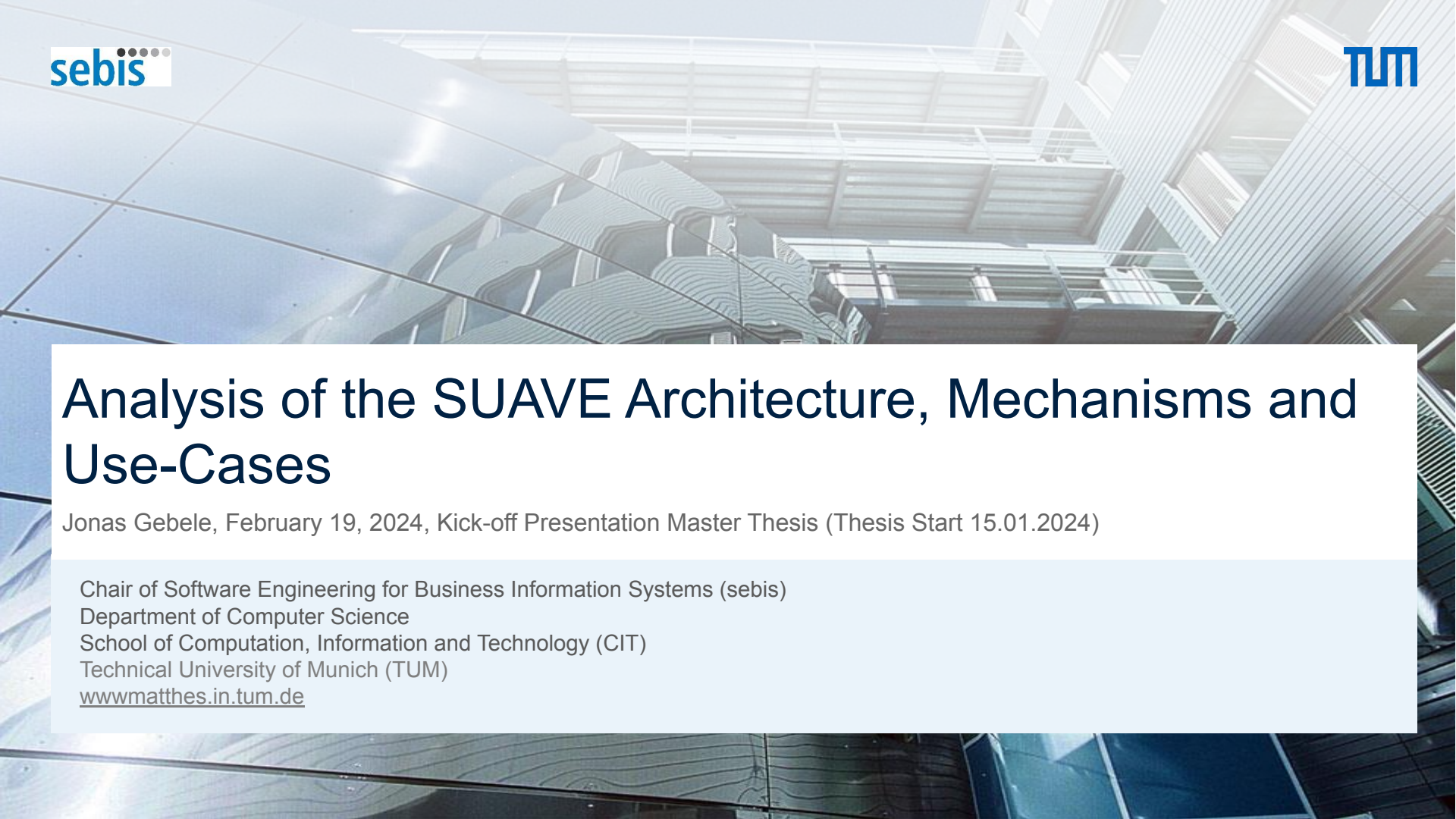


Analysis of the SUAVE Architecture, Mechanisms and Use-Cases

Jonas Gebele, February 19, 2024, Kick-off Presentation Master Thesis (Thesis Start 15.01.2024)

