slug: introducing-rollup-boost title: Introducing Rollup-Boost - Launching on Unichain authors: [flashbots] tags: [rollup, decentralization, platform, l2, optimism, unichain] hide_table_of_contents: false image: /img/rollupboost/header.png forum_link: https://collective.flashbots.net/t/introducing-rollup-boost-launching-on-unichain/3959

import Figure from "@site/src/components/Figure/Figure";

We've developed a platform for performance, programmability, and decentralization extensions for Rollups. It is powering the upcoming Unichain.

Today, we are announcing Rollup-Boost, a verifiable block building platform for rollups, enabled by Trusted Execution Environments (TEE) technology. Rollup-Boost was co-designed with Uniswap Labs and OP Labs, and its first deployment powers the upcoming Unichain, enabling fast confirmation times, strong user guarantees, and MEV internalization for the next generation of Defi apps.

Rollup-Boost introduces the idea of Rollup Extensions, which are modular components for upgrading rollups across performance, programmability, and decentralization. We are launching Rollup-Boost with two initial extensions:

- **250ms "Flashblocks**" that provide fast confirmation times, native revert protection for users, and increased gas throughput.
- **Verifiable priority ordering** within each Flashblock, giving greater guarantees to users and allowing applications to internalize their MEV.

In its final form, this extension model combined with the unique properties of TEEs will allow rollups to harmonize two previously opposing forces: user experience and geographic decentralization. TEEs are a novel form of technology that allows for horizontal scaling of distributed applications across the trust boundaries of their operators, and introduces new trade-off points on what is sometimes referred to as the "MEV trilemma".

In its first release, Rollup-Boost is a lightweight sidecar designed to upgrade existing sequencers. We believe this is the first step to enabling TEE-centric programmable privacy solutions that will be critical for rollup decentralization in the presence of MEV. We plan to iterate Rollup-Boost to support this decentralized endgame.

We welcome the open source community to join us, to achieve these goals together.

The problem

In achieving Ethereum's ambitious rollup-centric roadmap, projects are often forced to balance the features their users demand with the decentralization targets of their ecosystem.

One example is **fast confirmation times**, which matters for user experience. By making different tradeoffs, alternative L1 blockchains such as Solana have been able to innovate here, reducing block time to up to 400ms compared to Ethereum's 12 seconds. But with this approach, building rollup infrastructure in a decentralized way that can support a wide range of node participants or geographies efficiently remains difficult.

Further, the MEV trilemma posits that MEV will be extracted one way or another – chain designers can only choose between an explicit auction, a spam auction, or a latency auction. Naive approaches to fast blocks often default to latency auction, which is additionally geographically centralizing, while spam auctions cause negative externalities in the form of frequent reverts and excessive gas congestion.

The opportunity

Using TEEs and future technologies, we have an opportunity to escape the dilemma set up by UX and decentralization, introducing a new tradeoff point that didn't exist before.

TEEs allow us to create infrastructure that is scalable across trust boundaries, by delegating computation with the full integrity guarantees provided by remote attestation. This horizontal and global scaling can escape these negative and self-defeating externalities, and outsource key components of what is now centralized infrastructure.

We believe that the novel scaling properties combine with the information security guarantees TEEs provide to users, allowing users to leverage their information and the MEV they create to achieve the best possible outcomes. These improved outcomes through decentralization can then furnish the economic fuel that accelerates decentralization of global finance through better execution, achieving the ultimate goals of crypto as a whole.

We further believe TEEs accelerate the next phase in rollup evolution, unlocking new dimensions in confirmation times, user guarantees, and developer innovation. Initially, TEEs upgrade existing sequencers, while also providing the platform from

which future decentralization can be developed.

We will now describe the two extensions that we are releasing, as the first step on this journey.

Flashblocks

Flashblocks is a streaming layer that gives users near-instant UX while still running an explicit auction every 250ms. We achieve this in a few ways:

1. Creating and streaming partial blocks every 250ms to other nodes.
2. Providing users with early execution confirmations.
3. Allowing nodes to incrementally download and continuously execute transactions rather than wait for new blocks.
4. Calculating the state root and consensus once for multiple partial blocks, amortizing costly parts of block production.
5. Serving early execution state over the existing, unmodified Ethereum JSON-RPC standard, enabling easy wallet and front end integration.

Flashblocks draw inspiration from innovations in block propagation and execution, such as Solana's shreds and Celestia's data squares. The "flashblock" specification for the OP Stack enables the streaming of partial blocks between clients. This approach dovetails seamlessly with execution innovations from reth and our modular rust block builder. The result is a potential multiple-fold increase in gas per second, pushing the boundaries of what's possible in rollup performance.

