params are selected and undergoes regular updates

Introduction

Motivation 2/2

1. Various L1/L2 solutions with different properties

2. Several technologies discussed in order to make the system more robust and introduce new features

3. Each protocol has additional configuration parameters, but often no structured approach why such params are selected and undergoes regular updates

- HW specifications & Requirements
- P2P network structure
- Block size,
- Versioning…

Introduction

Motivation

Structured approach to assessing the capabilities of various distributed systems e.g., blockchains, cryptographic protocols, peer-to-peer systems, and privacy preserving systems…

- In a **reproducible** manner
- Compare different **architectures** and their implications
- Identify **common ground** for evaluation without external noise

Focus on deployments of systems in a controlled environment → emulation of realistic deployments

Analysis
Scenarios

Example of two blockchains with very different consensus mechanisms and different properties

Considering the lifecycle of a transaction/block/message propagation

Overhead on each peer and expected HW specs

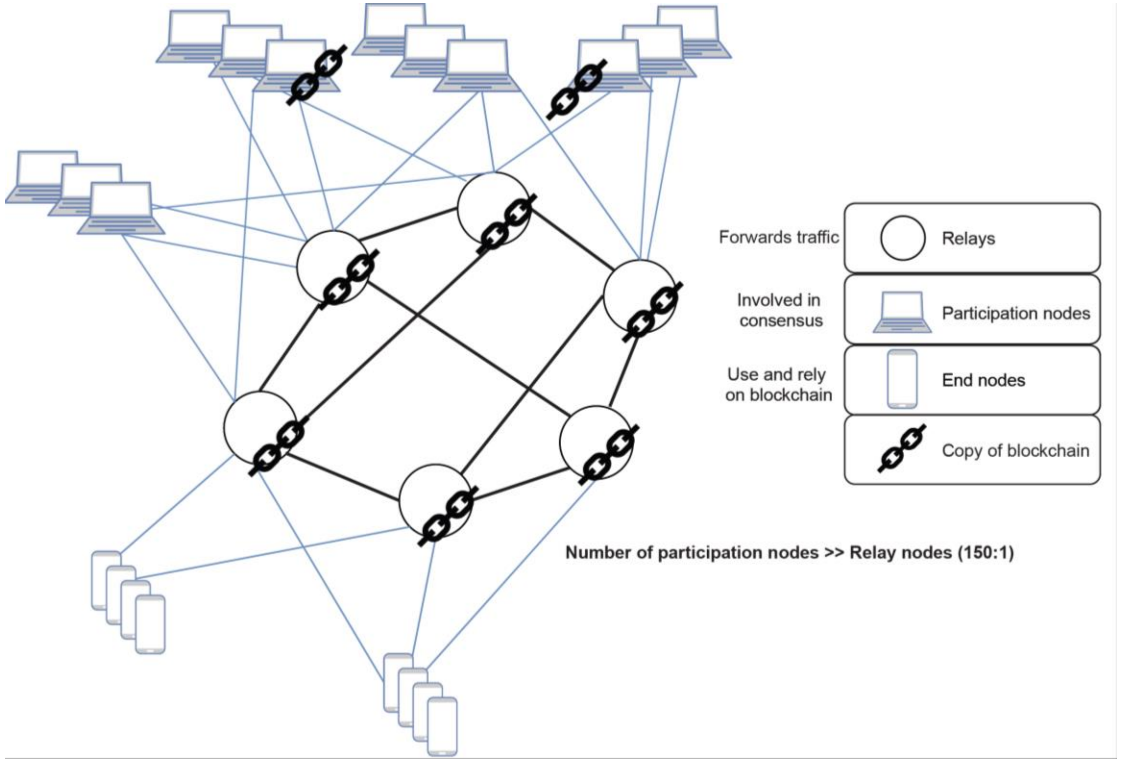
P2P network structure and technology

What types of transactions do we consider?

