Constitutional proposal

Abstract

This proposal adopts RIP-7212 (Rollup Improvement Proposal), a precompile for verifying the secp256r1 curve on Arbitrum One and Arbitrum Nova. Other major L2s have committed to adopting RIP-7212. Adding support for this precompile would enable account abstraction wallets to cheaply verify a type of signature widely used in passkeys and secure enclaves.

Motivation

Wallet security is one of the most prominent pain points for crypto users today. Adopting RIP-7212 will reduce the costs of using passkey-based wallets on Arbitrum One and Nova, making them more feasible for everyday use and enabling dApp developers and protocols to offer their users improved UX.

Passkey-based wallets offer a better level of security than a typical EOA and seamless cross-device support. Specifically, adding this precompile will reduce the costs of verifying the secp256r1 curve for account abstraction wallets. Passkeys offer a solution that removes the need for personally storing a private key. They leverage WebAuthn, a global standard for passwordless authentication used by Google, Facebook, Microsoft, and all major web browsers. The private key generated when creating a passkey can be encrypted and then stored in the iCloud Keychain (or the Android Keystore for Android devices). The decryption of the private keys happens in a specialized module located in every iPhone (and other smartphones) called the Secure Enclave. The Secure Enclave ensures a user's private key can never leave the device, transforming a smartphone into a hardware wallet. Users can authorize transactions with biometric features like Touch ID or Face ID when using passkey-based wallets for key management. These qualities add flexibility and significantly improve UX while maintaining high security.

Ethereum currently has a precompile for the secp25k1 curve, which all EOA wallets use as their signature scheme. Account abstraction wallets can use alternative signature schemes, such as the one that passkeys utilize: secp256r1. Without a precompile, verifying this signature onchain is extremely expensive. Adding support for RIP-7212 would decrease the costs of verifying the secp256r1 curve by 99% when compared to current implementations. This makes implementing passkey-based wallets feasible for everyday use. Many wallets, and notably, apps using embedded wallets, have been requesting this feature for over a year.

Rationale

This proposal is aligned with the Arbitrum community's mission and values as per the Constitution:

Ethereum-Aligned

: RIP-7212 is the first Rollup Improvement Proposal adopted by the broader Ethereum ecosystem. The RIP stakeholders coordinate with Ethereum Core Devs to ensure Ethereum will continue to be compatible with the upgrade.

Accessibility

: Many users who are not crypto-native will refuse to write down a seed phrase or buy a dedicated hardware wallet. While options exist to get around those pain points, this upgrade empowers account abstraction wallets to provide high-level security without UX tradeoffs.

Secure

: Passkeys and secure enclaves offer hardware-level security since a user's private key can never leave the device. This is a great alternative to EOAs that does not compromise on usability.

Inclusivity

: RIP-7212 was discussed publicly among all major L2s before being adopted. The codebase is open-source, and anyone can implement the upgrade.

Key Terms

- RIP (Rollup Improvement Proposal)

: A process to establish optional norms and standards for L2s to extend the EVM and related tooling while limiting conflicts with the L1 EVM and preventing a proliferation of mutually incompatible standards among L2s.

- Precompile

: Predefined smart contracts with special addresses that provide specific functionality executed not at the EVM bytecode

level but natively by the client.

Specifications

The specifications of RIP-7212, including test cases, can be found in theRIP repository. If approved, Arbitrum One will use this specification as the reference for implementation.

The Ethereum Magicians Forum discusses design decisions, iterations, and the transformation of the proposal from an EIP (Ethereum Improvement Proposal) to a RIP.

Steps to Implement

If the Arbitrum DAO approves the AIP, the path would consist of:

1. Discussion of the proposal on the forum and governance call(s)
2. A vote on Snapshot to enable RIP-7212 on Arbitrum Sepolia
3. Sufficient time for testing on a public testnet that emulates production environments
4. An onchain vote to deploy the upgrade on Arbitrum One and Arbitrum Nova

Timeline

This proposal will be included in the vote to upgrade to the next version of ArbOS along with Stylus, which will move to a Snapshot vote once it is production-ready.

NOTE:

If this vote passes on Snapshot, the tentative plan is to upgrade Arbitrum Sepolia to arbOS 30 the week of June 10th.

If Arbitrum Sepolia upgrades to arbOS 30, there will be an ecosystem-wide plan to ensure non-breaking compatibility of infrastructure and applications with Stylus, which will take several weeks or months. The ultimate goal is that the experience for EVM developers remains as unchanged as possible if arbOS reaches mainnet. Once enough confidence is reached, there will be an onchain vote to upgrade Arbitrum One and Nova to arbOS 30. The Arbitrum community will be informed of any significant updates as they arise.