Special thanks to Andrew Miller for his valuable feedback and reviews.

:::info

:bulb: Check out the awesome-sgx-blockchain repo on GitHub.

:::

:::info

Check out the announcement tweet.

:::

Introduction

Trusted Execution Environments (TEEs) and SGX (Software Guard Extensions) plays a critical role in enhancing security by offering hardware-based memory encryption and isolation. SGX allows user-level code to allocate private regions of memory called enclaves, which are designed to be protected from processes running at higher privilege levels. This granular level of control and protection applies to other high-level processes running at the time, and even the operating system. By leveraging SGX, developers can enhance the security of their applications and protect sensitive code and data from unauthorized access.

TEEs and Intel SGX have various use cases in blockchain technology. They enable secure smart contract execution, ensuring the protection of sensitive data and logic. TEEs also facilitate confidential transactions, preserving privacy and confidentiality. Additionally, TEEs support privacy-preserving data analytics and secure oracles, ensuring data integrity and confidentiality. They can also play a role in decentralized identity systems, securely managing private keys and enabling secure authentication on the blockchain.

Blogs & Writings

- The Sting Framework (SF)
- PROF: Fair Transaction-Ordering in a Profit-Seeking World
- Block Building inside SGX
- Running Geth within SGX: Our Experience, Learnings and Code
- SGX-Based Backrunning and Covert Channels
- TEE-based Smart Contracts and Sealing Pitfalls
- MEV-SGX -- A sealed bid MEV auction design
- Avalanche Bridge: Secure Cross-Chain Asset Transfers Using Intel SGX
- SUAVE Andromeda and Helios
- Blockchains + TEEs Day 1 Summary
- Blockchains + TEEs Day 2 Summary
- Blockchains in Trusted Execution Environments (TEEs)
- Intel® SGX and Blockchain: The iExec End-to-End Trusted Execution Solution
- Why trusted execution environments will be integral to proof-of-stake blockchains
- 4 Ways to Compare Trusted Execution Environments and Zero-Knowledge Proofs
- Trusted Execution Environments and the Polkadot Ecosystem
- How Intel® SGX is hardening data privacy on the blockchain
- How Secret Network Uses SGX

Papers

- Intel SGX Explained

- SoK: TEE-assisted Confidential Smart Contract
- When Blockchain Meets SGX: An Overview, Challenges, and Open Issues
- TEBDS: A Trusted Execution Environment-and-Blockchain-supported IoT data sharing system
- Lessons Learned from Blockchain Applications of Trusted Execution Environments and Implications for Future Research
- A Blockchain Based on Gossip
- Blockchain and Trusted Computing: Problems, Pitfalls, and a Solution for Hyperledger Fabric
- Security with Intel SGX: Enhancements, Applications and Privacy
- SGXonerated: Finding (and Partially Fixing) Privacy Flawsin TEE based Smart Contract Platforms Without Breaking the TEE
- Town Crier: An Authenticated Data Feed for Smart Contracts
- Teechain:Scalable Blockchain Payments using Trusted Execution Environments
- LucidiTEE: A TEE-Blockchain System for Policy-Compliant Multiparty Computation with Fairness
- Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts
- PoQ: A Consensus Protocol for Private Blockchains Using Intel SGX
- *General SGX-related papers from various topics, such as cloud computing, operating systems, and others*.

Slides

- SGX and cryptocurrencies
- [SUAVE smart contract programming model:

TEE-based smart contracts for block building]
(https://docs.google.com/presentation/d/18Fc1_TfMW3BEi_GF0YJtyrNyU1c2r9989WM9nC6-QtE/edit#slide=id.g225be28fa40_2_76)

Useful Websites

- sgx.fail
- Town Crier: An Authenticated Data Feed for Smart Contract

Codes & Repos

- geth-sgx-gramine - Geth (Go-Ethereum)-in-SGX provides an example of running go-ethereum in SGX by Flashbots.
- FHE-in-TEE - A framework to run Fully Homomorphic Encryption (FHE) computations (especially using the SEAL library) on Trusted Execution Environments (TEEs). This framework also includes a scheme to verifiably offload some computations to untrusted hardware for faster evaluation.
- Ledger BOLOS - A simple, portable and flexible Trusted Computing Base environment for blockchain applications.
- luckychain/lucky - Proof of luck Intel SGX and IPFS based blockchain.
- Town Crier - Town Crier: an Authenticated Data Feeds for Smart Contracts
- infobiac/eEVM - Enclave ready EVM (eEVM) is an open-source, standalone, embeddable, C++ implementation of the Ethereum Virtual Machine. http://microsoft.com/blockchain
- hyperledger-labs/fabric-private-chaincode - This lab enables Secure Chaincode Execution using Intel SGX for Hyperledger Fabric.
- hyperledger/avalon - Hyperledger Avalon (formerly Trusted Compute Framework)
- smartcontractkit chainlink - node of the decentralized oracle network, bridging on and off-chain computation.
- skalenetwork/sgxwallet - sgxwallet is the first-ever opensource high-performance hardware secure crypto wallet that is

based on Intel SGX technology.

- Secret Network - Secret Network is the first blockchain with data privacy by default for smart contracts and entirely based on Intel SGX technology. https://scrt.network/
- phala-blockchain - Phala Network is a blockchain-based confidential computing cloud.
- substraTEE - Trusted Off-Chain Compute Framework for substrate blockchains
- automata - Web 3.0 Realized with Traceless Privacy and Seamless Compatibility.

Videos & Talks & Workshops

- Private Smart Contracts are Worth the Price of the SGX, Andrew Miller
- SGX Panel: Andrew Miller, Jonathan Passerat Palmbach, Phil Daian, Justin Drake
- Enabling Cross Chain Transfers Using SGX
- Blockchains + TEEs: Day 1
- Blockchains + TEEs: Day 2

Other

- SGX Block Builder on Etherscan

Let’s talk

If you have any comments or any project, please don't hesitate to reach out to me. I would love to hear your thoughts and engage in a conversation with you.

- Twitter
- Mail
- Website