Analysis of the SUAVE Architecture, Mechanisms and Use-Cases

Jonas Gebele, July 22, 2024, Final Presentation Master Thesis

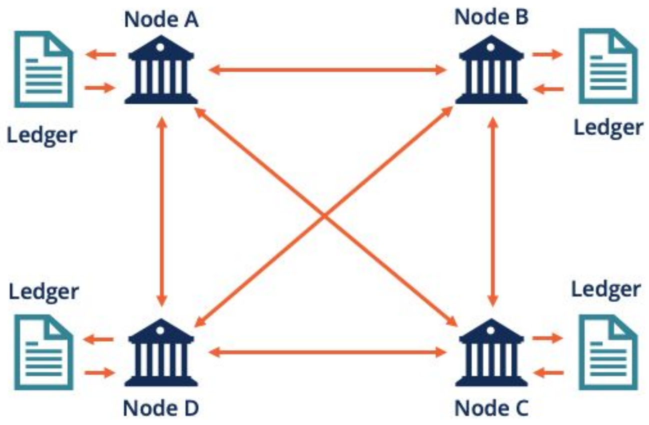
Chair of Software Engineering for Business Information Systems (sebis)
Department of Computer Science
School of Computation, Information and Technology (CIT)
Technical University of Munich (TUM)
wwwmatthes.in.tum.de

Outline

Blockchain Fundamentals: Trust Through Transparency

Blockchain Fundamentals

- Replaces trust in centralized entities
- Enables self-verification through public data
- Allows full history verification

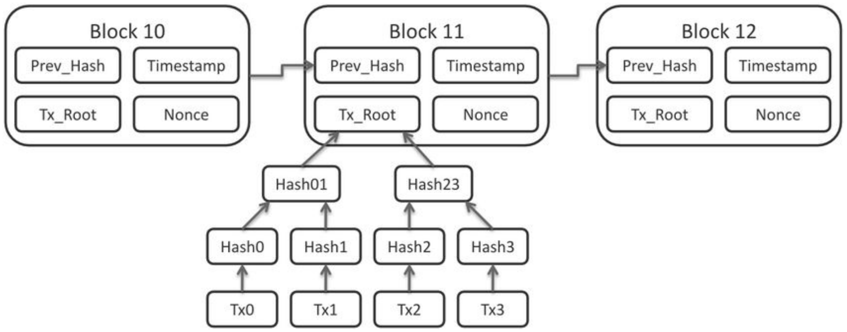


Bitcoin Example

- Public transaction data
- Independent verification of balances and transfers
- System integrity through transparency

The Transparency Trade-off

- Transparency crucial
- **May have unintended consequences**



Blockchain Auctions: Promise vs. Reality

publish bids

Potential Benefits

+ Decentralized bidding process
+ Transparency in winner selection
+ Reduced risk of fraud

Unexpected Challenges

- Bid visibility
- Last-minute bidding issues
- Vulnerability to attacks

Blockchain transparency can be a double-edged sword

Solution: **Confidential Transactions**

Privacy Solutions for Blockchain Auctions

1. publish **hashed bids**

2. reveal bids

Cryptographic Approaches

- Commit and Reveal Scheme
- Secure Multi-Party Computation (MPC)
- Fully Homomorphic Encryption (FHE)

Limitations of Crypto-based PPSC

- Application-specific implementations
- Developer effort for each use case
- Performance overhead or additional interaction needed

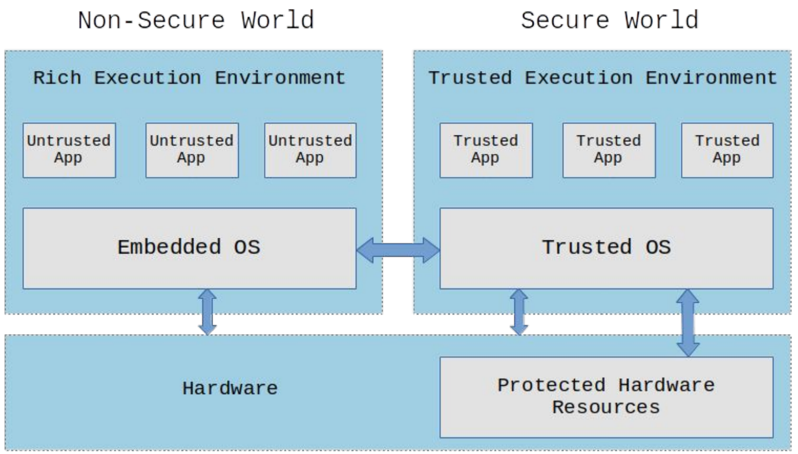
A New Direction: **Trusted Execution Environments** (TEEs) as **general-purpose solution**

Outline

Trusted Execution Environments: Enhancing Blockchain Privacy

What is a TEE?

- Secure, isolated operating environment
- Separate from main operating system
- Protects against interference and data leakage



Key Features

- Isolation from other software and OS
- Protection from host owner access
- Ensures confidentiality of running applications

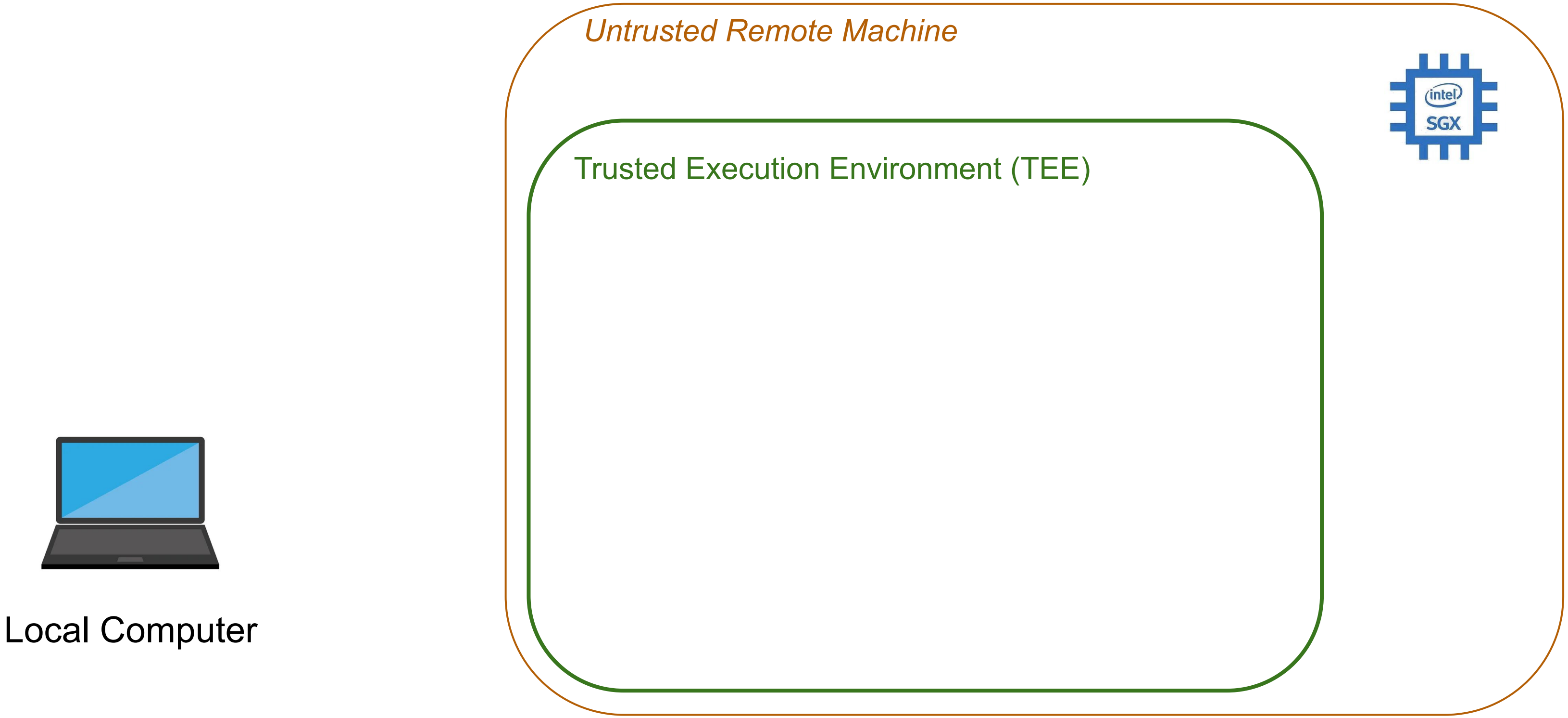
TEEs + Blockchain = Privacy-Preserving Smart Contracts