- Token transfer, smart contracts, …

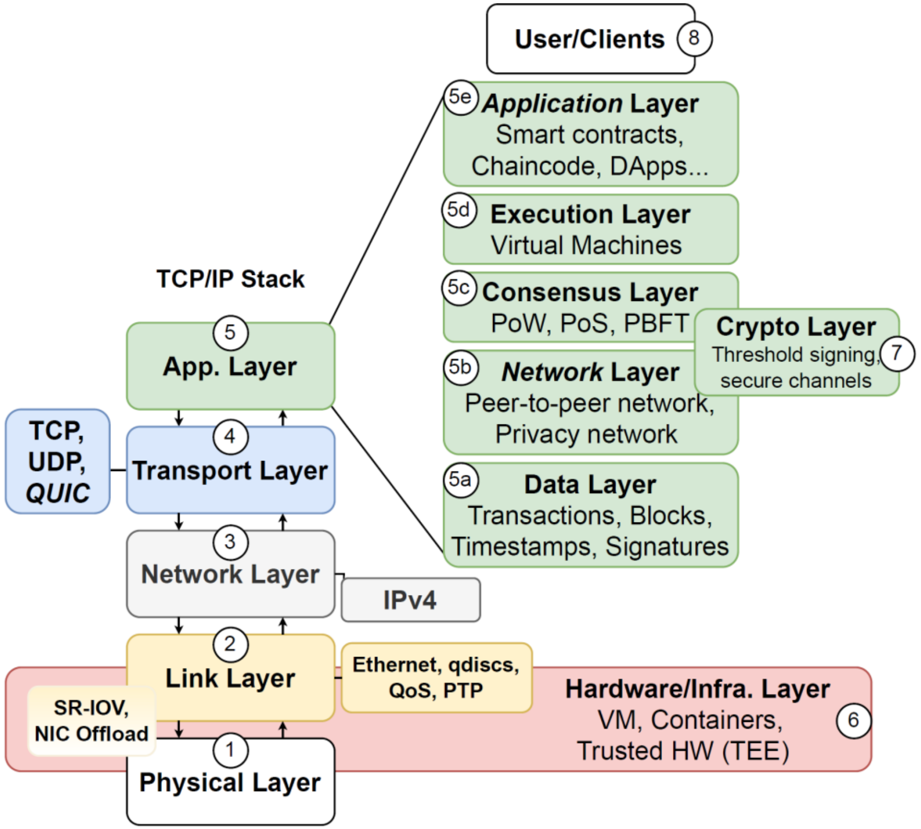
Threshold and MPC cryptography protocols, ZK, …

Infrastructure layer



Analysis
Overview Stack

- Builds on top of Internet infrastructure
- Forms overlay peer-to-peer network
- Exchange of transactions/blocks
- Agreement on blocks as a part of the consensus
- Applications – Smart Contracts & DApps
- Users/clients – rely on the infrastructure



Analysis
Evaluation methodology

- Deployment strategies – cloud, local deployment
- Experiment design – theoretical assessment, black vs white box testing

Analysis

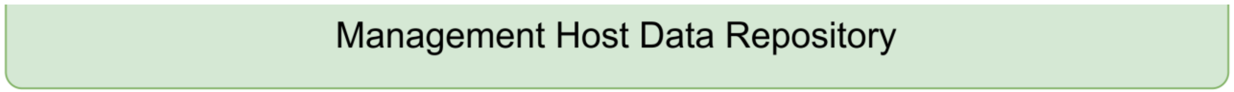
Evaluation methodology

- Experiment Metrics
  - Throughput
  - Latencies
  - Finality
  - Queue size
  - CPU, RAM, I/O

- Experiment parameters
  - Number of peers
  - Threshold
  - Runtime config
  - Message size
  - HW specs
  - Fault injection

