Ethereum's primary aim is to offer its users access to trustless computing and storage capabilities. Historically, achieving trustless computation on Ethereum necessitated the execution and verification of computations across all nodes on the network. However, advancements in proving techniques have ushered in a new era where much of this computation can be offloaded to off-chain processors. This shift enables on-chain validators to simply verify the outcomes, transforming Ethereum into a global, immutable record-keeping platform.

Through the utilization of computation proofs, including Zero-Knowledge (ZK) Proofs and Trusted Execution Environments (TEEs), the integrity of transactions can be assured. These proofs, once posted on Ethereum, provide not only a verifiable timestamp but also a secure, unalterable history of computations.

TEEs stand out by offering a means to delegate computations to third-party providers without compromising data privacy or the integrity of operations. It allows code to be executed in a trusted, isolated area of a specialized processor in the server, without the ability for even the owner or administrator of the server to inspect memory, or to tamper with the code.

It enables verifiable confidential computation by providing tools with which anyone can verify that the code is running in an authentic TEE processor. This feature is particularly valuable for decentralized applications (dApps) demanding high levels of integrity, confidentiality, and resistance to censorship. By integrating with blockchain technology, TEEs enrich smart contract environments with secure, off-chain computing capabilities.

The necessity for verifiable off-chain computation stems from the inherent mistrust in opaque, external systems. By submitting computation proofs, whether through TEEs, zero-knowledge, or optimistically, protocols can mitigate trust issues, allowing for off-chain computations without compromising on security or transparency (more info in this post on the different trust models and their tradeoffs). This verifiable approach is critical for dApps requiring off-chain computing resources, ensuring data privacy and integrity without forsaking trust.

ML proof techniques tradeoffs table by Marlin Protocol on Eth Denver

While coverage and hype have been around zk-coprocessors, TEEs are currently more practical from a latency and cost perspective, particularly in applications demanding both high performance and privacy, such as AI and ML frameworks. Unlike ZKPs that confirm the correct execution of a program, TEEs ensure that only the authorized configuration and execution occur, offering a unique layer of security for certain dApps.

TEEs also offer a crucial feature known as remote attestation (“RA”), which significantly enhances their utility by enabling trust verification in off-chain TEE nodes. This process allows entities, including smart contracts, to verify the integrity of a TEE node, thereby establishing a secure communication pathway. This mechanism is crucial for thwarting attempts by malicious actors to impersonate TEE operations, thereby safeguarding transmitted data.

An example of TEEs and Remote Attestation in production is illustrated by Puffer Finance's anti-slashing technology, heralded by Binance Research as a "key innovation."

Binance Research´s mention of Puffer´s anti-slashing tech in their Restaking post.

This system includes a "Secure-signer" that utilizes TEEs to prevent slashing events, such as double-signing, and a Remote-attestation-verifier (RAVe), enabling on-chain validation of a TEE's execution environment. Puffer's RAVe facilitates permissionless validator integration by authenticating TEE-produced evidence and managing validator public keys on the blockchain.

I believe TEE coprocessors, and particularly Automata, are undervalued given their multifaceted applications:

1. Trustless MEV-Supply Stack Development with Flashbots:

Instead of relying on a trusted service (Flashbots, as a centralized operator, running MEV-share or MEV-boost), the off-chain service can be executed within a TEE. Automata is facilitating the development of a trustless TEE-based MEV supply stack for Suave through its on-chain remote attestation verifier.

1. Enhancing Layer 2 Scalability and Security:

Through the implementation of SGX (TEE) alternate proofs, Automata enables a multi-proving model that boosts the liveness and security for optimistic and zk rollups. Scroll's adoption of Automata's technology highlights the growing confidence in TEEs.

1. Enabling On-Chain AI and DEPIN verification:

Automata's technology paves the way for on-chain AI by making Large Language Model (LLM) outputs accessible to smart contracts. Furthermore, many DePiN projects need to verify on-chain that their inclusion to the network is being done on a unique and genuine device (attesting that you are using a mobile phone, or a computer).

Trustless MEV-Supply Stack Development with Flashbots:

Instead of relying on a trusted service (Flashbots, as a centralized operator, running MEV-share or MEV-boost), the off-chain service can be executed within a TEE. Automata is facilitating the development of a trustless TEE-based MEV supply stack

for Suave through its on-chain remote attestation verifier.

Enhancing Layer 2 Scalability and Security:

Through the implementation of SGX (TEE) alternate proofs, Automata enables a multi-proving model that boosts the liveness and security for optimistic and zk rollups. Scroll's adoption of Automata's technology highlights the growing confidence in TEEs.

