We're thrilled to unveil the latest milestone in our journey towards building an encrypted, Shutterized mempool for the OP Stack, marking a significant leap towards a more secure, front-running, and censorship-resistant Optimism ecosystem. This announcement not only encapsulates the completion of pivotal phases in our project but also outlines the future trajectory we're set to embark on.

More specifically, we're working towards a release of a testnet of a Shutterized OP Stack L2 in February

, which opens up any OP Stack chain or L2 to easily add a shutterized, encrypted mempool to their L2. We also have an awesome OP Stack L2 who wants to launch their OP Stack variant as a separate testnet (and eventually mainnet) with us!

More specifically, we're working towards a release of a testnet of a Shutterized OP Stack L2 in February

If you want to find out more about the background, architecture, and goals for having an encrypted mempool, this roadmap extends on our previous work to define the architecture and requirements and research the viability of an encrypted mempool for the OP Stack as well as our more recent demo (running against a mock sequencer).

define the architecture and requirements and research the viability of an encrypted mempool for the OP Stackdemo (running against a mock sequencer).## Why an encrypted mempool for OP Stack?

Why an encrypted mempool for OP Stack?

The integration of an encrypted mempool for OP Stack rollups aims to enhance the security and fairness of DeFi trading by mitigating front-running and malicious MEV (Maximal Extractable Value) practices. These are some of the expected benefits of using an encrypted mempool:

- Safer, more profitable trading for DEFI users (Front-Running Mitigation)
- Added (real-time) censorship resistance (even for centralized sequencers)
- Reducing sequencer trust assumptions: The encryption "blinds" the sequencer to a certain degree, disarming them and thus reducing the degree of trust required in the sequencer
- Sequencers can plausibly argue that they no longer have the ability to front-run transactions nor censor transactions based on their content by design (potential compliance, image, and regulatory benefits for the sequencer operator)
- Sequencer still retains the ability to collect or distribute back-running related MEV (arbitrage and liquidations)

Safer, more profitable trading for DEFI users (Front-Running Mitigation)

Added (real-time) censorship resistance (even for centralized sequencers)

Reducing sequencer trust assumptions: The encryption "blinds" the sequencer to a certain degree, disarming them and thus reducing the degree of trust required in the sequencer

Sequencers can plausibly argue that they no longer have the ability to front-run transactions nor censor transactions based on their content by design (potential compliance, image, and regulatory benefits for the sequencer operator)

Sequencer still retains the ability to collect or distribute back-running related MEV (arbitrage and liquidations)

Roadmap Overview

Roadmap Overview

Milestone

Description

(Projected) Completion Date

Mock Rollup Demo

Demonstrated the feasibility and effectiveness of Shutter in a controlled environment.

Done (Nov 2023)

Milestone 1: Dev-Internal Milestone

Achieved initial development milestone with successful encrypted transaction processing.

Done (Dec 2023)

Milestone 2: OP Integration

Integration of Shutter technology with OP-node and OP-geth.

Early Feb 2024

Milestone 3: Sepolia Release

Launch of a Shutterized OP Stack L2 on the Sepolia test network.

Feb 2024

Joint Testnet Release

Public release of Shutterized L2 testnet in collaboration with an OP Stack L2.

March 2024

Milestone

Description

(Projected) Completion Date

Mock Rollup Demo

Demonstrated the feasibility and effectiveness of Shutter in a controlled environment.

Done (Nov 2023)

Milestone 1: Dev-Internal Milestone

Achieved initial development milestone with successful encrypted transaction processing.

Done (Dec 2023)

Milestone 2: OP Integration

Integration of Shutter technology with OP-node and OP-geth.

Early Feb 2024

Milestone 3: Sepolia Release

Launch of a Shutterized OP Stack L2 on the Sepolia test network.

Feb 2024

Joint Testnet Release

Public release of Shutterized L2 testnet in collaboration with an OP Stack L2.

March 2024

Milestone

Description

(Projected) Completion Date

Milestone

Milestone

Milestone

Description

Description

Description

(Projected) Completion Date

(Projected) Completion Date

(Projected) Completion Date

Mock Rollup Demo

Demonstrated the feasibility and effectiveness of Shutter in a controlled environment.

Done (Nov 2023)

Mock Rollup Demo

Mock Rollup Demo

Mock Rollup Demo

Demonstrated the feasibility and effectiveness of Shutter in a controlled environment.

Demonstrated the feasibility and effectiveness of Shutter in a controlled environment.

Demonstrated the feasibility and effectiveness of Shutter in a controlled environment.