- Integrate blockchain systems within TEEs
- Enable confidential smart contract execution
- Empower developers to create privacy-preserving applications
- Intel SGX, Framework for TEEs on Intel CPUs

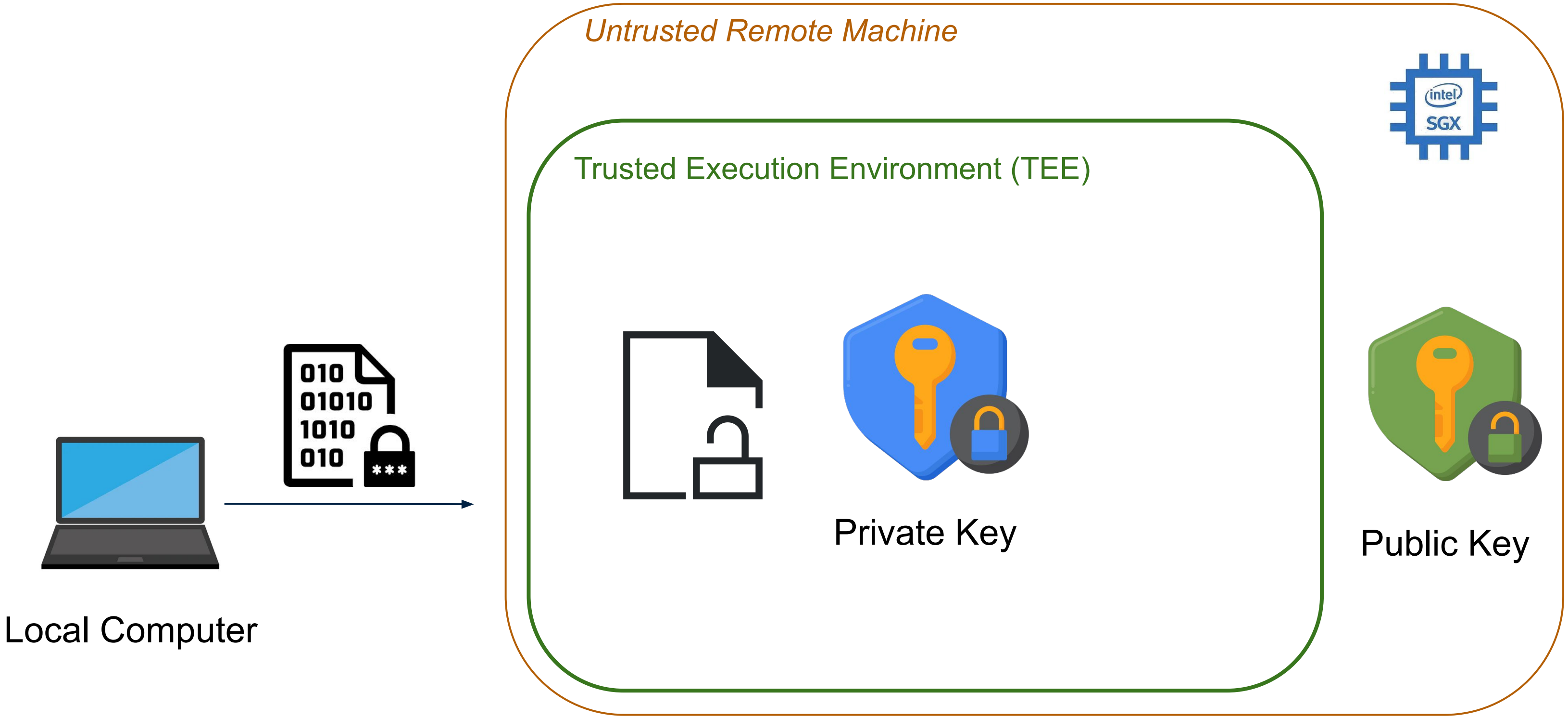
Outline

1. Motivation and Background Information
2. Problem Statement
3. Research Objectives
    3.1. SUAVE Architecture and Mechanisms
    3.2. Development Process and Use-Cases of SUAPPs
4. Limitations
5. Conclusion

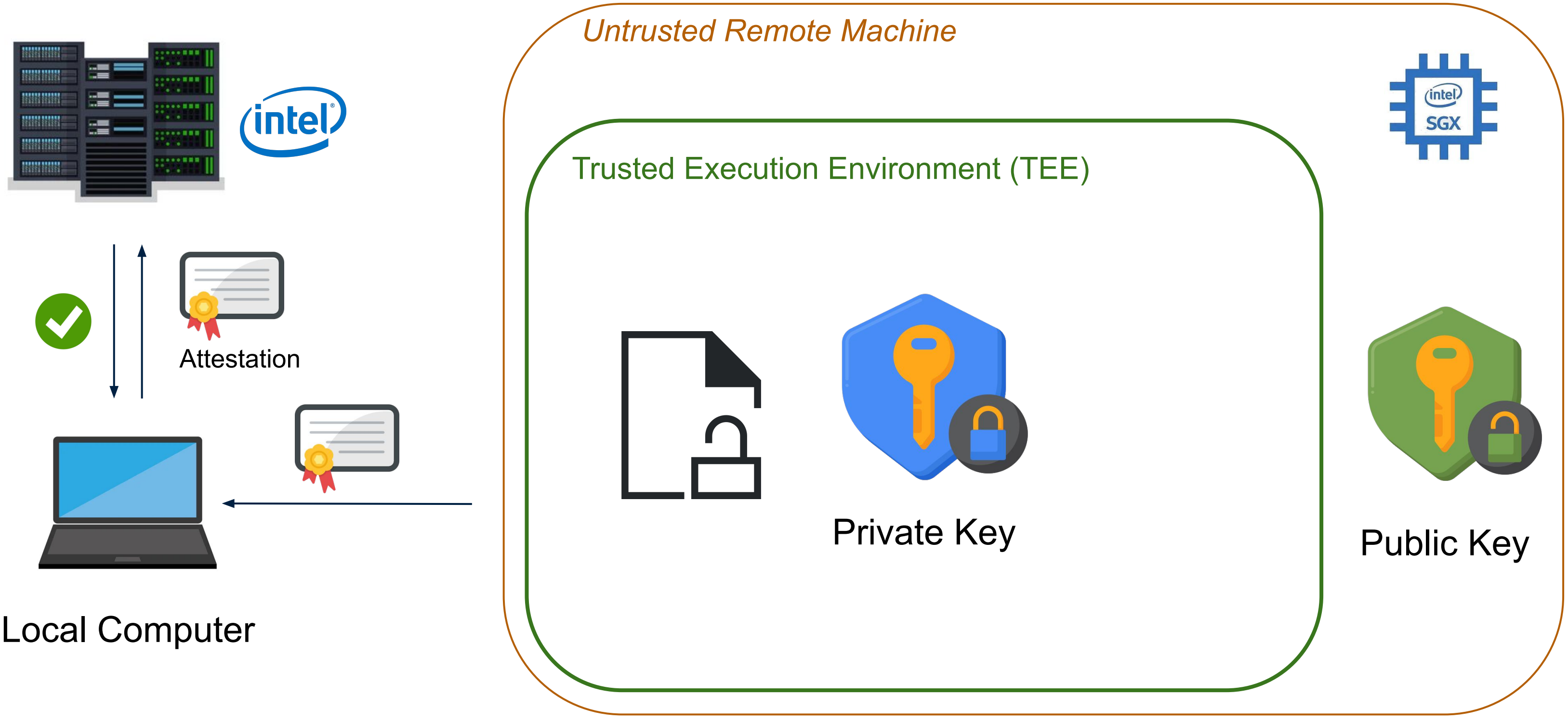
(simplified) SUAVE Architecture: Building Blocks