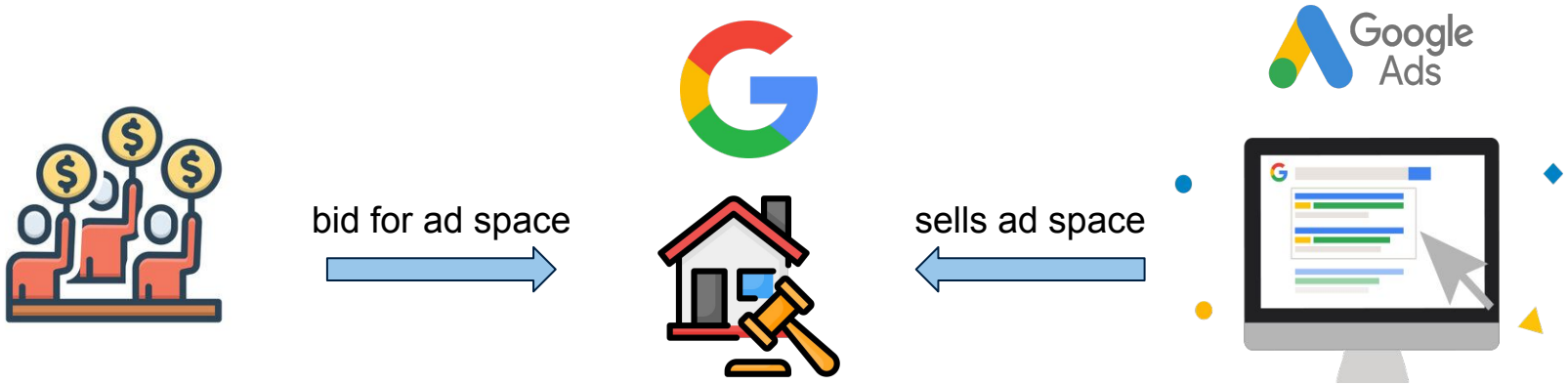
Chair of Software Engineering for Business Information Systems (sebis)
Department of Computer Science
School of Computation, Information and Technology (CIT)
Technical University of Munich (TUM)
wwwmatthes.in.tum.de

Outline

1. Motivation and Background Information
2. Problem Statement
3. Research Objectives
   - 3.1. Analysis of SUAVE System Architecture and Mechanisms
   - 3.2. Analysis of the Development Process for SUAVE Applications (SUAPPs)
   - 3.3. Analysis of Potential Use-Cases of SUAPPs
4. Timeline

Auction Mechanisms in Digital Advertising

Motivation and Background Information



- Auctions ubiquitous across the internet
- Google Ads employs auction process to allocate ad space
- Centralized auction systems, while efficient, pose risks
  - **Collusion** among participants or with the auctioneer
  - **Censorship or preferential treatment**
  - **Conflicts of interest** (auctioneer has stakes in the outcome)

Auction Mechanisms in Digital Advertising

Motivation and Background Information

Marketing Brew

Google exec says company adjusted ad auctions to meet revenue goals

It's "possible" that rates were upped as much as 10% in some instances, Google Ad VP Jerry Dischler testified during the Department of...

21.09.2023

- Auctions ubiq
- Google Ads e
- Centralized au
  - **Collusion** among participants or with the auctioneer
  - **Censorship or preferential treatment**
  - **Conflicts of interest** (auctioneer has stakes in the outcome)