Done (Nov 2023)

Done (Nov 2023)

Done (Nov 2023)

Milestone 1: Dev-Internal Milestone

Achieved initial development milestone with successful encrypted transaction processing.

Done (Dec 2023)

Milestone 1: Dev-Internal Milestone

Milestone 1: Dev-Internal Milestone

Milestone 1: Dev-Internal Milestone

Achieved initial development milestone with successful encrypted transaction processing.

Achieved initial development milestone with successful encrypted transaction processing.

Achieved initial development milestone with successful encrypted transaction processing.

Done (Dec 2023)

Done (Dec 2023)

Done (Dec 2023)

Milestone 2: OP Integration

Integration of Shutter technology with OP-node and OP-geth.

Early Feb 2024

Milestone 2: OP Integration

Milestone 2: OP Integration

Milestone 2: OP Integration

Integration of Shutter technology with OP-node and OP-geth.

Integration of Shutter technology with OP-node and OP-geth.

Integration of Shutter technology with OP-node and OP-geth.

Early Feb 2024

Early Feb 2024

Early Feb 2024

Milestone 3: Sepolia Release

Launch of a Shutterized OP Stack L2 on the Sepolia test network.

Feb 2024

Milestone 3: Sepolia Release

Milestone 3: Sepolia Release

Milestone 3: Sepolia Release

Launch of a Shutterized OP Stack L2 on the Sepolia test network.

Launch of a Shutterized OP Stack L2 on the Sepolia test network.

Launch of a Shutterized OP Stack L2 on the Sepolia test network.

Feb 2024

Feb 2024

Feb 2024

Joint Testnet Release

Public release of Shutterized L2 testnet in collaboration with an OP Stack L2.

March 2024

Joint Testnet Release

Joint Testnet Release

Joint Testnet Release

Public release of Shutterized L2 testnet in collaboration with an OP Stack L2.

Public release of Shutterized L2 testnet in collaboration with an OP Stack L2.

Public release of Shutterized L2 testnet in collaboration with an OP Stack L2.

March 2024

March 2024

March 2024

Detailed Roadmap

Detailed Roadmap

Nov 2023: Mock Rollup Demo

Nov 2023: Mock Rollup Demo

Completed a mock demonstration showcasing Shutter's potential to secure transactions against front-running, laying the groundwork for further development.

This facilitated an end-to-end encryption/decryption cycle but was based on an older design for Shutter / Rollup integration and mocked the Layer 2 execution.

Dec 2023: Dev-Internal Milestone

Dec 2023: Dev-Internal Milestone

Named "Shutter Node Activation," this milestone marked the first successful test of Shutter contracts and keyper (the Shutter DKG key committee) integration within our local docker devnet setup, showcasing a big part of the operational capabilities of Shutter within the OP Stack. The transaction decryption in the EVM / execution client has independently been finalized for this Milestone as well.

[wip: dev-milestone working state · shutter-network/optimism@dfdd99c

The Optimism monorepo. Contribute to shutter-network/optimism development by creating an account on GitHub.

GitHub

shutter-network

](https://github.com/shutter-network/optimism/commit/dfdd99c94477e5991ac99acc14dada9365230d28?ref=blog.shutter.network)

[wip: dev-milestone working state · shutter-network/optimism@dfdd99c

The Optimism monorepo. Contribute to shutter-network/optimism development by creating an account on GitHub.

GitHub

shutter-network

](https://github.com/shutter-network/optimism/commit/dfdd99c94477e5991ac99acc14dada9365230d28?ref=blog.shutter.network)wip: dev-milestone working state · shutter-network/optimism@dfdd99c

The Optimism monorepo. Contribute to shutter-network/optimism development by creating an account on GitHub.

GitHub

shutter-network

wip: dev-milestone working state · shutter-network/optimism@dfdd99c

The Optimism monorepo. Contribute to shutter-network/optimism development by creating an account on GitHub.

GitHub

shutter-network

GitHub

shutter-network

[GitHub - shutter-network/shop-contracts at 5af044fb2122e1f0796566b83ef627fd86b7f9b0

The system contracts of Shutterized Optimism. Contribute to shutter-network/shop-contracts development by creating an account on GitHub.

GitHub

shutter-network

](https://github.com/shutter-network/shop-contracts/tree/5af044fb2122e1f0796566b83ef627fd86b7f9b0?ref=blog.shutter.network)

[GitHub - shutter-network/shop-contracts at 5af044fb2122e1f0796566b83ef627fd86b7f9b0

The system contracts of Shutterized Optimism. Contribute to shutter-network/shop-contracts development by creating an account on GitHub.