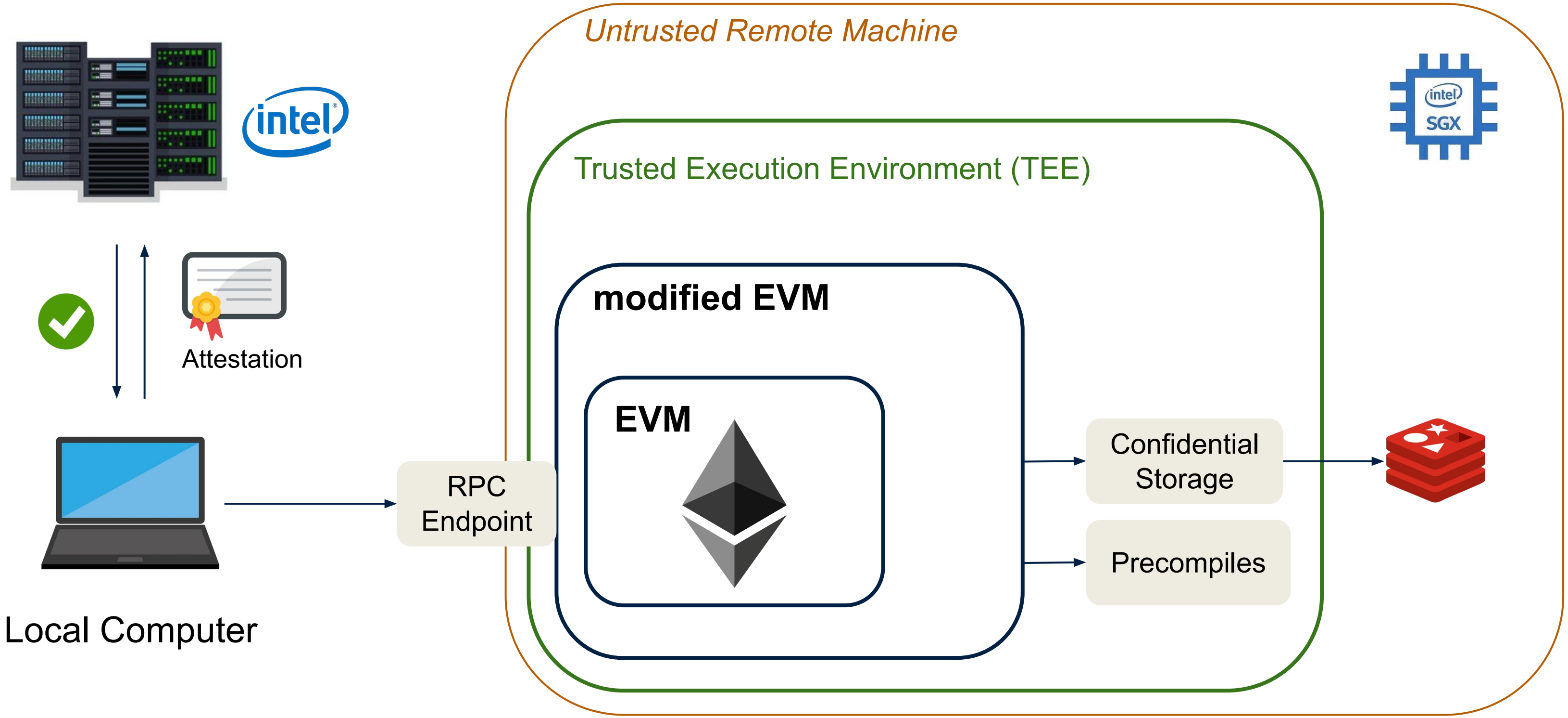
(simplified) SUAVE Architecture: Building Blocks



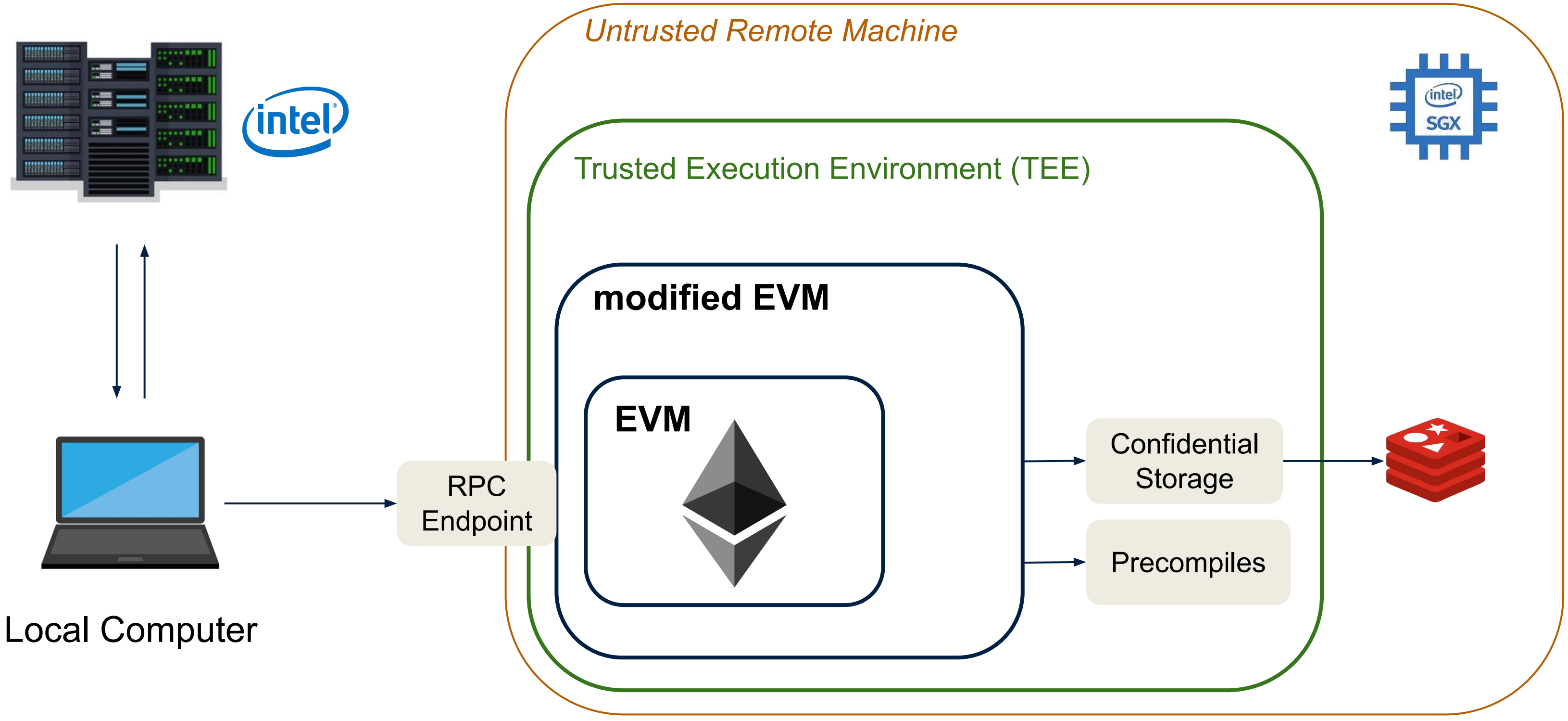
(simplified) SUAVE Architecture: Building Blocks