Decentralizing Ad Auctions

Motivation and Background Information

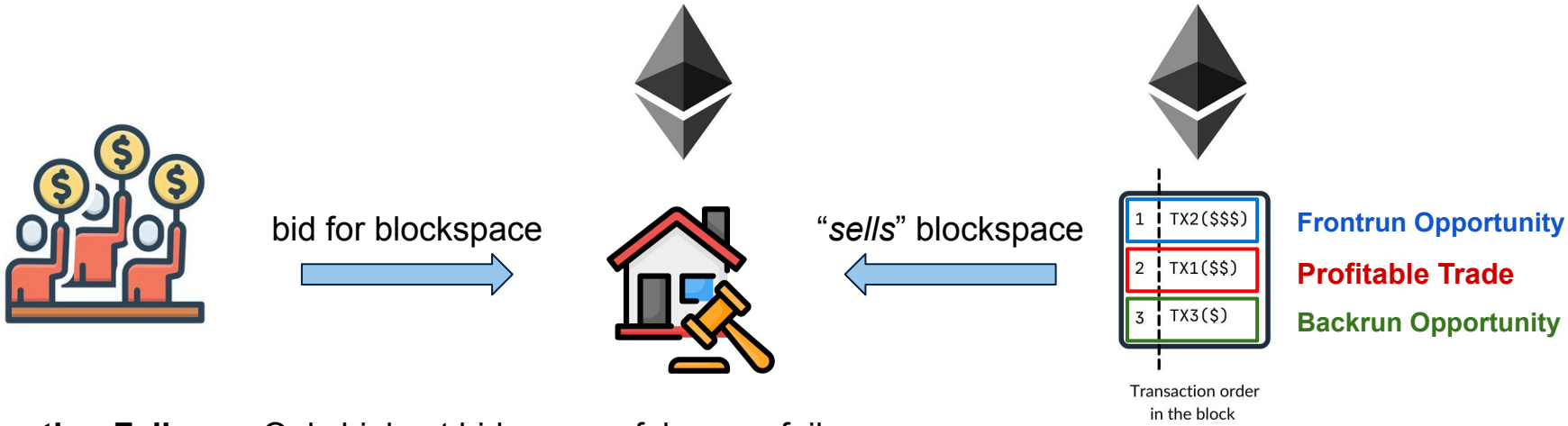
Decentralized Auctions: Implementing decentralized auctions using Ethereum-based smart contracts

+ Enhanced Transparency
+ Reduced Conflict of Interest
+ Minimized Corruption and Censorship

- Excessive transparency introduces new challenges like strategic manipulation

Ethereum Blockspace Auction

Motivation and Background Information



Transaction Failures: Only highest bid successful, some fail
Public Bids: All bids are visible, vulnerable to exploitation/front-running
Last-Moment Bidding: Incentive to wait until expected deadline, causing network congestion
Network Gaming: Anticipated peak times, can be targeted for disruption

Decentralizing auctions addresses key issues, introduces new challenges
Cryptography may be used to obscure bids, preventing exploitation by sophisticated actors

Outline

1. Motivation and Background Information
2. Problem Statement
3. Research Objectives
   - 3.1. Analysis of SUAVE system architecture and mechanisms
   - 3.2. Analysis of the Development Process for SUAVE Applications (SUAPPs)
   - 3.3. Analysis of Potential Use-Cases of SUAPPs
4. Timeline

Trusted Execution Environments

Problem Statement

Encrypt bids to hide content, replace trust of central entity by cryptography

Trusted **E**xecution **E**nvironments safeguard sensitive operations by isolating trusted apps from the main OS, enhancing data security and operational integrity

- Isolation of Sensitive Operations
  Isolates trusted applications from general OS vulnerabilities
- Protection of Critical Data
  Shields critical data within protected hardware
- Enhanced Privacy for Transactions
- Replaces centralized trust with cryptographic guarantees within TEEs