GitHub

shutter-network

](https://github.com/shutter-network/shop-contracts/tree/5af044fb2122e1f0796566b83ef627fd86b7f9b0?ref=blog.shutter.network)GitHub - shutter-network/shop-contracts at 5af044fb2122e1f0796566b83ef627fd86b7f9b0

The system contracts of Shutterized Optimism. Contribute to shutter-network/shop-contracts development by creating an account on GitHub.

GitHub

shutter-network

GitHub - shutter-network/shop-contracts at 5af044fb2122e1f0796566b83ef627fd86b7f9b0

The system contracts of Shutterized Optimism. Contribute to shutter-network/shop-contracts development by creating an account on GitHub.

GitHub

shutter-network

GitHub

shutter-network

Early Feb 2024: OP Integration

Early Feb 2024: OP Integration

In this milestone, we will fully integrate the Shutter services with the OP Stack consensus client (op-node) and execution client (op-geth). This will allow for end-to-end encrypted transaction handling from the user up to the rollup's EVM.

Feb 2024: Sepolia Release

Feb 2024: Sepolia Release

Launching Shutterized Optimism on the Sepolia testnet, providing a real-world environment for testing and feedback, marking a critical step towards full deployment. This phase aims to establish a comprehensive and robust deployment framework for Shutterized Optimism, ensuring scalability and reliability across the network. In this first iteration, we will still focus on an openly accessible but encapsulated hosted setup for every service except the Layer 1 backend.

March 2024: Joint Testnet Release

March 2024: Joint Testnet Release

In collaboration with an awesome rollup that utilizes the OP Stack (stay tuned), we will publicly release a Shutterized OP Stack L2 testnet, showcasing a live demonstration of its capabilities to secure and decentralize transaction processing.

Throughout the roadmap and beyond, we and others will deploy demo applications to illustrate Shutter's utility and supporting tooling like faucets. We have some cool ideas for this. Stay tuned!

We'll also continuously be working to fully decentralize the infrastructure, starting with practicality, a shipping-first approach, and then taking off training wheels as we go.

In addition to this, the shutterized, encrypted mempool will also be available soon as a testnet to deploy via roll-op by Norswap.

roll-opBecause of all the prior work done, once we have the testnets up and running for a couple of weeks and have taken additional steps to decentralize all the infrastructure, we're optimistic that any mainnet releases can follow up shortly after.

Conclusion and next steps

We think this roadmap, culminating in the launch of a testnet in February, marks a pivotal step towards achieving our goals for more base layer neutrality and mempool accessibility.

On a related note, we've also submitted amission request to OP DAO to build a generalized encryption interface for the OP-Stack, focusing on a shutterized/threshold encrypted variant as a prototype. This mission, aiming to offer a flexible, secure transaction environment, is crucial for us and the broader ecosystem. We'd appreciate the community's feedback and support on this mission request to ensure it meets the ecosystem's needs and expectations!

mission request to OP DAO to build a generalized encryption interface for the OP-StackWe'd appreciate the community's feedback and support on this mission request to ensure it meets the ecosystem's needs and expectations!

Follow along with development progress

Follow along with development progress

[Shutter Network

Shutter Network has 25 repositories available. Follow their code on GitHub.

GitHub

](https://github.com/shutter-network?ref=blog.shutter.network)

[Shutter Network

Shutter Network has 25 repositories available. Follow their code on GitHub.

GitHub

](https://github.com/shutter-network?ref=blog.shutter.network)Shutter Network

Shutter Network has 25 repositories available. Follow their code on GitHub.

GitHub

Shutter Network

Shutter Network has 25 repositories available. Follow their code on GitHub.

GitHub

GitHub

Our journey is ambitious, and community involvement is vital to our success. We look forward to your insights and contributions as we work towards a more private, secure, and base layer neutral OP Stack ecosystem.

Links/resources

- Definition, architecture, and research into the viability of an encrypted mempool for the OP Stack
- Demo and completion of our builders grant
- Mission request to OP DAO to build a generalized encryption interface for the OP-Stack
- Github

Definition, architecture, and research into the viability of an encrypted mempool for the OP Stack

Definition, architecture, and research into the viability of an encrypted mempool for the OP StackDemo and completion of our builders grant

Demo and completion of our builders grantMission request to OP DAO to build a generalized encryption interface for the OP-Stack

Mission request to OP DAO to build a generalized encryption interface for the OP-StackGithub

Github