METHODA Design
Overview

Orchestrated from the management host



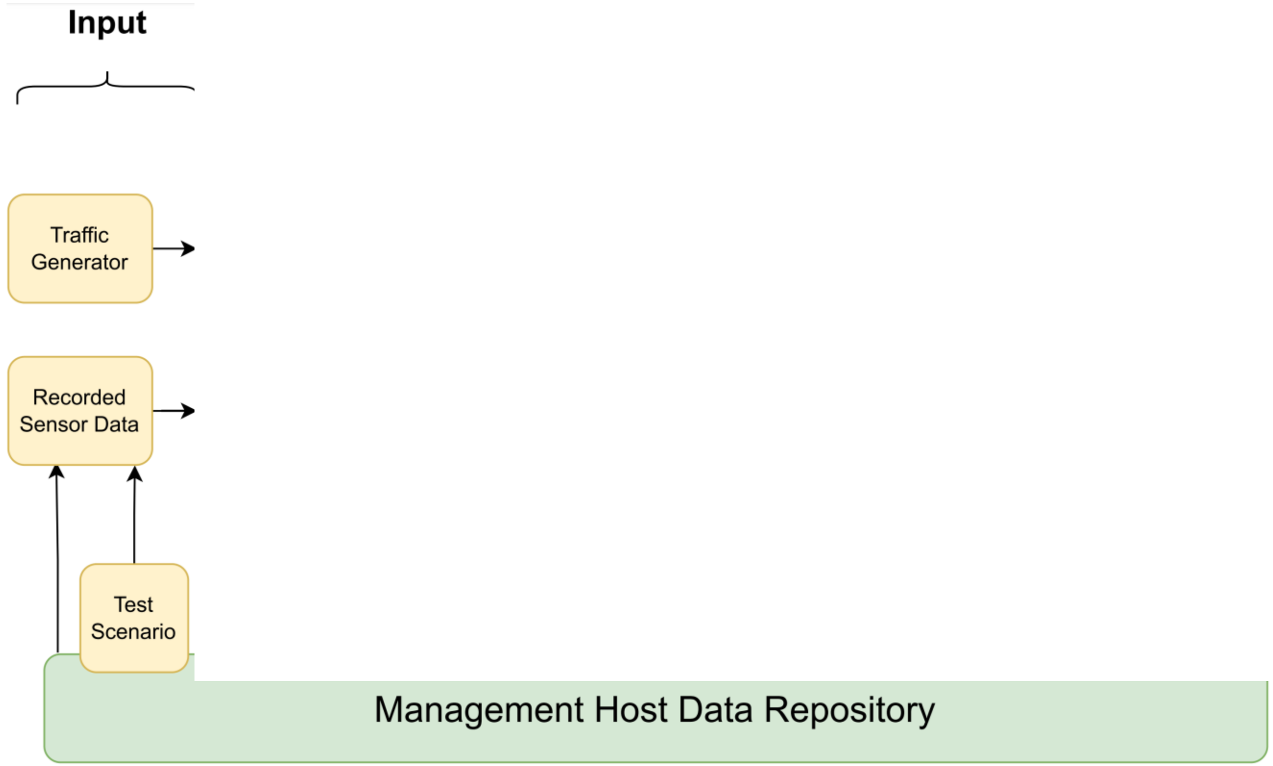
METHODA Design
Overview

Orchestrated from the management host

Three parts of each experiment

Input

- Defines the experiment
- Specifies data sources and network



METHODA Design
Overview