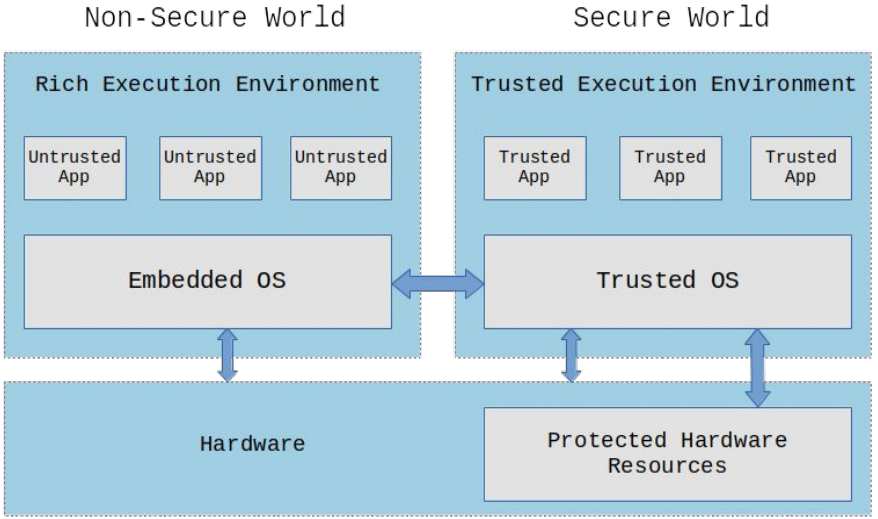


Image: https://sergioprado.blog/introduction-to-trusted-execution-environment-tee-arm-trustzone/

Trusted Execution Environments

Problem Statement

1. User encrypts transaction using the public key of the TEE (*xPub*) Kettle of the smart contract
2. User submits encrypted transaction, **bids remain confidential**
3. A private key (*xPriv*) securely managed by the TEE Kettle can be used to decrypt the data
4. After the TEE Kettle have performed the confidential computations, results are attested (signed and verified) and can be verified

