Unichain

October 2024

Hayden Adams
hayden@uniswap.org

Mark Toda
mark@uniswap.org

Alex Karys
alex.karys@uniswap.org

Xin Wan
xin@uniswap.org

Daniel Gretzke
daniel.gretzke@uniswap.org

Eric Zhong
eric.zhong@uniswap.org

Zach Wong
zach.wong@uniswap.org

Daniel Marzec
dan@flashbots.net

Robert Miller
robert@flashbots.net

Hasu
hasu@flashbots.net

Karl Floersch
karl@oplabs.co

Dan Robinson
dan@paradigm.xyz

ABSTRACT

Unichain is an optimistic rollup optimized for efficient markets by delivering fast state updates, offering a framework for applications to internalize MEV, and providing an economic finality system for quick settlement across blockchains.

1 INTRODUCTION

Ethereum's rollup-centric roadmap has successfully scaled onchain activity through the proliferation of rollups over the last few years. However, this approach has introduced new challenges for the DeFi ecosystem, including suboptimal execution quality, degraded user experience, and fragmented liquidity.

This paper introduces Unichain, an optimistic rollup built on the OP Stack [16], designed to address these core challenges through two key innovations:

- **Verifiable Block Building**: A block building mechanism built in collaboration with Flashbots, initially designed to deliver:
  - 200-250ms effective block times by splitting each block into four "Flashblocks."
  - Transparent enforcement of priority ordering within each Flashblock, allowing applications to allocate some of their maximal extractable value (MEV) for the benefit of their users.
  - Trustless revert protection for transactions.
- **Unichain Validation Network**: A decentralized network of Unichain node operators designed to reduce certain key risks of the block sequencing process, enabling faster economic finality for quicker settlement of cross-chain transactions and supporting potential future extensions.

Unichain is built on the Superchain, a scalable and interconnected network of rollups on the OP Stack, as a foundational environment to promote the seamless movement of liquidity. Alongside an intents-based, cross-chain bridge [21] and fast finality from the Unichain Validation Network, connectivity with the Superchain is intended to enable quick, inexpensive and broad access to liquidity for rollup users. Unichain is being developed through an iterative, open source process, making its codebase available to other OP Stack rollups. The features described in this document will be thoroughly tested on a publicly accessible testnet called *Unichain Experimental* before being deployed to Unichain mainnet.

2 PRIOR WORK AND CURRENT CHALLENGES

Ethereum has made great progress towards a robust, permissionless, and credibly neutral network. However, various issues have emerged as adoption of blockchain technology has increased. One of the most pressing issues is the unpredictability and high cost of gas fees during periods of network congestion [1, 2], which is caused by limitations in throughput. Rollups have been proposed as a strategy to scale the overall processing capacity of the underlying network, and have been suggested as the main strategy by the community [6]. Currently, the technology underlying the most popular rollups are developed by OP Labs [16, 17] and Offchain Labs [12], among others. Most of these rollups require trust that the sequencer will comply with their stated block building protocols.

In addition, a block production environment that enables users to extract maximal extractable value ("MEV" [8]) from other users limits the efficiency of markets and applications that can be built. Solutions such as private mempools were introduced as a mitigation to MEV extraction risk, but they introduce single points of failure [2, 9, 15, 18], to which trusted execution environments (TEEs) have been proposed as a solution [10].

Automated market makers (AMMs) [3–5], pioneered by Uniswap Labs, have also seen significant growth on blockchains like Ethereum [22]. While they have revolutionized digital asset trading by making liquidity provision permissionless, other challenges have emerged. Specifically, constraints of existing blockchains such as long block times increase adverse selection risks for onchain liquidity providers [13, 14], while public mempool and unconstrained transaction ordering could lead to sandwich attacks [19].

To address the current set of challenges, Unichain introduces two main features, *Verifiable Block Building* and *Unichain Validation Network*. These features draw inspiration from the aforementioned research and innovations.

3 VERIFIABLE BLOCK BUILDING

Block building plays a crucial role in determining MEV leakage and latency characteristics. Unichain adopts a novel block building protocol optimized for user experience and value preservation, while maintaining neutrality. This is enabled by *Rollup-Boost* [11], developed in collaboration with Flashbots.

3.1 Sequencer Builder Separation

Unichain separates the role of block building from the sequencer with the Verifiable Block Builder, built in collaboration with Flashbots. Block building operations are executed inside a trusted execution environment (TEE), allowing external users to verify compliance with stated ordering rules. TEEs offer enhanced trust and security guarantees relative to the servers they replace.

The initial TEE builder will run an open source builder codebase [1] on Intel's TDX hardware, which offers both private data access and verifiable execution through its computational integrity property [7]. Execution attestations will be posted publicly, allowing users to verify that blocks were built inside the TEE according to stated policies.