Orchestrated from the management host

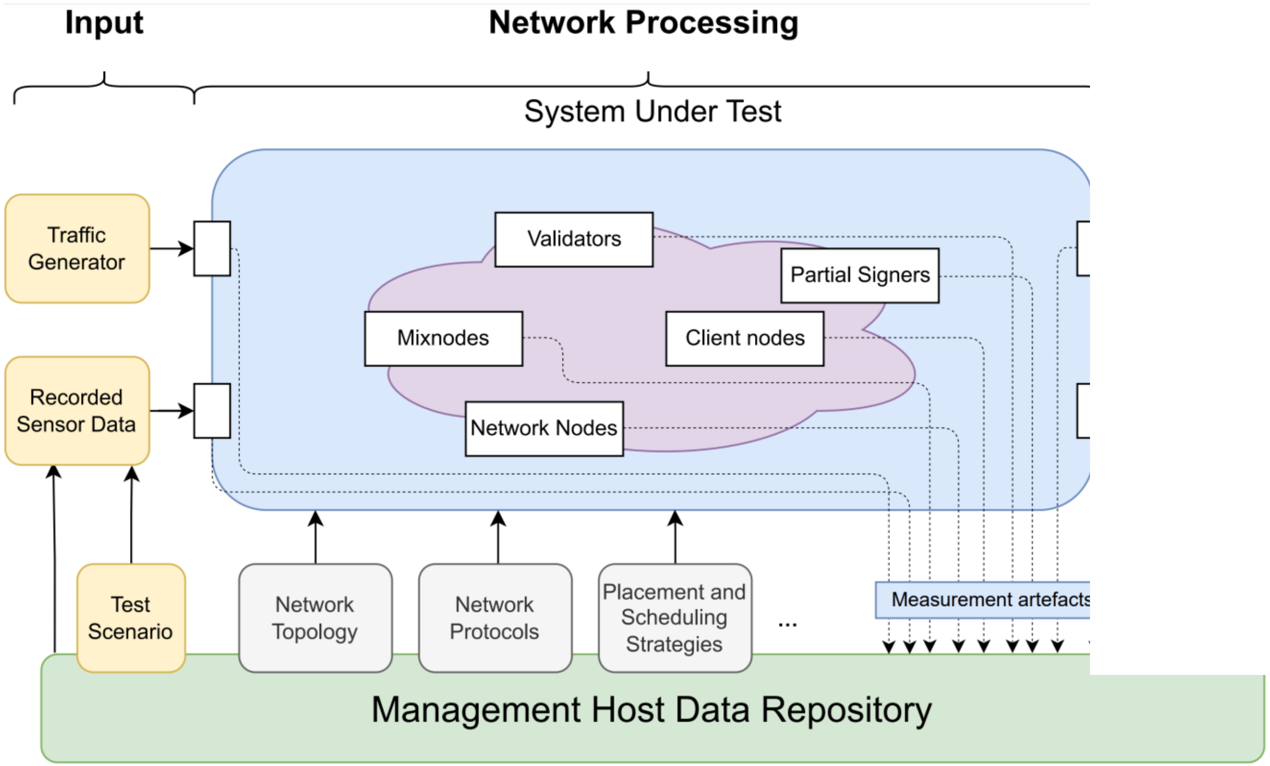
Three parts of each experiment

Input

- Defines the experiment
- Specifies data sources and network

Network Processing

- Encompasses the tested system
- Takes configuration from input
- Supports the experiment