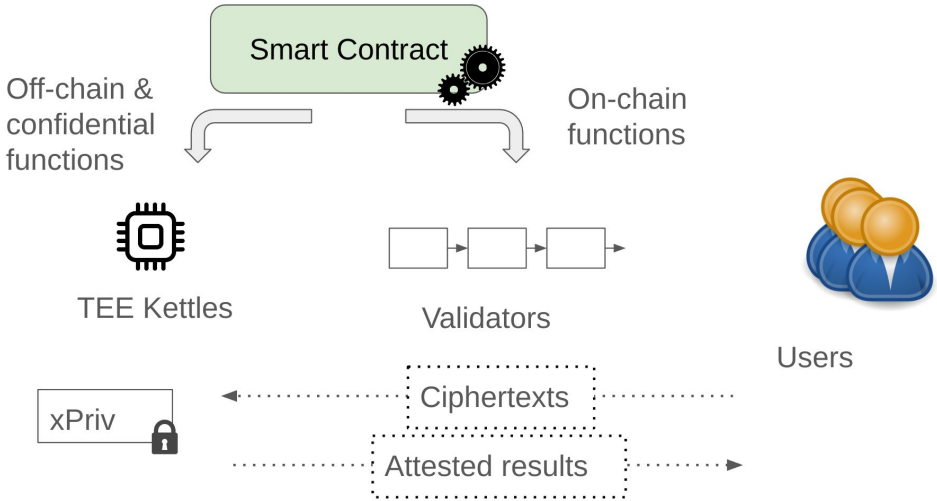


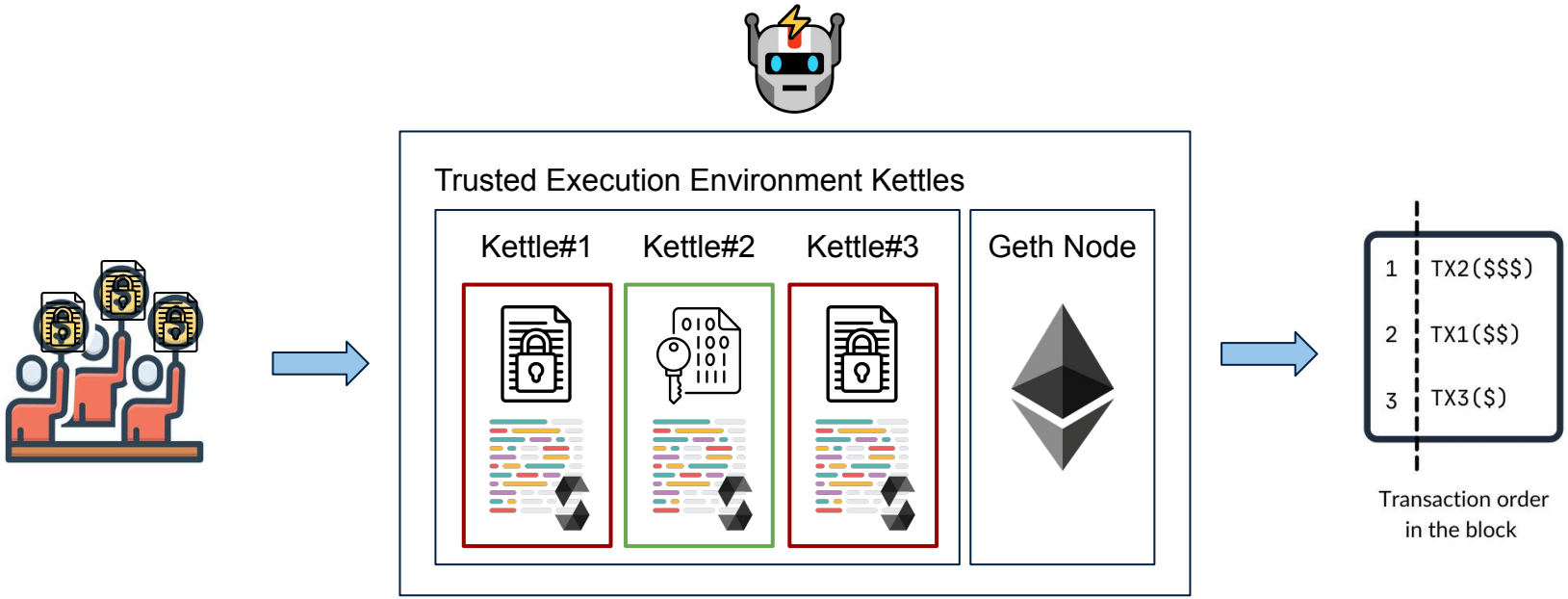
Image: https://writings.flashbots.net/suave-tee-coprocessor

SUAVE (Single Unifying Auction for Value Expression)

Problem Statement

Originally build to fix trust-issues in blockspace auctions on Ethereum
But can be also used for lots of other applications like Google ads auction

Extend functionality of Ethereum node with TEEs and Precompiles



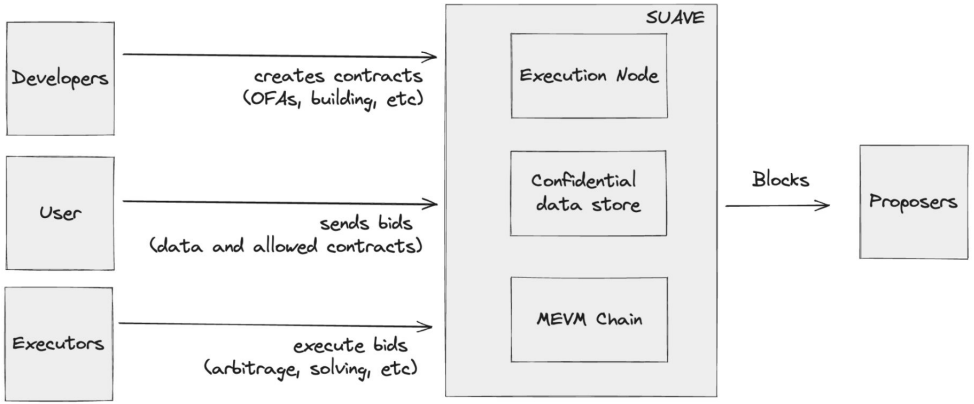
Outline

1. Motivation and Background Information
2. Problem Statement
3. Research Objectives
   - 3.1. Analysis of SUAVE system architecture and mechanisms
   - 3.2. Analysis of the Development Process for SUAVE Applications (SUAPPs)
   - 3.3. Analysis of Potential Use-Cases of SUAPPs
4. Timeline

Analysis of SUAVE System Architecture and Mechanisms

Research Question 1

Many different stakeholders interacting with the system



Ongoing Research

- Consensus
- Output Validity
- Economic Security Model
- TEE Key Distribution/Management

Image: https://writings.flashbots.net/suave-tee-coprocessor

Analysis of Development Process for SUAVE Applications (SUAPPs) and Potential Use-Cases of SUAPPs