Unichain uses Flashblocks to:

- Provide a great UX with 250ms confirmation times and native revert protection.
- Reduce adverse selection costs for liquidity providers, resulting in lower spreads and a more competitive trading environment than centralized exchanges (CEXs).

Verifiable priority ordering

Rollup-Boost's verifiable ordering allows users to verify how their transactions are executed by leveraging the information security properties of TEEs. The ability to credibly commit to any ordering rule also opens a new design space for ordering algorithms unavailable on Ethereum L1.

One such ordering rule recently advocated by Robinson and White is priority ordering, a proposed rule to allow applications to capture and redistribute some of their MEV. Should the TEE degrade, the system simply defaults back to normal case best-effort priority fee guaranteed ordering with no verifiability.

We plan to support a range of MEV-aware sequencing extensions on the platform, and call on the community and on rollup developers to discover more decentralized and robust solutions to achieve the full potential of the rollup-centric roadmap.

Unichain uses verifiable ordering to:

- Remove trust in block ordering, guaranteeing to users how their transactions are ordered.
- Internalize MEV for LPs, reducing liquidity costs and lowering spreads for users.
- Attract and retain third-party applications previously unable to internalize MEV., preventing them from fragmenting the L2 ecosystem by moving to their own appchains.

Future roadmap

Rollup-Boost will launch with **Flashblocks** and **Credible Priority Ordering**, but our roadmap is ambitious, and we want to highlight three key extensions we're currently working on.

Encrypted Mempool

At launch, transactions are streamed to the TEE block builder from a centralized RPC, and from the TEE block builder to a centralized sequencer. By moving the RPC and sequencer into TEEs as well, we ensure transactions are never visible to any third party outside the secure hardware, during their entire lifecycle from intent to execution.

TEE Validity Proofs

Rollups need permissionless proving to qualify as Stage 2. However, the current immaturity of proving mechanisms makes it risky to implement a fully permissionless system. To address this challenge, rollups can use a multi-prover approach, essentially creating a "2 of 2" multi-signature scheme.

In this setup, two separate proving systems must agree for the system to proceed. If there's a discrepancy, the bridge is automatically paused as a safety measure. By introducing a TEE prover as a cheap and fast option to serve as this "second prover," we can accelerate the transition to stage 2 while maintaining robust security measures.

This approach offers several advantages:

- It provides an additional layer of verification, enhancing the overall security of the rollup.
- The use of TEE technology ensures that the proving process remains tamper-resistant and private.
- The speed and cost-effectiveness of TEE provers allow for quicker iterations and improvements in the proving mechanism.

TEE coprocessing

Finally, we are very excited about the potential unlock for rollups and developers from TEE coprocessing.

In short, TEE coprocessors give developers superpowers through cheap, private, and decentralized compute alongside the EVM. The two use cases we are the most excited about are to scale existing applications and to create net new apps.

TEE coprocessing helps to scale existing applications by replacing on-chain logic with provable, ultra-cheap off-chain execution (similar to rollups). More importantly, it enables new applications that trustlessly interact with web2, store private data, and execute private programs. As an example, we recently released Teleport - an app that uses TEE coprocessing to have smart contracts control Twitter accounts.

We've developed prototypes of Solidity based Coprocessors, Private searcher code Coprocessors, Web3 to Web2 Coprocessors, and even WASM Coprocessors. All of these will become available with rollup extensions, including FHE and MPC coprocessors. If you'd like to help develop this technology with us, get in touch!

Conclusion

We believe this is the first of many steps to achieving the rollup future that Ethereum deserves. We believe new cryptographic technologies, especially today in the form of TEEs, enable a new wave of advancements that have the potential to harmonize efficiency and decentralization.

By upgrading rollups with these technologies, we can achieve features their users demand, without sacrificing a roadmap that viably decentralizes their underlying infrastructure. We are seeking contributions across the Ethereum community, including from:

- **Rollup Operators**: Are you interested in adopting Rollup-Boost or any of the Rollup Extensions discussed? Fill out this form to get in touch..
- **App Developers**: Build on the Toliman testnet to familiarize yourself with developing on a TEE co-processor and leveraging its capabilities.
- **Chain Developers**: Contribute to our open source rollup-boost and rust block builder.
- **Researchers:** Many of these new technologies, concepts, and systems require principled, deep work. Submit an FRP or get in touch with us if that excites you.
- **Community Members:** Explore our TEE resources and join the conversation (Youtube, Forum)

As a community, it has finally come time to escape the MEV trilemma. As MEV matures, we are continually discovering new ways to harness the power of this financial energy to build more, rather than less, decentralization. Will you join us on this journey?