TEE block building is a powerful primitive for rollups, not only mitigating the risk of discretionary block ordering, but also providing a framework for making transparent incremental improvements.

3.2 Flashblocks

Flashblocks are block pre-confirmations issued by the TEE block builder. Shorter block times lower adverse selection costs for liquidity providers [13, 14], reduce latency for users, and foster a more efficient onchain market. As transactions are streamed to the TEE builder, it incrementally commits to Flashblocks, which are ordered sets of transactions that will be included in the eventual proposed block. The sequencer then broadcasts these Flashblocks as pending blocks, providing users, applications, and integrators with the experience of block times multiple times faster than the default. In most current rollup architectures, block proposals face high fixed latency due to serialization and state root generation, making sub-second block times infeasible. Flashblocks bypass this overhead over short timescales, enabling low latency blockchain interaction.

The TEE enforces priority ordering for each Flashblock and supports a Flashblock bundle type that enables users to target specific Flashblocks for inclusion. The combination of these two features facilitates allocation of MEV for the benefit of users by applications, such as through MEV tax [20].

3.3 Trustless Revert Protection

The verifiable builder enables trustless revert protection, reducing the risk that a user pays for a failed transaction. The TEE simulates transactions while building blocks, and is programmed to detect and remove any reverting transactions.

Revert protection reduces friction for users and improves the efficiency of AMMs and intents-based systems, as participants can have greater confidence in their transactions.

3.4 Future Work

The verifiable block builder is a primitive on which many future improvements to Unichain can be built, such as:

- **Encrypted Mempool**: Users could encrypt transactions, enhancing their pre-transaction privacy.
- **Scheduled Transactions**: The TEE could be programmed to allow users or smart contracts to submit automatic transactions to execute scheduled or recurring actions.
- **TEE Coprocessor**: The TEE could allow smart contracts to request private, verifiable computation.

4 UNICHAIN VALIDATION NETWORK

Unichain addresses the risks associated with single-sequencer architectures by introducing the Unichain Validation Network (UVN), a decentralized network of node operators that independently validate the latest blockchain state. While rollups benefit from the strong security of the base blockchain, the sequencer's behavior can affect the blockchain's liveness, MEV dynamics, and finality. The UVN is an extensible platform, with an initial focus on verifying blocks for faster finality.

Two major risks in particular emerge in single sequencer rollups that affect the speed of cross-chain settlement:

- **Block Equivocation Risk**: The possibility that the sequencer proposes multiple conflicting blocks at the same height, creating uncertainty around which block will ultimately be finalized.
- **Invalid Block Risk**: The risk that a sequencer posts an invalid block, leading to a chain reversion when fault proofs are submitted, further delaying settlement.

These risks cause longer wait times for finality of the blockchain, hindering the seamless flow of liquidity across networks. The UVN addresses these challenges by having verifiers attest to the canonical chain as blocks are proposed, providing faster economic finality.

4.1 Staked Validators

In order to become eligible as a validator in the UVN, node operators must stake UNI on Ethereum mainnet. Stakes are tracked on Unichain in a smart contract, which receives notifications over the native bridge of stake and unstake operations. Unichain blocks are segmented into epochs of a set length. At the start of each epoch, the currently staked balances are snapshotted, blockchain fees are collected, and a reward per staked token value is calculated. Participants can also stake and vote for a validator, increasing the validator's stake-weight. A limited number of validators with the highest UNI stake-weight will be considered the active set, and are eligible to post attestations and earn the earmarked compensation for the epoch.

Active validators are expected to be online, running an instrumented Reth Unichain node that performs validation of proposed

[1] https://github.com/flashbots/rbuilder

blocks. Validators sign block hashes and publish them to the UVN Service smart contract on Unichain once per epoch as a public attestation of their validity to the network. The Service smart contract validates these attestations as they are posted, and compensates the validator immediately based on the validator's stake-weight. Validators who fail to post a valid attestation for the epoch will not receive their allocation, and this compensation will roll over into the next epoch.

The specific checks performed in each attestation are extensible. To start, UVN validators will perform simple block attestations to increase confidence in the state of the canonical chain.

5 POTENTIAL FUTURE WORK

The Unichain Validators Network is intended to be a platform on which various checks can be performed with respect to the sequencing process . Some future extensions to the system could include:

- **Credible Neutrality**: Validators can monitor the rollup's mempool, ensuring that transactions are being included in a timely manner.
- **Limiting Posting**: The BatchPoster contract can require a certain attestation weight before including blocks, effectively limiting the sequencer's ability to post blocks that don't follow specific rules.

6 CONCLUSION

Unichain addresses some of the most pressing challenges for trading in Ethereum's rollup-centric scaling strategy, notably liquidity fragmentation and inefficient cross-chain interactions. By introducing innovative technologies like Flashblocks, Unichain Validation Network and integrating with the Superchain, Unichain aims to become the home for DeFi liquidity and best place to access DeFi across rollups.

