**Ethereum’s ERC-4337 Account Abstraction Smart Contract is Live**

ERC-4337 will introduce a new mempool for user operations

BY[BESSIE LIU](https://blockworks.co/author/bessieliu)/

MARCH 2, 2023 07:25 AM



Shizume/Shutterstock.com modified by Blockworks

SHARE

An audited version of the Ethereum Foundation’s ERC-4337 account abstraction standard is now available on Ethereum mainnet.

The standard has been implemented through the smart contract [EntryPoint](https://etherscan.io/address/0x0576a174D229E3cFA37253523E645A78A0C91B57" \l "code" \t "_blank), which has been running for a few weeks already — and is designed to change how users interact with wallet services.

Most of Ethereum’s existing wallets are externally owned accounts (EOA). The list, which makes up a majority of wallets now in the [Ethereum](https://blockworks.co/tag/ethereum) ecosystem, includes providers like MetaMask and imToken.

And it even extends to hardware wallets such as Ledger Nano, where only one key controls an account — meaning that if its key is compromised or lost, any tokens within the wallet would be, too.

With account abstraction, the idea would be to make the account flexible to match users needs, according to Yoav Weiss, a security fellow at the Ethereum Foundation.

The foundation is a nonprofit dedicated to supporting the development of the Ethereum ecosystem, including its native token, ether ([ETH](https://blockworks.co/price/eth)).

“For some users, this may simply mean getting the user experience of a bank — where someone can always help recover your bank account even if you lose your password,” Weiss, an author of the ERC-4337 [proposal](https://eips.ethereum.org/EIPS/eip-4337), told Blockworks. “For more sophisticated users, it could mean adding more controls or features to your account.”

An example? Adding two-factor authentication to spend more than $5,000 dollars, Weiss said. The measure also allows users to use the cryptographic signature of their choosing, and it also authorizes transactions securely through cell phones.

Unlike EOAs, account abstraction enables users to use smart contract wallets with arbitrary verification logic.

“So now, users don’t need to think about writing down 12 words on a piece of paper, but instead, they are able to add and remove devices and include recovery options with a friend or a lawyer,” Weiss said.

Implementing an ERC-4337 standard

Account abstraction has been in the works for over nine years. It’s been difficult to reach a consensus and change an entire protocol to support it.

“We needed to better understand security and better understand usability, but you can’t [take] action for something that requires a protocol change because there is no input, and that’s where ERC-4337 comes in,” Weiss said.

ERC — short for Ethereum request for comment — is an opt-in standard that no one is obligated to use. Instead of changing consensus rules, ERC ensures everyone agrees to a standard before they begin using it on-chain.

One prevalent example: the ERC-20 token standard. ERC-20 doesn’t alter Ethereum at its protocol level. But, because developers have agreed tokens should follow ERC-20 rules, it has set a standard.

“Having a standard creates an ecosystem,” Weiss said. “And what ERC-4337 does is it will create a standard for account abstraction.”

Existing products such as Gnosis Safe and Argent have already implemented features such as social recovery. But in order to maintain them, they would have to connect to a centralized relayer.

If a centralized relayer is attacked, users would not be able to access their accounts.

ERC-4337 will introduce a new mempool for user operations.

This mempool is serviced by “bundlers” — similar to validators and miners — but on an accounts function level. So rather than submitting a transaction, a user would submit a user operation to the mempool, and bundlers will take it from the mempool and include it in blocks on Ethereum or any other EVM chain, Weiss said.

One of the first protocols to comply with the ERC-4337 standard for bundlers is Stackup.

“We have a test for bundlers to make sure they are ready, and stackup was one of the first ones to be ready,” Weiss said.

The company will allow developers to build customized Web3 transaction flows and wallets using the latest ERC-4337 smart contract.

“Developers won’t need to think about how each blockchain works, the wallet only needs to support ERC-4337, and it can be deployed and used on any EVM chain,” Weiss said.

<https://blockworks.co/news/ethereum-erc4337-account-abstraction-smart-contract>