Announcing Our New SUAVE Testnet: Toliman

[

suave_toliman_5

1920×1005 168 KB

](https://collective.flashbots.net/uploads/default/original/2X/5/5b093ba43f3a91d514f4bd274c9c6b7ad6a8e043.jpeg)

We are thrilled to announce the Toliman testnet, a significant milestone in our journey towards building a decentralized network for fast and private compute

. The Toliman testnet enables more powerful and private Solidity coprocessing via two new features:

- EIP-712 signature transactions

: Users can make transactions on SUAVE without switching their RPC, instead signing EIP-712 signatures that are valid SUAVE transactions no matter their RPC or connected network. Moreover, dapp developers are empowered to handle where and how their users orderflow is sent

, offering new avenues for monetization and better transacting experiences.

- TEE Kettles

: SUAVE Kettles provide fast and private compute to applications on the Toliman Testnet, and now they are in TEEs! This is the first step in a line of work to bring more secure kettles to Toliman soon! Using the same language dapp developers love, program your coprocessor in Solidity and ensure it's security with TEEs.

You can use these features live on the Toliman testnet today! To get started developing, check out our quick start documentation and our explorer. And if you're interested in playing around with the network, checkout our demo section below. In the rest of this blog post we'll briefly review each of these features and their impact.

EIP-712

[

toliman_712

1920×1005 128 KB

](https://collective.flashbots.net/uploads/default/original/2X/4/463fc7cec976883440dc790129b34cc644f7e304.jpeg)

SUAVE gives developers superpowers to create innovative apps with all the benefits of blockchain—credible compute and commitments—without the typical downsides such as slow speeds, high costs, transparency issues, and lack of web2 access. Unlike typical offchain apps, SUAVE apps are fully verifiable and transparent smart contracts with built-in access to multiple other chains. Now we're leveling up the UX with this release by removing the need for users to switch RPCs to use SUAVE

.

This new feature means SUAVE nodes are no longer restricted to the standard Ethereum protocol transaction format and now accept a more permissive format following the EIP-712 standard. Below you can see an example implementation from suave-viem, that shows how we encode and sign the EIP712 wrapper of ConfidentialRecord

, our native confidential compute request message format as spec'ed here and previously signed using a legacy signature scheme.

```
async signEIP712ConfidentialRequest( request: PreparedConfidentialRecord, ): Promise> { if (request.isEIP712 === false) throw new Error('cannot sign an EIP712 CCR with isEIP712=false')

const eip712Tx = { ...request, nonce: BigInt(request.nonce), } const rawSig = await client.signTypedData({ primaryType: 'ConfidentialRecord', message: eip712Tx, types: { Eip712Domain: [ { name: 'name', type: 'string' }, { name: 'verifyingContract', type: 'address' }, ], ConfidentialRecord: [ { name: 'nonce', type: 'uint64' }, { name: 'gasPrice', type: 'uint256' }, { name: 'gas', type: 'uint64' }, { name: 'to', type: 'address' }, { name: 'value', type: 'uint256' }, { name: 'data', type: 'bytes' }, { name: 'kettleAddress', type: 'address' }, { name: 'confidentialInputsHash', type: 'bytes32' }, ], }, domain: { name: 'ConfidentialRecord', verifyingContract: eip712Tx.kettleAddress, }, }) return hexToSignature(rawSig) },
```

In addition to the improved UX, this feature also gives front-ends the unprecedented power to control where orderflow is directed. No matter which wallet or front-end package is used, the user is able to sign without the infamous issue of being forced to broadcast. Using the same language your dapp developers love, programmatically control your dapp's orderflow in Solidity and use existing smart contract tooling to monitor!

TEE Kettles

[

toliman_kettles

1920×1005 120 KB

](https://collective.flashbots.net/uploads/default/original/2X/2/26bddd063b6c7aa3493caea12981d63872254344.jpeg)

SUAVE Kettles are at the heart of the SUAVE Network, providing fast, cheap, and private computing capabilities to your apps. Typically developing with privacy enhancing technologies has come at the cost of added complexity and poor UX, which is why our last Rigil devnet was focused on making Kettle primitives as easy as adding a few lines of solidity. Now with this release we're leveling up the privacy guarantees by running Kettles on Intel TDX, the latest generation of Trusted Execution Environments (TEEs) with blazing fast performance.

This new feature takes one step further towards removing the need to trust Flashbots when using SUAVE, making it much harder for the Kettle operator to access or alter your app's private data and computations. While there is a potential risk of collusion between the hardware manufacturer and cloud provider to breach TEE integrity, compromising a TEE is far more complex than tampering with existing plaintext MEV supply chain components. This is only one step in our privacy journey and our next testnet, Proxima, will focus on further enhancing privacy guarantees by more securely using the TDX Attestation Protocol, creating onchain Kettle certificate records, and more!