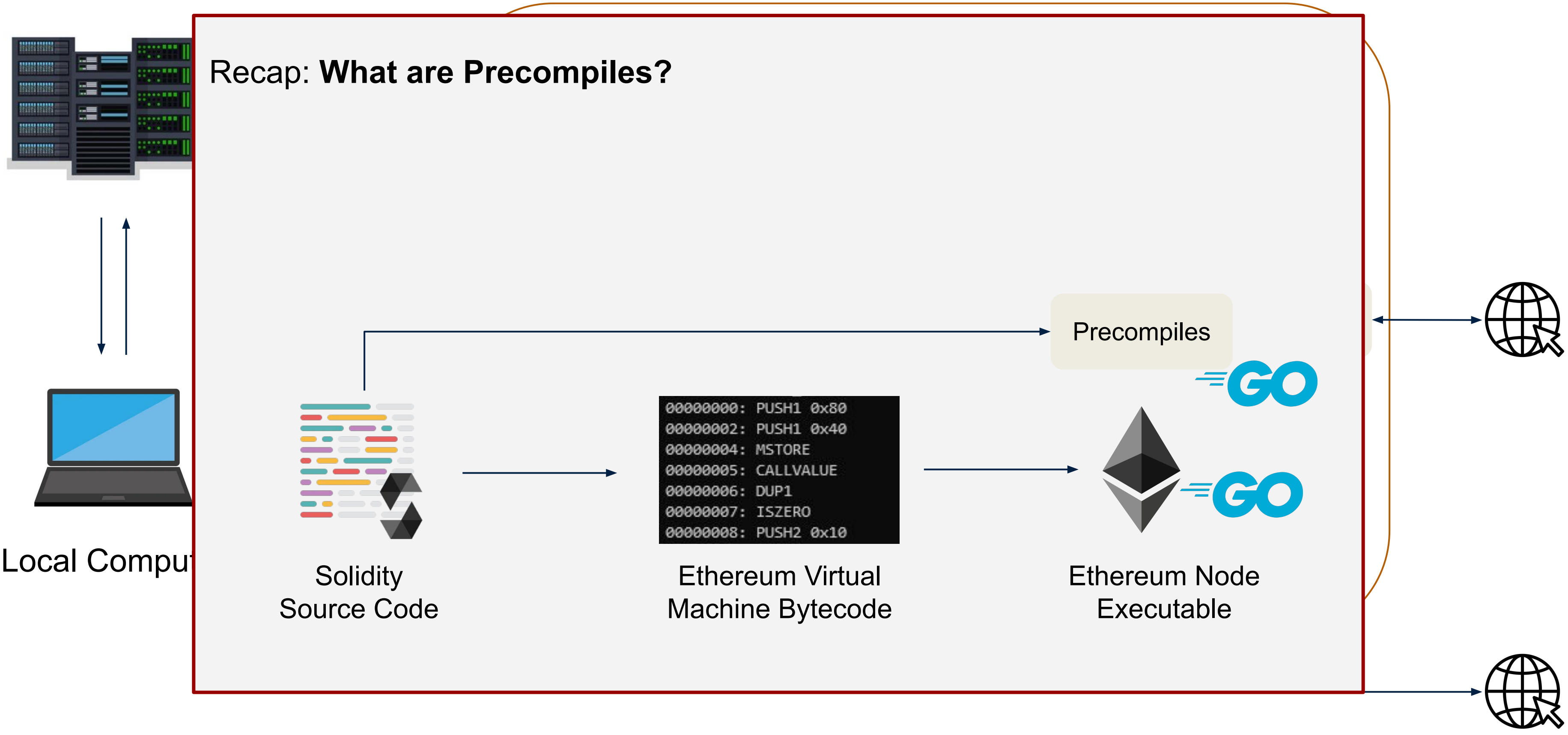
(simplified) SUAVE Architecture: Building Blocks



(simplified) SUAVE Architecture: Building Blocks



(simplified) SUAVE Architecture: Building Blocks



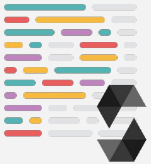
(simplified) SUAVE Architecture: Building Blocks

Local Comput

Recap: **What are Precompiles?**

```
function recoverSignature(bytes32 hash, uint8 v, bytes32 r, bytes32 s)
public view returns (address) {
    address signer = ecrecover(hash, v, r, s);
    require(signer != address(0), "Invalid signature");
    return signer;
}
```

Precompiles



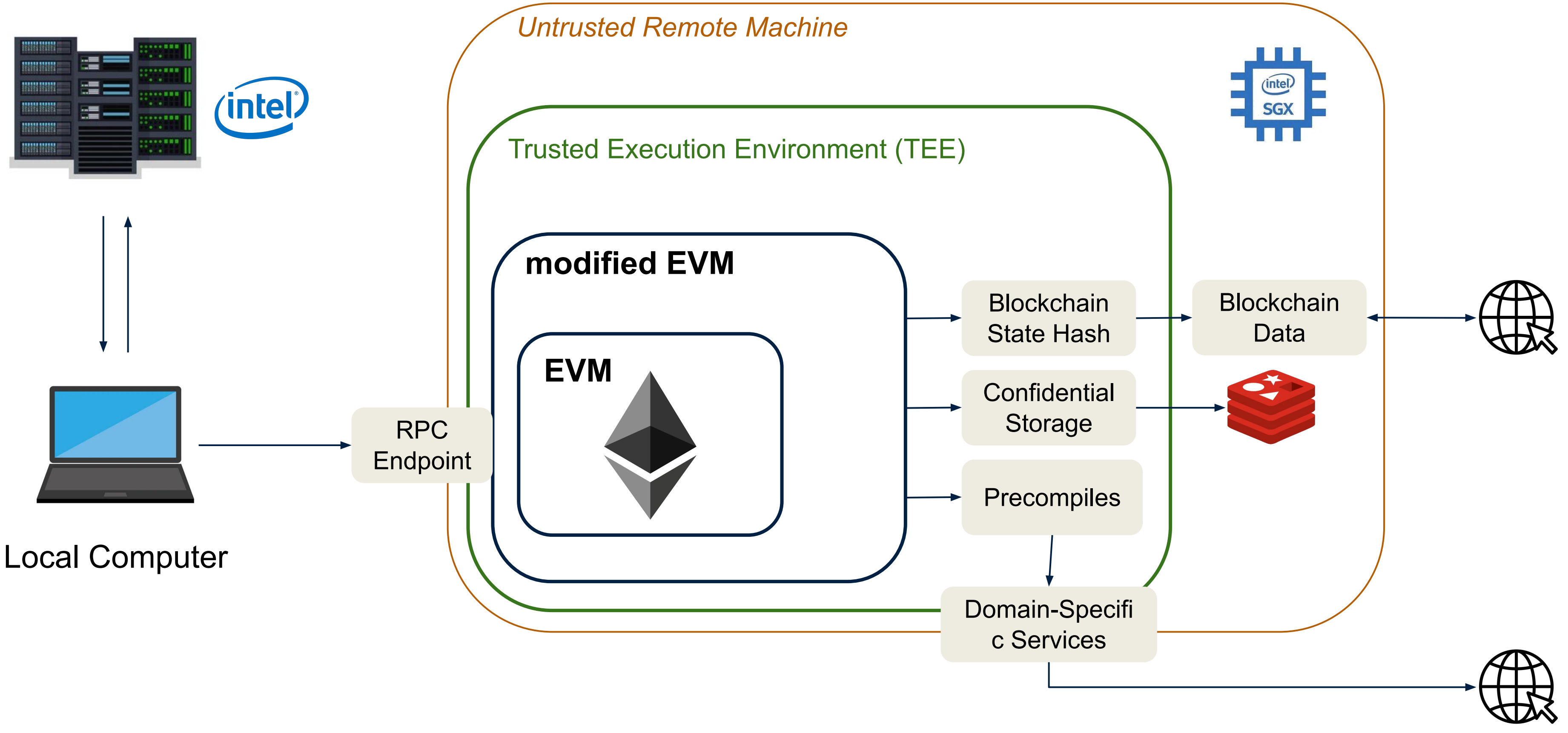
Solidity
Source Code

```
00000000: PUSH1 0x80
00000002: PUSH1 0x40
00000004: MSTORE
00000005: CALLVALUE
00000006: DUP1
00000007: ISZERO
00000008: PUSH2 0x10
```