Enabling On-Chain AI and DEPIN verification:

Automata's technology paves the way for on-chain AI by making Large Language Model (LLM) outputs accessible to smart contracts. Furthermore, many DePiN projects need to verify on-chain that their inclusion to the network is being done on a unique and genuine device (attesting that you are using a mobile phone, or a computer).

To achieve this, Automata is launching a modular attestation chain

, which will go live as an Eigenlayer AVS. This app-chain will aggregate remote attestations from off-chain computations, making them publicly verifiable and easily accessible. It will also involve the implementation of new tokenomics

that will introduce token sink mechanisms.

SUAVE

The current existing MEV supply stack relies on off-chain trusted providers such as Flashbots (running MEV-share and MEV-Boost) and CowSwap (offering MEVBlocker).

Trusted actors in the MEV supply chain

MEV-share (aka Flashbots Protect), for instance, enables searchers to access user orders through an Order Flow Auction (OFA), ensuring value generated from MEV activities is returned to users. A critical aspect of its system is the 'matchmaker' role designed to match user txns with searcher bundles effectively. This is currently a permissioned position held by Flashbots, which aims to prevent bidding wars that could reduce the value returned to users and guarantee that bundles meet specific validity conditions, ensuring MEV gains are rightfully distributed.

Flashbots has a solution for its centralization concerns. They aim to create a platform (called “SUAVE”) where these trusted actors can be replaced by a set of specialized privacy-preserving hardware, TEEs alongside a censorship-resistant chain managing them. It will be something similar to a “TEE Party”.

SUAVE's emphasis on privacy serves dual purposes:

1. Decentralizing the MEV-supply chain by enabling users to internalize the value of their MEV without relying on permissioned environments like off-chain auctions.

2. Introducing "programmable privacy," allowing users to control the release of information to relevant parties during MEV negotiations, promoting scalability and avoiding closed, permissioned markets.

Decentralizing the MEV-supply chain by enabling users to internalize the value of their MEV without relying on permissioned environments like off-chain auctions.

Introducing "programmable privacy," allowing users to control the release of information to relevant parties during MEV negotiations, promoting scalability and avoiding closed, permissioned markets.

Implementation of programmable privacy involves interconnected TEEs called "Kettles," where users interact with SUAVE's applications via Confidential Compute Requests (CCRs). This approach shifts sensitive data computation off-chain, minimizing trust requirements.

Infographic from Eden Network of how Suave will work and the different parties involved

SUAVE's implementation involves two stages:

- Centauri

: Initially, execution nodes operate in a trusted or centralized manner, maintaining the status quo.

- Andromeda

: Execution nodes transition to TEEs (SGX), reducing reliance on centralized operators and expanding participation. This intermediate layer is expected to launch with SUAVE's mainnet in Q2 '24.

https://x.com/jon_charb/status/1764818338041966614?s=20

Centauri

: Initially, execution nodes operate in a trusted or centralized manner, maintaining the status quo.

Andromeda

: Execution nodes transition to TEEs (SGX), reducing reliance on centralized operators and expanding participation. This intermediate layer is expected to launch with SUAVE's mainnet in Q2 '24.

https://x.com/jon_charb/status/1764818338041966614?s=20

Future plans for SUAVE include augmenting SGX with cryptography (ZK and FHE) to further reduce trust requirements, although this is not immediate.

This network of TEEs still needs some on-chain implementation to: a) verify that computation and the code being run off-chain on these TEEs nodes is what it is supposed to be, and b) establish a secure channel to them.

Flashbots explains this concept in their latestblog post where they walk through an implementation of a simple TEE co-processor:

We need to use the remote attestation feature of TEE so that our smart contracts can verify that a message came from a TEE. To do this, we add a new precompile so that Solidity code is allowed to generate a remote attestation. It's a bit like Gramine for Solidity, since we are exposing a fairly low-level interface directly to the smart contract environment. While generating an attestation requires an SGX processor, verifying the attestation occurs entirely on-chain. The remote attestation is just a certificate chain, and the verifier is written in Solidity.

We specifically use the Automata-V3-DCAP repository

, which is an open source Solidity library for verifying these.

I have also included some screenshots from Flashbots´ latest blog writing with highlights of Puffer and Automata mentions:

On the left, Flashbot´s latest blog writing on TEE coprocessors for when "Andromeda" goes live; on the right, GitHub contest for dev experimentation with TEEs and remote attestation. Highlighted are mentions of Automata and Puffer.