METHODA Design
Overview

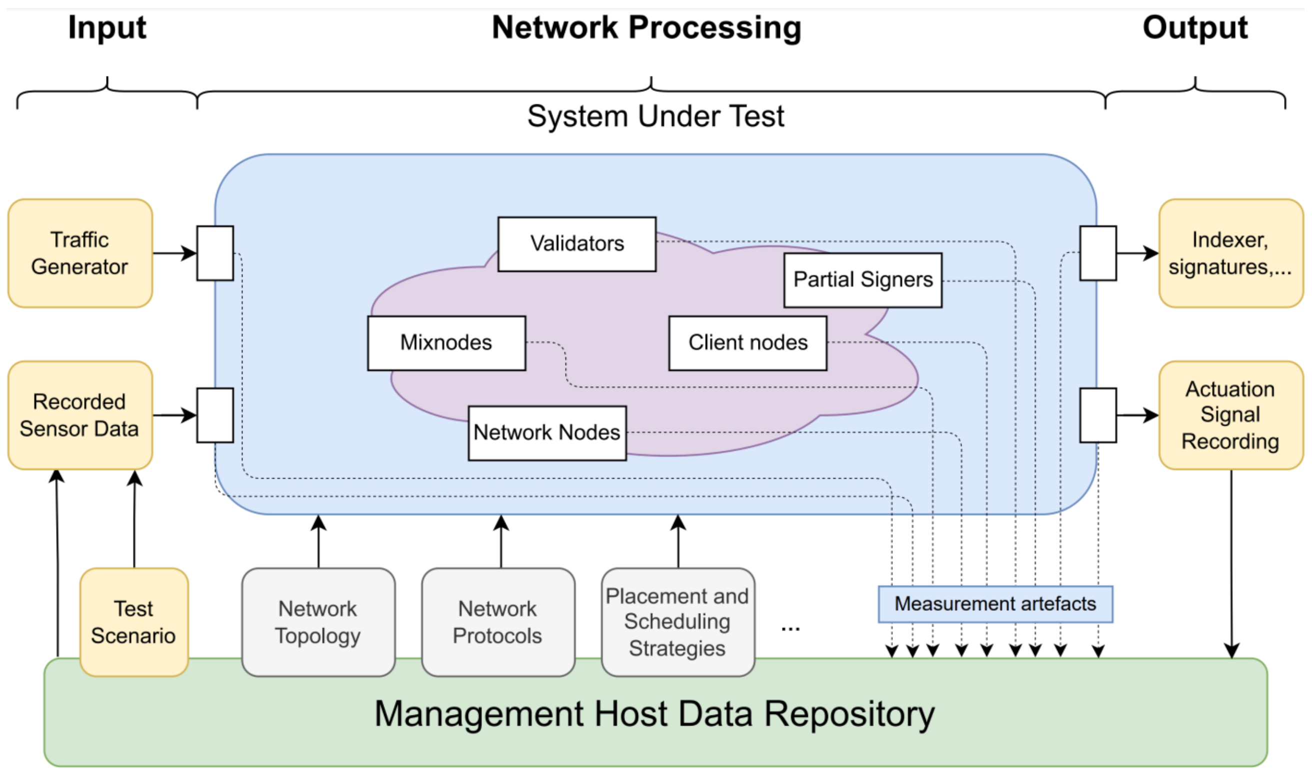
Orchestrated from the management host

Three parts of each experiment

Input
- Defines the experiment
- Specifies data sources and network

Network Processing
- Encompasses the tested system
- Takes configuration from input
- Supports the experiment

Output
- Records experiment results
- Can include physical actuation



Validation
Set of experiments

Focus on **Trusted Execution Environments** e.g., AMD SEV-SNP

Threshold Cryptography

MEV behavior on Algorand

End-to-end delay between client and a mempool on Ethereum
- Understand processing overhead caused by the node stack (black box testing)