Ethereum Virtual
Machine Bytecode

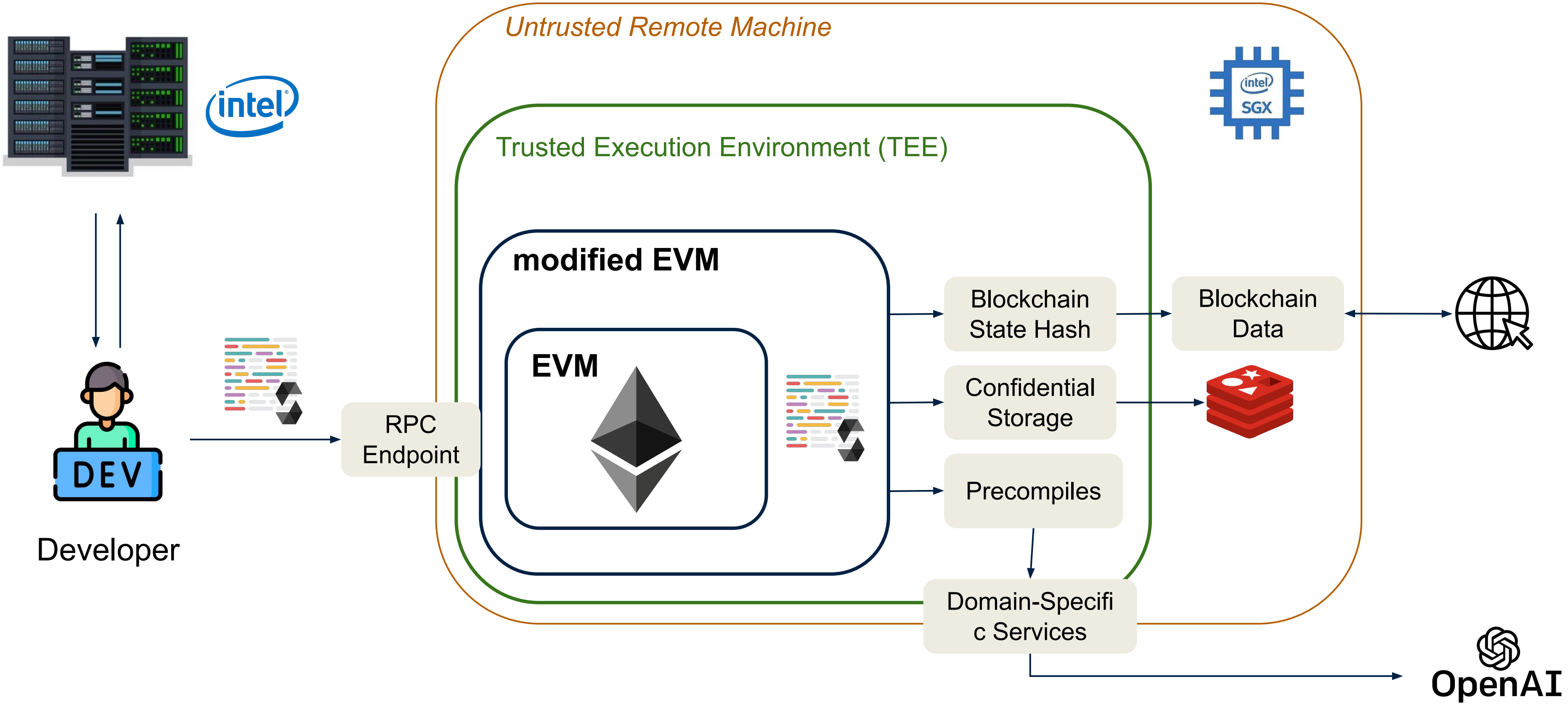
Ethereum Node
Executable

(simplified) SUAVE Architecture

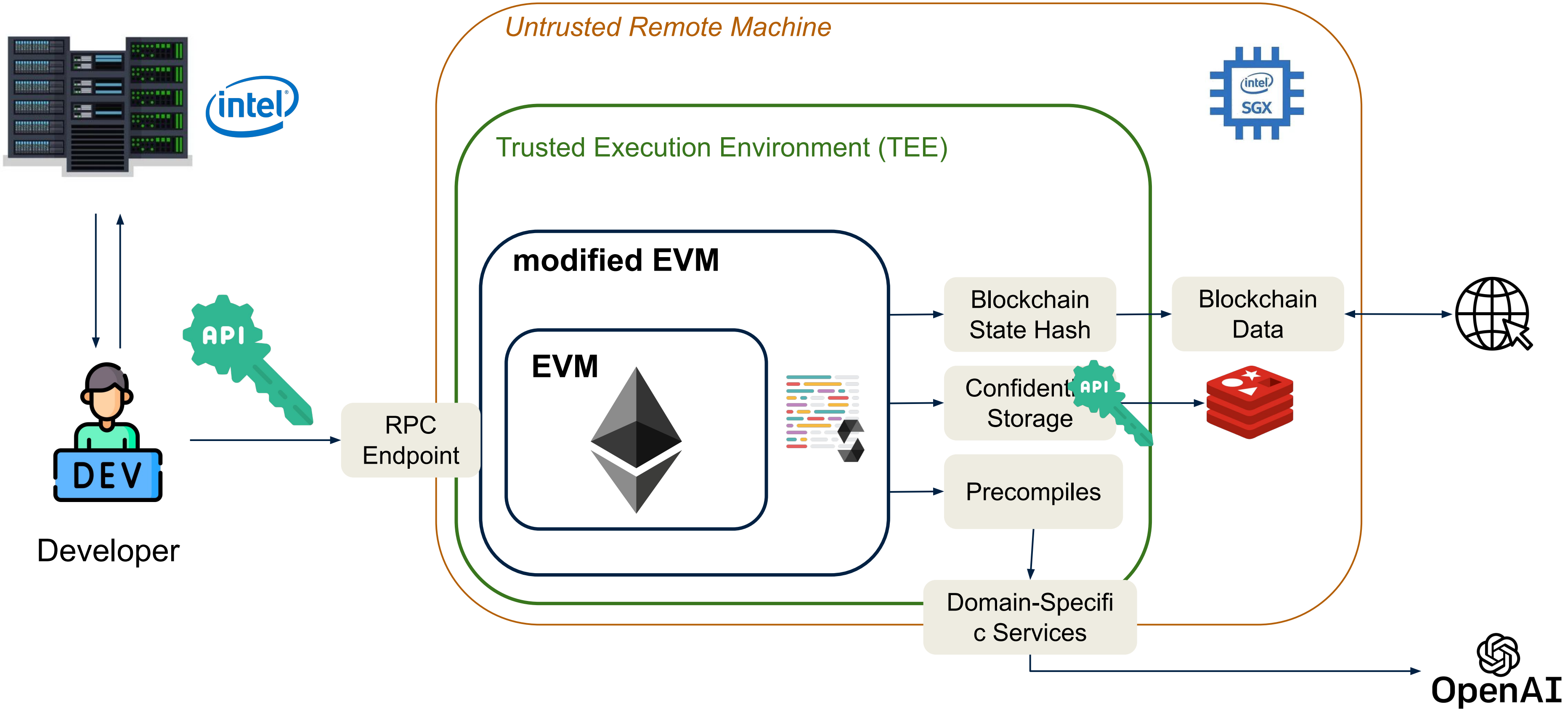


Outline

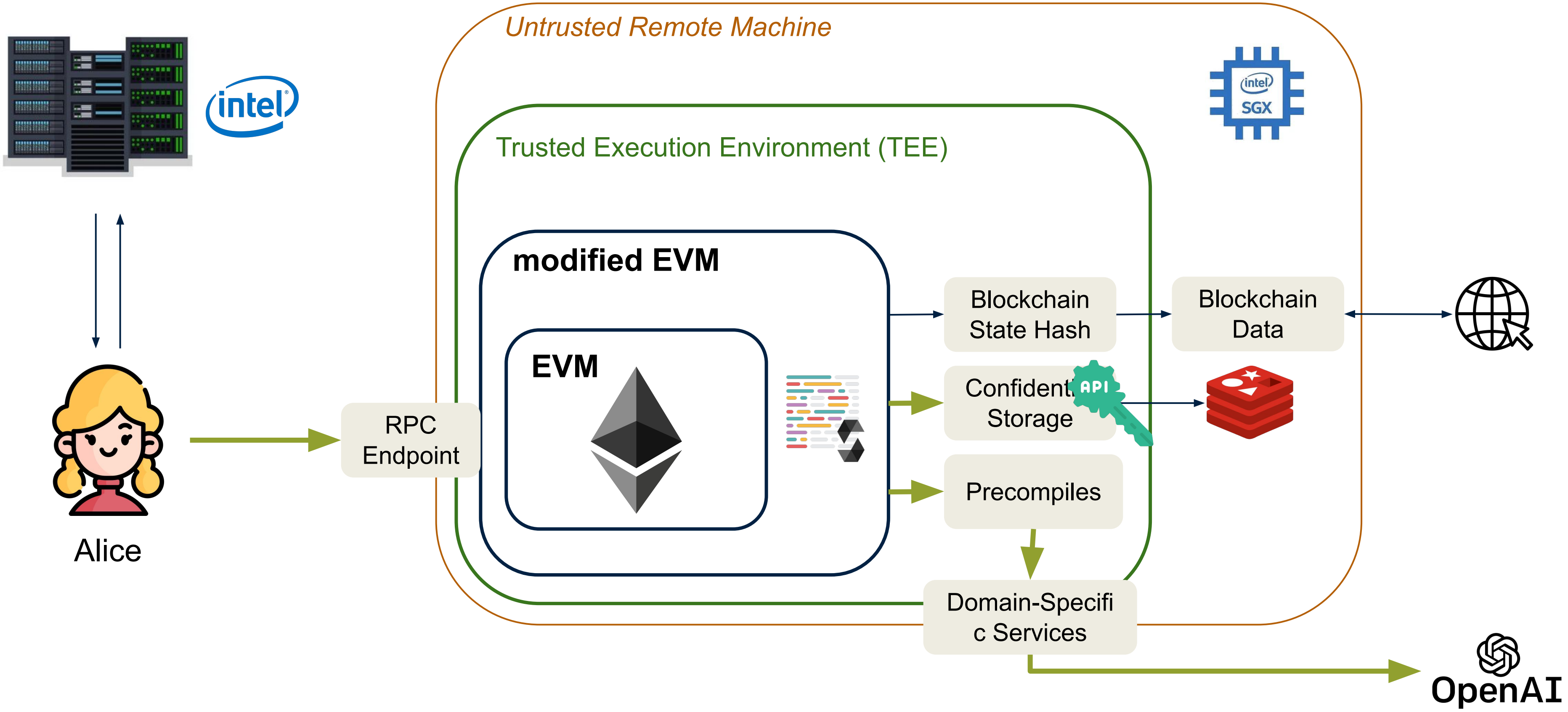
Development and Use-Cases of SUAPPs



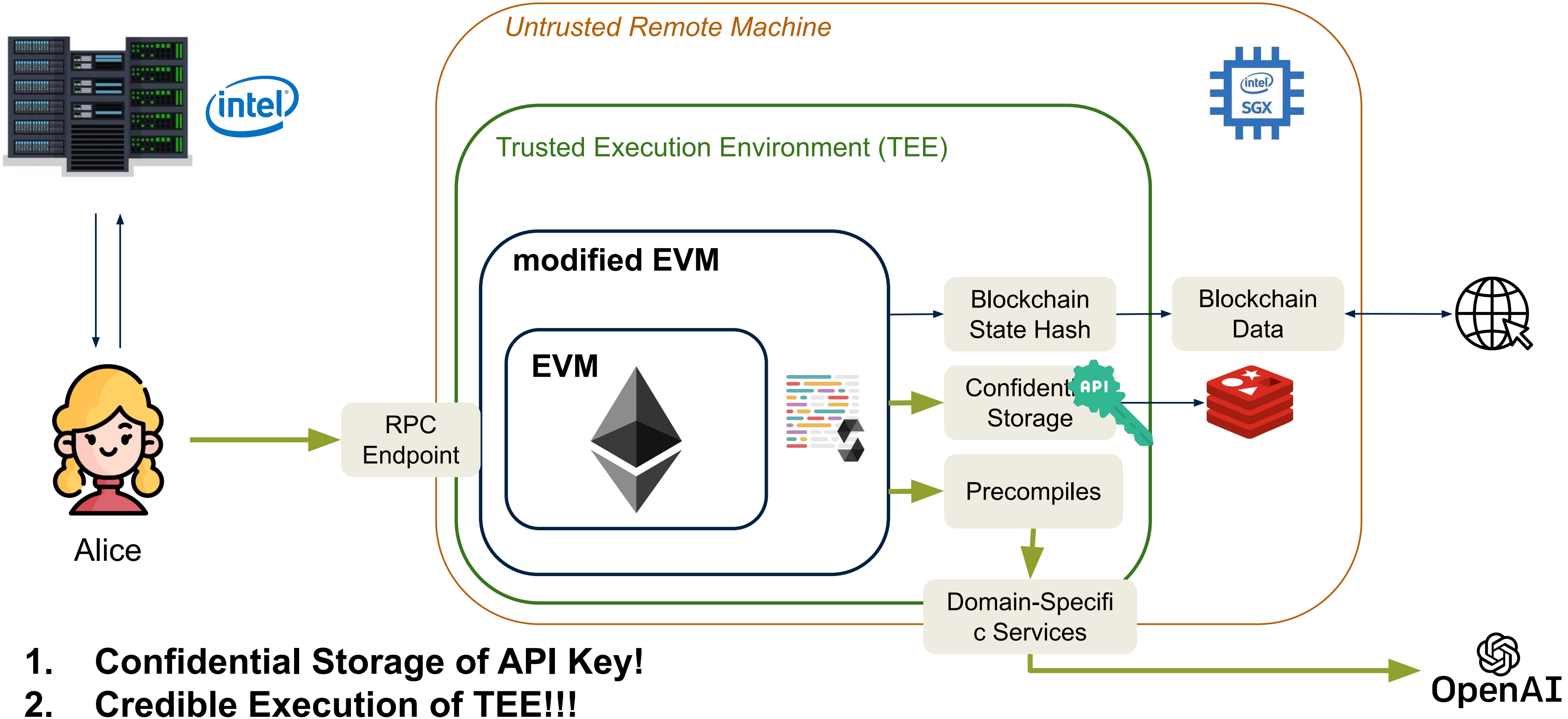
Development and Use-Cases of SUAPPs