REFERENCES

[1] Austin Adams. 2024. Layer 2 be or Layer not 2 be: Scaling on Uniswap v3. *arXiv preprint arXiv:2403.09494* (2024).

[2] Austin Adams, Benjamin Y Chan, Sarit Markovich, and Xin Wan. 2023. Don't Let MEV Slip: The Costs of Swapping on the Uniswap Protocol. *arXiv preprint arXiv:2309.13648* (2023).

[3] Hayden Adams. 2018. *Uniswap v1 Core.* Retrieved Jun 12, 2023 from https://hackmd.io/@HaydenAdams/HJ9jLsfTz

[4] Hayden Adams, Noah Zinsmeister, and Dan Robinson. 2020. *Uniswap v2 Core.* Retrieved Jun 12, 2023 from https://uniswap.org/whitepaper.pdf

[5] Hayden Adams, Noah Zinsmeister, Moody Salem, River Keefer, and Dan Robinson. 2021. *Uniswap v3 Core.* Retrieved Jun 12, 2023 from https://uniswap.org/whitepaper-v3.pdf

[6] Vitalik Buterin. 2020. *A rollup-centric ethereum roadmap.* https://ethereum-magicians.org/t/a-rollup-centric-ethereum-roadmap/4698

[7] Victor Costan and Srinivas Devadas. 2016. Intel SGX Explained. Cryptology ePrint Archive, Paper 2016/086. https://eprint.iacr.org/2016/086

[8] Philip Daian, Steven Goldfeder, Tyler Kell, Yunqi Li, Xueyuan Zhao, Iddo Bentov, Lorenz Breidenbach, and Ari Juels. 2020. Flash boys 2.0: Frontrunning in decentralized exchanges, miner extractable value, and consensus instability. In *2020 IEEE Symposium on Security and Privacy (SP)*. IEEE, 910–927.

[9] Flashbots. [n. d.]. *MEV Protection Overview.* https://docs.flashbots.net/flashbots-protect/overview

[10] Flashbots. 2022. *The Future of MEV is SUAVE.* https://writings.flashbots.net/the-future-of-mev-is-suave

[11] Flashbots. 2024. *Introducing Rollup Boost.* https://writings.flashbots.net/introducing-rollup-boost

[12] Harry Kalodner, Steven Goldfeder, Xiaoqi Chen, S Matthew Weinberg, and Edward W Felten. 2018. Arbitrum: Scalable, private smart contracts. In *27th USENIX Security Symposium (USENIX Security 18)*. 1353–1370.

[13] Jason Milionis, Ciamac C Moallemi, and Tim Roughgarden. 2023. Automated market making and arbitrage profits in the presence of fees. *arXiv preprint arXiv:2305.14604* (2023).

[14] Jason Milionis, Ciamac C Moallemi, Tim Roughgarden, and Anthony Lee Zhang. 2022. Automated market making and loss-versus-rebalancing. *arXiv preprint arXiv:2208.06046* (2022).

[15] Robert Miller. 2023. *MEV-Share: programmably private orderflow to share MEV with users.* https://collective.flashbots.net/t/mev-share-programmably-private-orderflow-to-share-mev-with-users/1264

[16] Optimism. [n. d.]. *Optimism Docs.* https://docs.optimism.io/

[17] Optimism. 2019. *Introducing the OVM.* https://medium.com/plasma-group/introducing-the-ovm-db253287af50

[18] COW Protocol. [n. d.]. *MEV Blocker.* https://cow.fi/mev-blocker

[19] Dan Robinson and Georgios Konstantopoulos. 2020. *Ethereum is a Dark Forest.* https://www.paradigm.xyz/2020/08/ethereum-is-a-dark-forest

[20] Dan Robinson and Dave White. 2024. *Priority Is All You Need.* https://www.paradigm.xyz/2024/06/priority-is-all-you-need

[21] Mark Toda, Matt Rice, and Nick Pai. 2024. *ERC-7683: Cross Chain Intents: An interface for cross-chain trade execution systems.* https://eips.ethereum.org/EIPS/eip-7683

[22] RT Watson. 2024. *Uniswap hits a historic $2 trillion in trading volume.* https://www.theblock.co/post/286679/uniswap-hits-a-historic-2-trillion-in-trading-volume

DISCLAIMER

This paper is for general information purposes only. It does not constitute investment advice or a recommendation or solicitation to buy or sell any investment and should not be used in the evaluation of the merits of making any investment decision. It should not be relied upon for accounting, legal or tax advice or investment recommendations. This paper reflects current opinions of the authors and is not made on behalf of Uniswap Labs, Paradigm, Flashbots, OP Labs, or their affiliates and does not necessarily reflect the opinions of Uniswap Labs, Paradigm, Flashbots, OP Labs, or their affiliates. The opinions reflected herein are subject to change without being updated.