[

testnet_tables_2

1920×638 74.2 KB

](https://collective.flashbots.net/uploads/default/original/2X/c/c2eb767222659fe5a665056fcd6d8a2292bea7e7.jpeg)

Adopting TEEs is crucial for our vision of enabling anyone worldwide to permissionlessly participate as a SUAVE Kettle operator while still ensuring strong privacy. Additionally, TEE integrity means that the computations performed within the TEE are reliable and can be trusted by other offchain apps, enabling composability between TEE-based offchain apps. When combined with cryptographic proofs of data integrity and authenticity for HTTPS sessions, such as those provided by TLSNotary, entirely new app designs spaces are opened including securely interacting with web2 data from onchain. If you're interested in exploring TEEs further, check out our post Speedrunnig a TEE Coprocessor and our first Flashwares session where we cover What Are TEEs.

Demos

To showcase the power of the two new features released in Toliman, EIP-712 Messages and TEE Kettles, Flashbots, in conjunction with the SUAVE community, have designed and developed a few SUAVE apps to showcase their power! Try any out below and note that these apps are only proof-of-concepts. We encourage you to fork, improve, and make them your own!

- Extra Data Auction

(demo | code) - Have you ever wanted to put your twitter handle in the extra data of an Ethereum Execution block? Well for the right price now you can! You might even help develop an inscription standard for this under utilized Ethereum resource. This SUAVE app utilizes Kettle privacy to ensure that bids are sealed and bid contents aren't observable until after the auction! Developed by Miha and Caleb at Eden Network.

- Suciphus

(demo | code) - Think you're smarter than AI? If so, you could win a jackpot in this PvE LLM game! This SUAVE app utilizes the ability to make network calls, as well as SUAVE's confidential data store to keep prompts private so you don't leak your strategy! Developed by Taylor and Brock.

- ChatNFT

(demo | code) - Mint an AI generated NFT, the better the prompt, the rarer the NFT! This SUAVE app utilizes the unique ability to make network calls to an LLM from Solidity! Developed by Brock.

Toliman for Developers

Toliman introduces a suite of unique features to super power your offchain application:

- MEV Coprocessing:

Develop your app as a solidity Coprocessor during block production.

- Public and Private State:

Take advantage of both public and private states in your app. Public state is accessible on the SUAVE Chain, and private state through the solidity accessible Confidential Data Store each kettle maintains. Note: Private state currently has a 14 day expiry window, and can be refreshed indefinitely.

- Multichain

: SUAVE Kettles are equipped with RPCs to simulate and build blocks for both the Holesky testnet and Ethereum mainnet, and you can add a new network with 2 lines of solidity! Note: Using Ethereum Mainnet assets on SUAVE is currently not recommended.

- Build Secure Applications:

Leverage TEE for enhanced security, data privacy, and integrity.

To start interacting with the testnet, check out the documentation. We also provide multiple tools to get started, including, but not limited to: Kettle RPCs, SDKs (Typescript, Golang, and Solidity), Forge Support, Local Dev Net, Starter Code and Examples, and a list of SUAVE app Ideas! If you have technical or non-technical questions, feel free to post an issue on github, a post on our forum, or find our SUAVE.dev telegram channel in our documentation.

Toliman for Orderflow Originators

Toliman empowers orderflow originators with greater control and flexibility over transaction routing and execution, enhancing profitability and user experience:

- Direct Orderflow Routing Control:

Gain precise control over transaction routing directly from your front-end, optimizing execution quality.

- Customizable User Experience:

Tailor the transaction process to fit the needs of your users.

- Monetization Opportunities:

Explore new business models by leveraging controlled orderflow.

Community Engagement

Engage with the Toliman testnet today to explore these features and start developing or optimizing your applications. Join our vibrant community for support and collaboration:

- Community Forum and Discussions:

Post questions or share insights on our collective forum.

- Live Support:

Connect with other developers and our core dev team in real-time through the SUAVE Dev Telegram channel, linked in our documentation.

- SUAPP Office Hours:

Don't miss our upcoming SUAPP Office Hours on August 28th. We will discuss the latest developments and how you can help contribute to the future of MEV!

Looking Ahead: The Proxima Testnet

The next phase in our roadmap is the Proxima testnet, which will focus on improving security guarantees with the work from SUAVE Sirrah, as well as enabling support for various rollups to enable new cross-chain capabilities. We are gathering developer feedback to prioritize features that meet your needs. If you're working on rollups or SUAVE applications, please reach out to help shape our future roadmap!

Disclaimer

: Toliman ("Toliman") is NOT the official launch of SUAVE. While certain persons may access SUAVE on the mainnet and use non-testnet cryptocurrency, the purpose of Toliman is strictly to test the capabilities of SUAVE. By accessing or utilizing any services provided by Flashbots Ltd., ("Flashbots") including but not limited to the Toliman: SUAVE Testnet and any other versions of SUAVE, you agree to be bound by Flashbots' Terms of Service.