Development and Use-Cases of SUAPPs

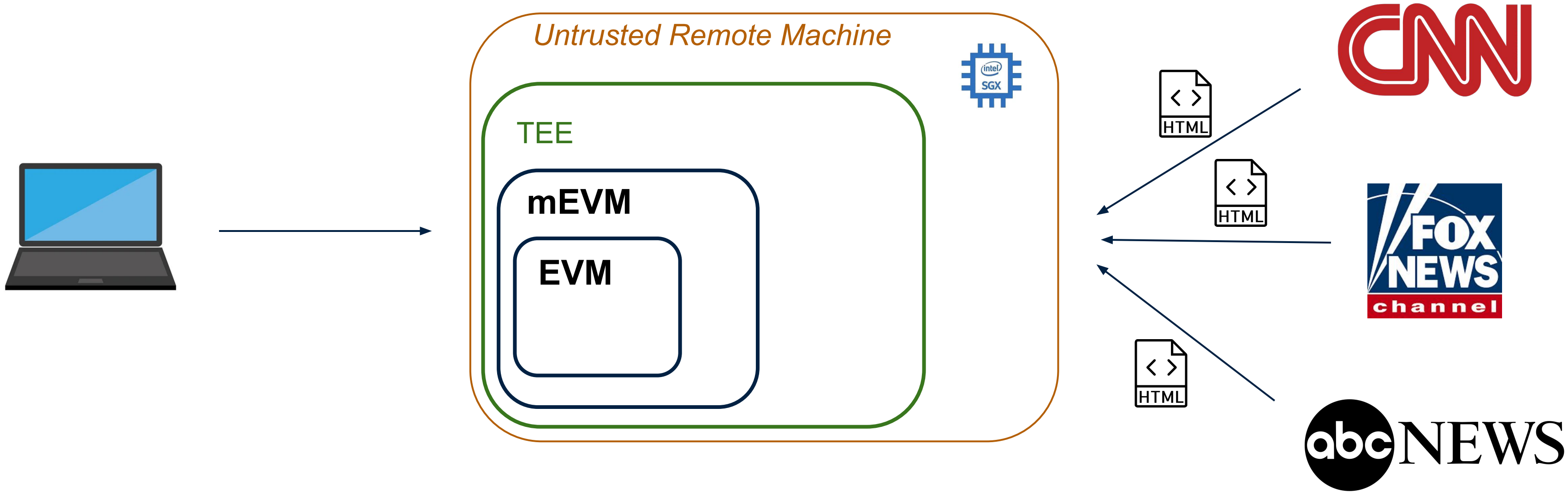


Development and Use-Cases of SUAPPs



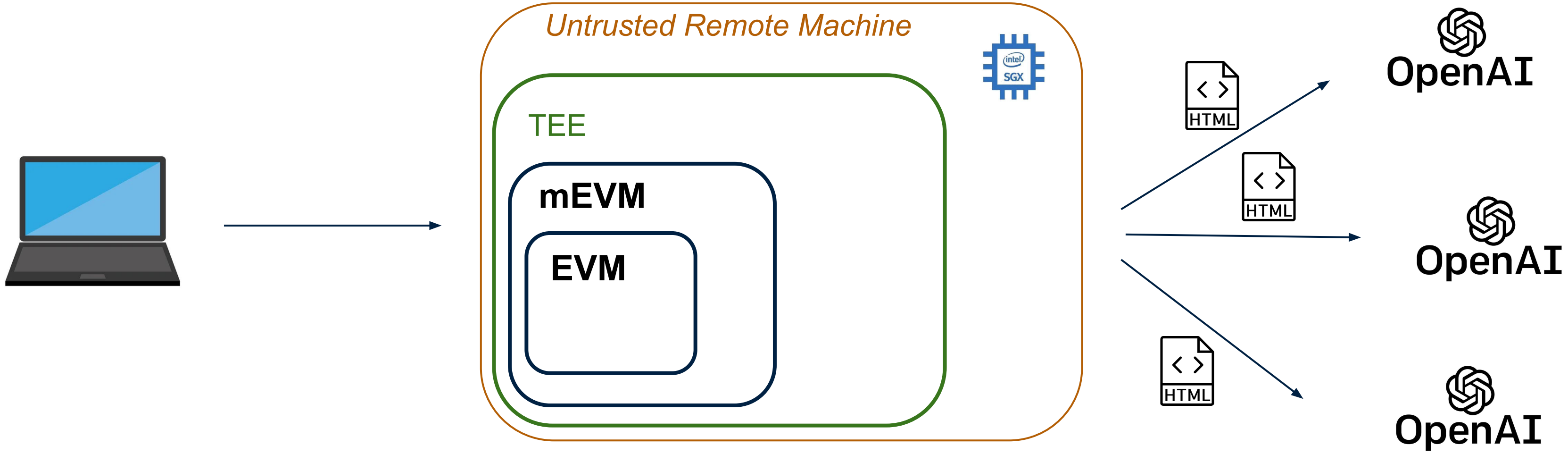
1. **Confidential Storage of API Key!**
2. **Credible Execution of TEE!!!**

Development and Use-Cases of SUAPPs



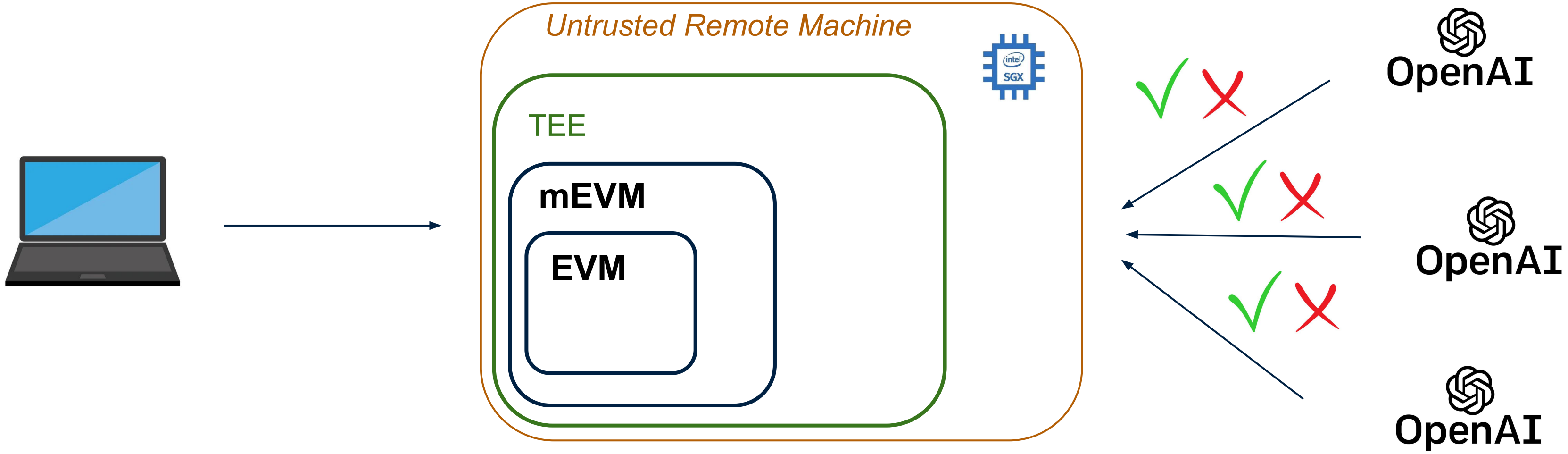
Use-Case: **Presidential Election Betting Contract**

Development and Use-Cases of SUAPPs



Prompt: “*Given the news websites content, is Joe Biden still a contender at the presidential election? Answer with 0 if yes, answer with 1 if no, answer with -1 if you don't know given that information. Just return an integer.*”