While both Puffer Finance and Automata are mentioned by Flashbots, Automata's verifier is recommended due to impending deprecation of EPID by Intel. Additionally, there have been suggestions from Phala Network (Jun Jiang) about transforming DCAP verification into a ZK-proof, which, though slower, may offer benefits in on-chain validation. This presents a trade-off spectrum, where while current zk VMs may be slow, you don´t need to verify DCAP quotes frequently.

.css-1wpjqbx{height:24px;width:24px;display:block;}

.css-1k55id8{visibility:hidden;border-radius:0.75rem;overflow:hidden;padding-left:1rem;padding-right:1rem;width:100%;display:-webkit-box;display:-webkit-flex;display:-ms-flexbox;display:flex;-webkit-box-pack:center;-ms-flex-pack:center;-webkit-justify-content:center;justify-content:center;max-width:32rem;}@media screen and (min-width: 768px){.css-1k55id8{padding-left:0px;padding-right:0px;}}.css-1k55id8>div{margin-top:0!important;margin-bottom:0!important;}

There's also consideration of using DCAP verification as a benchmark for zk, as suggested byAndrew Miller.

One "raw" way to compare existing on-chain remote attestation verifiers is by looking at historical GitHub stars of their respective repos. Includes: Puffer, Automata, Phala Network, Clique.

To summarize, SUAVE should be viewed as a big tailwind to put TEEs on the map as they integrate them into their chain and replace current trusted entities. Each SuApp, like Order Flow Auctions (OFA) or blockbuilders, will operate within a TEE forming a network called "Kettles." Verification of TEE computations and code integrity will be ensured through on-chain Remote Attestations (RAs), with Automata being the recommended solution by Flashbots for developers working on SuApps experimentation.

L2 multi-proving

L2 multi-proving offers a promising solution to the security concerns surrounding Layer 2s, especially as more assets migrate from Ethereum to L2s. Vitalik has emphasized the importance of addressing security issues within these complex systems, highlighting the potential catastrophic implications of bugs within single-prover validation setups. The need for diverse prover mechanisms becomes paramount in ensuring the integrity and security of L2 txns.

Scroll's collaboration with Automata represents a significant step towards enhancing the security of L2 networks through multi-proving. By incorporating a TEE prover as a secondary mechanism alongside traditional ZK proofs, Scroll aims to mitigate the risks associated with bugs and vulnerabilities inherent in complex software systems.

The rationale behind adopting a multi-proving approach lies in bolstering the security of L2s without compromising on finality time or significantly increasing transaction costs. By diversifying the validation mechanisms, Scroll aims to minimize the likelihood of invalid transactions infiltrating the system.

The design space for a multi-proof system on Scroll revolves around three key objectives: enhancing L2 security, maintaining reasonable finality times, and introducing minimal additional costs to L2 txns. While exploring various options for a secondary prover, including fraud proofs and alternative ZK provers, the adoption of a TEE prover emerged as the most viable solution. With negligible overhead associated with proving processes, TEE provers provide a faster and more cost-effective solution, thereby aligning with Scroll's objectives of enhancing security while maintaining operational efficiency.

Tradeoff spectrum from Scroll´s blog

The specifical implementation of the SGX (TEE) prover leverages Automata´s on-chain remote attestation verifier. It entails using a smart contract as a remote party to create a public and transparent on-chain anchor that enables trust composability — other smart contracts can also trust the computation from the enclave.

Automata-DCAP-V3-Attestation on-chain verifier being used for the verification of SGX Proofs on Scroll´s new multi-prover design

Forward-looking other zkL2s like Taiko, Linea, or even opL2s could be integrated and benefit from more diverse prover mechanisms.

Conclusion

Some liquid bets to get exposure to TEE coprocessors and take advantage of a potential rerating arising from ZK coprocessors launching soon at (expected) +1B FDVs:

TEE coprocessors comps

- $ATA: 160M FDV
- $PHA: 190M FDV
- $POND: 270M FDV

$ATA: 160M FDV

$PHA: 190M FDV

$POND: 270M FDV

Nomenclature:

- “TEEs” stands for Trusted Execution Environments, which acts as a safe space for executing critical tasks, isolated from the rest of the device's operations, and not even the hardware owner can look into.
- “SGX” is a type of TEE made by Intel, other vendors include AMD SEV and Arm TrustZone.

“TEEs” stands for Trusted Execution Environments, which acts as a safe space for executing critical tasks, isolated from the rest of the device's operations, and not even the hardware owner can look into.

“SGX” is a type of TEE made by Intel, other vendors include AMD SEV and Arm TrustZone.