HW specs impact on performance of Algorand blockchain

P2P networks, ZKs…

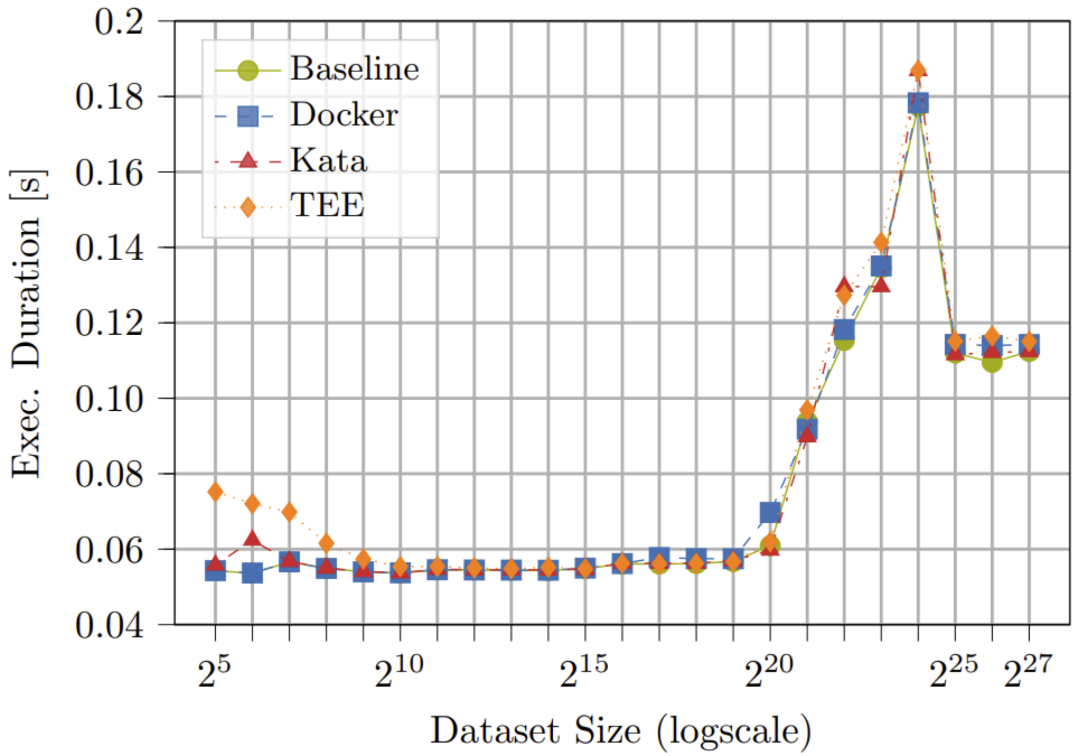
→ Overall, validates our approach and evaluation toolchain