Development and Use-Cases of SUAPPs

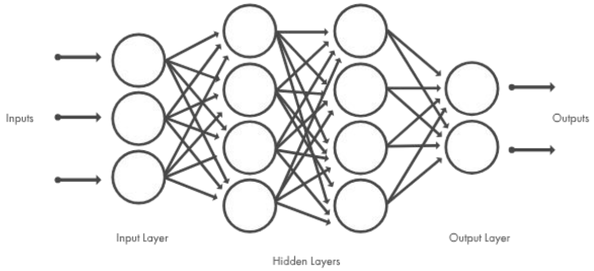


Thesis SUAPP Use Cases

1. Tackling Sybil Attacks of Cryptocurrency Airdrops using Twitter Authentication

2. Bridging Centralized Exchanged Liquidity to Decentralized Finance
   https://github.com/jonasgebele/snapshot-finance

3. Machine Learning on Confidential Data



Outline

1. Motivation and Background Information
2. Problem Statement
3. Research Objectives
   3.1. SUAVE Architecture and Mechanisms
   3.2. Development Process and Use-Cases of SUAPPs
4. Limitations
5. Conclusion

SUAVE and Intel SGX: Challenges and Limitations

Security Concerns

- Intel SGX vulnerabilities
- Confidentiality preservation risks

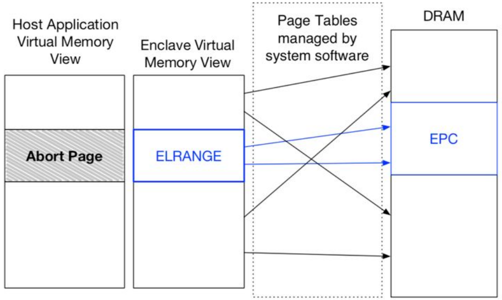
Practical Considerations

- TEE runtime storage limited to 128 MB
- Sealing data to disk introduces side-channel attack risks

Trust and Dependency Issues

- Remote attestation relies on Intel's infrastructure
- Potential for SGX compromise (though extremely difficult)

SGX.Fail



Outline

Conclusion

Solving the Auction Problem

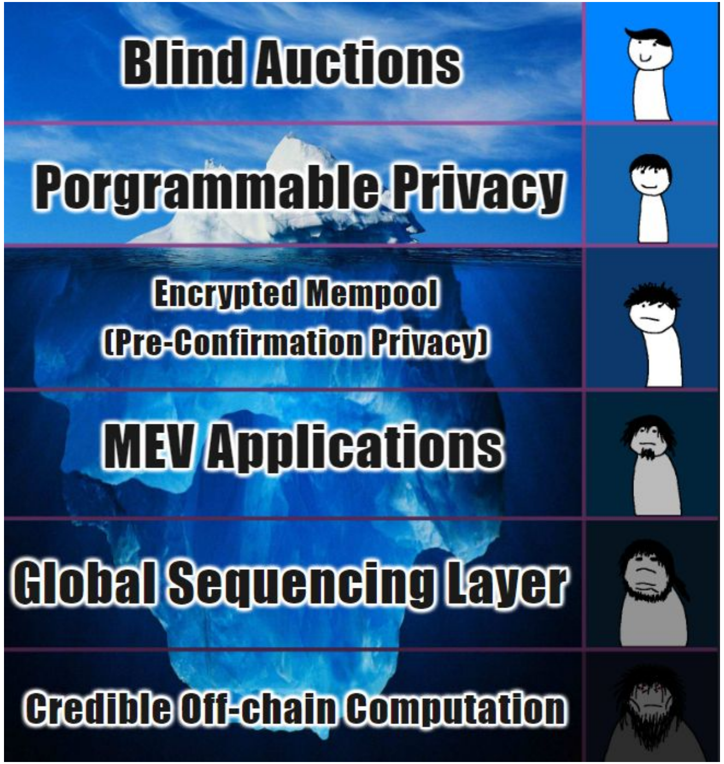
SUAVE as a privacy-preserving blockchain solution

Programmable Privacy, beyond specific use cases

MEV Mitigation
Pre-confirmation privacy eliminates front-running

Blockchain and Payload agnostic
Relaying layer for all blockchains

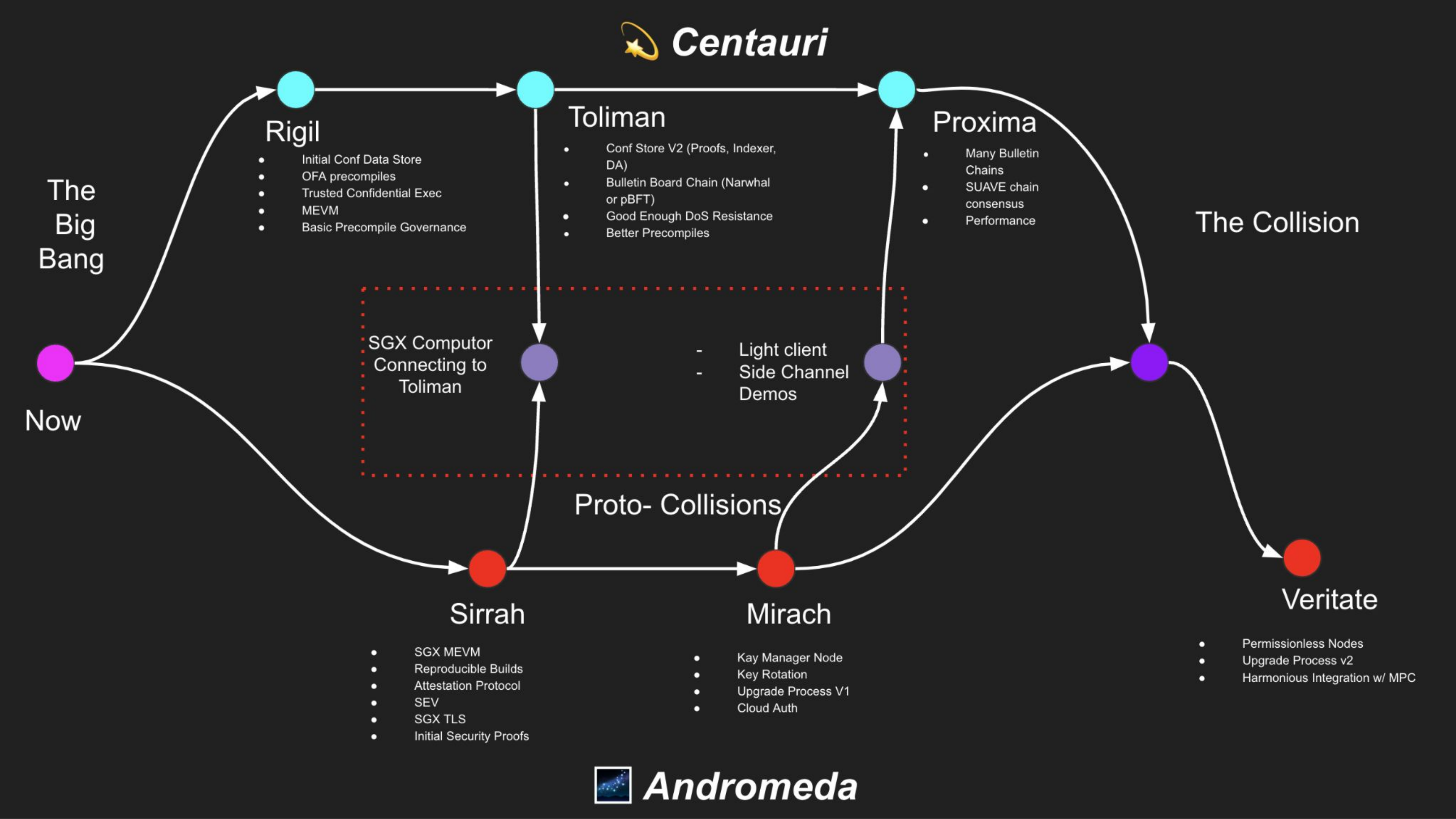
Platform for credible off-chain computation
Reimagining blockchain use cases



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