Research Question 2 + 3

Analyze Toolchain for Development

Identify Trust-Issues or Conflict of Interests with Existing Auction Platforms

Development of SUAPPs

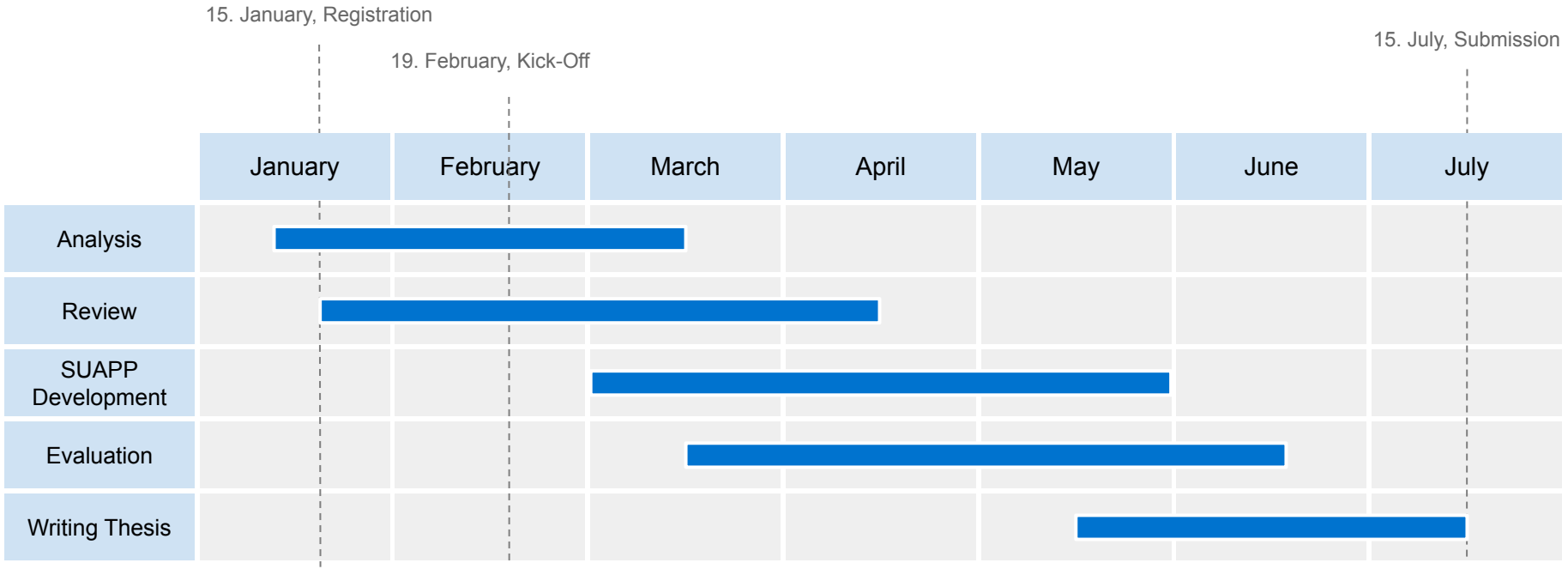
- Smart Contract using existing Precompiles
- Development of own Precompiles inside the TEEs

Outline

1. Motivation and Background Information
2. Problem Statement
3. Research Objectives
   - 3.1. Analysis of SUAVE system architecture and mechanisms
   - 3.2. Analysis of the Development Process for SUAVE Applications (SUAPPs)
   - 3.3. Analysis of Potential Use-Cases of SUAPPs
4. Timeline