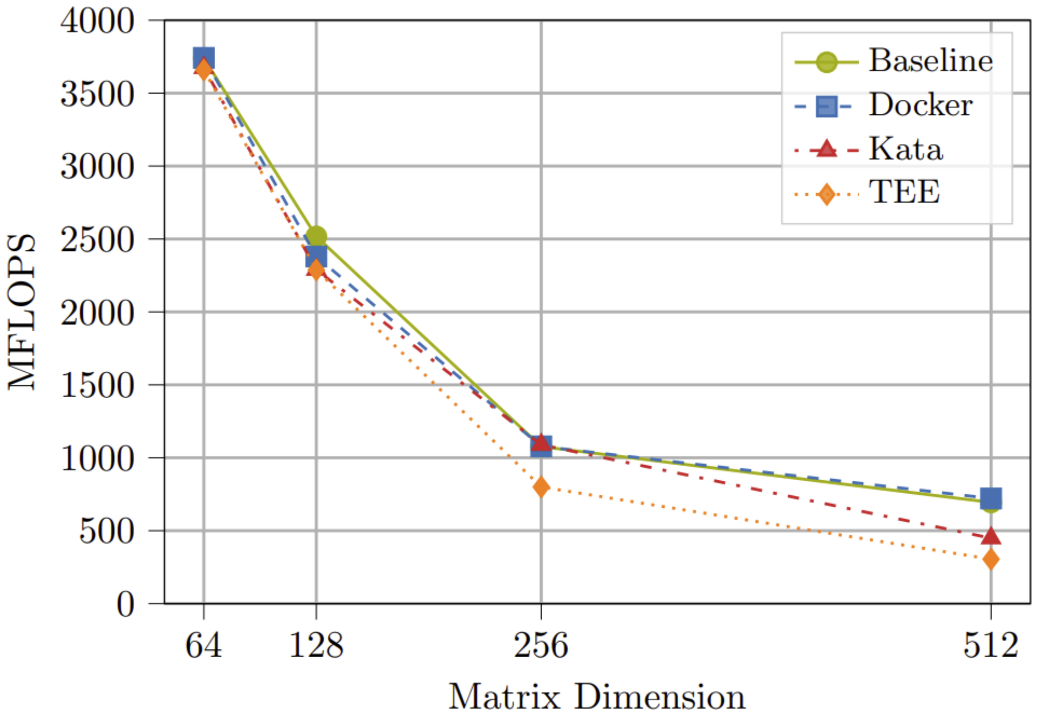
Validation

Set of experiments -- TEE

Evaluation of CPU compute bound – triad

Evaluation of CPU memory bound – matrix dimensions





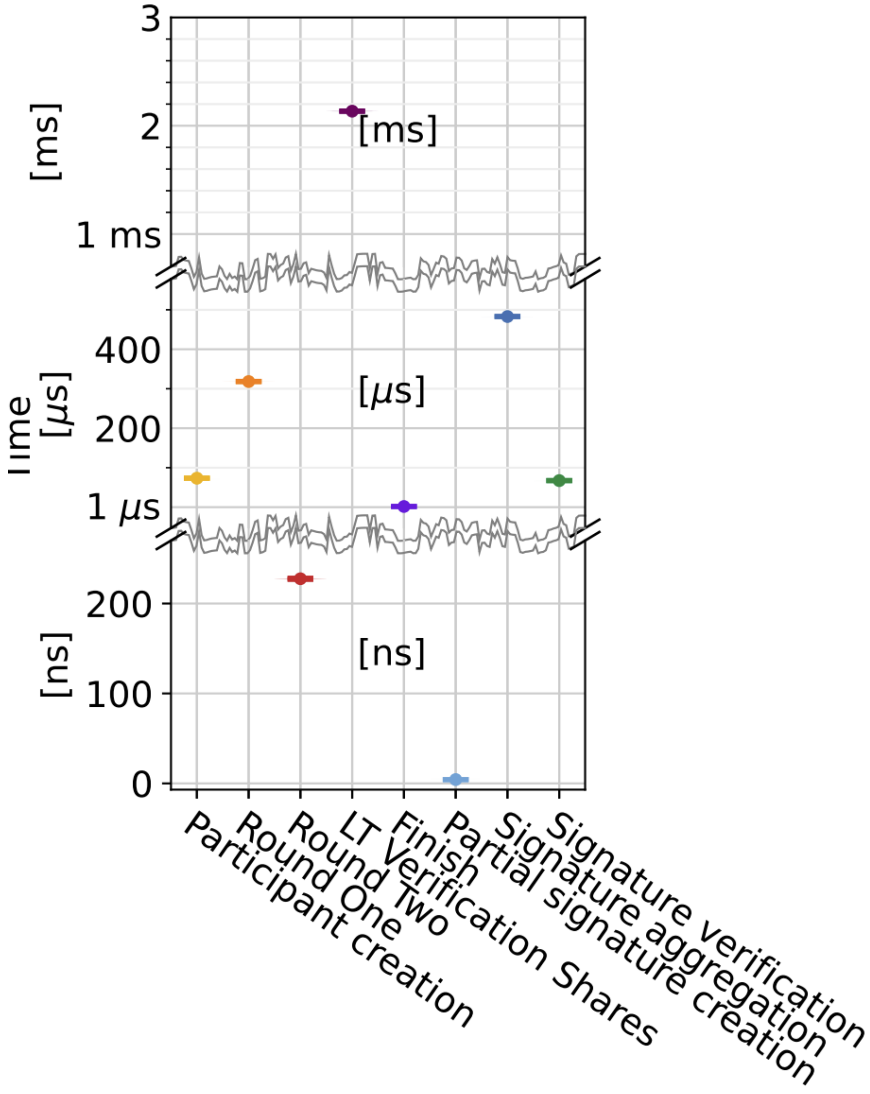
Validation

Microbenchmark of Threshold Schnorr scheme -- FROST

Evaluation of individual steps in the algorithm

Focus on:

- Key generation
- Pre-process
- Sign
- Verify

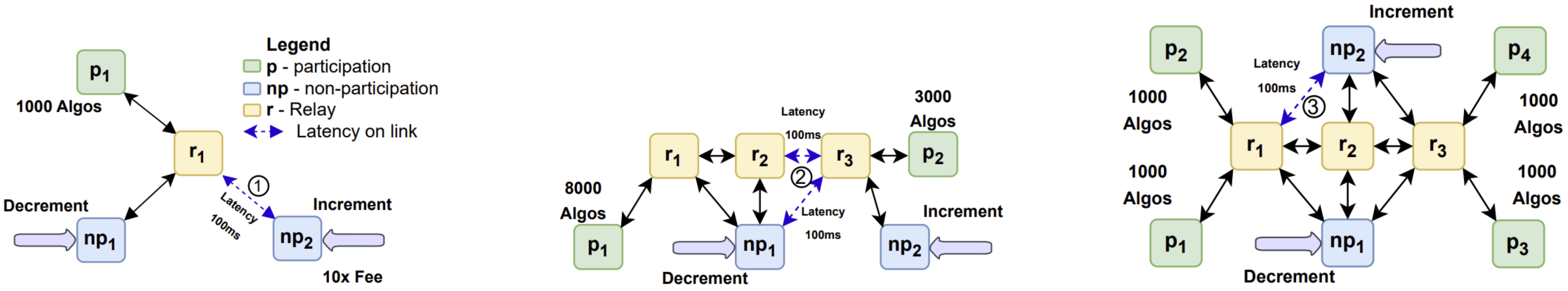


Validation

Evaluation of MEV behavior for FCFS

Various scenarios that validate of consensus and network layer

First-come first-serve (FCFS) transaction ordering [1]



(a) Scenario 1 (b) Scenario 2 (c) Scenario 3

[1] Playing the MEV Game on a First-Come-First-Served Blockchain
Burak Öz, Jonas Gebele, Parshant Singh, Filip Rezabek, Florian Matthes

Summary

Key takeaways and future work

Configurable framework providing granular control collecting diverse insights

Scale to accommodate for large scale deployments

Several open challenges

Unification of evaluation guidelines and metrics would be beneficial – currently still unclear

Steppingstone to achieve holistic view on interaction of individual layers

- Helps to develop a new generation of core developers to handle the complexity

Future work

Possible use cases

Different views

- Private computing on public blockchains and applications benefiting from that
- DePIN – building blocks
- Simulation vs Emulation
    - Interesting works regarding P2P network simulation and validation of the results in emulation infrastructure

Thank You!

Filip

@rezabfil

@rezabfil

rezabek@net.in.tum.de

METHODA

Revisit requirements

Reproducibility
Experiments can be easily reproduced

Security
System resilience to malicious activities

Scalability
The network can handle large-scale traffic

Interpretability
Generated logs can be analyzed and explained

Realism
Works with real-world data

Reliability
The system can handle HW malfunctions

Diversity
The system can handle a variety of data formats

Configurability
Choice of experiments and their parameters easily configurable

Autonomy
Experiments run without human interaction

Design

Satisfaction of requirements

Scalability

- Number of nodes, Transaction per Second (TPS), number of wallets

→ Our deployments should allow for representation of real deployments

Diversity

- Transaction formats, logs, network traffic, on-chain data,
- Each blockchain is very different
  - Node structure, consensus, features, programming language…
  - What are common metrics one can evaluate to make it a *fair* comparison

Interpretability

- Correlate data from different parts and be able to assess them

Design
Satisfaction of requirements

Configurability

- Allow for various configuration options of each layer
- Various HW specs
  - Are we CPU or network capped?
  - Impact of more compute power on performance
- Network behavior e.g., latencies, packet drops

Realism

- Now – what blockchain serves as a base? Not easy to get to all data e.g., validators on mainnet, relays
- What workloads do we assume? E.g., swap, DeFi products? Most likely combination of all
- Governance, tokenomics, …
- Network behavior – global systems in many scenarios
- → could be a whole another talk, but in general combination of probes and on-chain and off-chain, mainly WIP