Timeline and Future Work

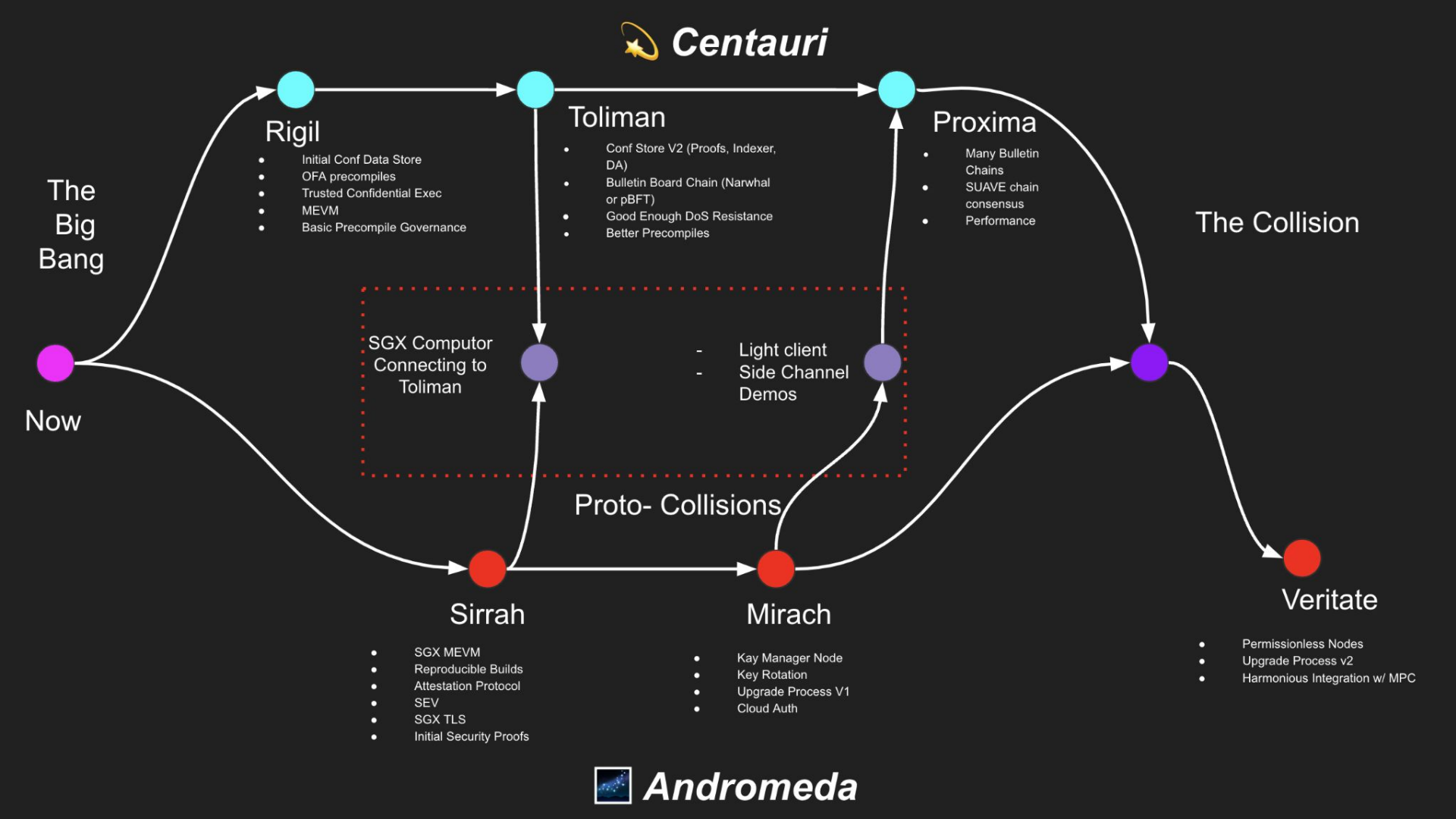
Timeline



Jonas Gebele
jonas.gebele@in.tum.de

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

Boltzmannstraße 3
85748 Garching bei München


Centauri
Rigil
Initial Conf Data Store
OFA precompiles
Trusted Confidential Exec
MEVM
Basic Precompile Governance
Toliman
Conf Store V2 (Proofs, Indexer, DA)
Bulletin Board Chain (Narwhal or pBFT)
Good Enough DoS Resistance
Better Precompiles
Proxima
Many Bulletin Chains
SUAVE chain consensus
Performance
The Big Bang
Now
The Collision
SGX Computor Connecting to Toliman
- Light client
- Side Channel Demos
Proto- Collisions
Sirrah
SGX MEVM
Reproducible Builds
Attestation Protocol
SEV
SGX TLS
Initial Security Proofs
Mirach
Kay Manager Node
Key Rotation
Upgrade Process V1
Cloud Auth
Veritate
Permissionless Nodes
Upgrade Process v2
Harmonious Integration w/ MPC
Andromeda