**Understanding ERC-4337: The Standard for Web3 Messaging**



Published

 2 months ago

on

 July 3, 2023

By

[**Kyrian Alex**](https://cryptotvplus.com/author/kyrian/)



The blockchain and Ethereum ecosystems have experienced remarkable progress due to the rise and acceptance of decentralized applications (dApps). One noteworthy advancement in this landscape is the emergence of the ERC-4337 standard, which has garnered considerable attention for its standardized messaging approach on the Ethereum blockchain.

In this article, we will delve into the intricacies of ERC-4337, comprehensively exploring its operational mechanisms and examining the multitude of advantages it brings to the ever-evolving blockchain space. By understanding the inner workings of this standard, we can gain valuable insights into its potential impact on enhancing the functionality and efficiency of decentralized applications, ultimately propelling the growth of the Ethereum ecosystem.

**What exactly is ERC-4337?**

In 2021, Ethereum co-founder Vitalik Buterin and a group of developers introduced [ERC-4337](https://eips.ethereum.org/EIPS/eip-4337) as a groundbreaking solution for account abstraction. This innovative standard was successfully deployed on the Ethereum mainnet in March 2023, marking a significant milestone in the evolution of the platform.

ERC-4337 serves as a standardized protocol for facilitating message passing on the Ethereum blockchain. Its primary objective is to establish seamless communication channels between smart contracts, dApps, and other decentralized entities operating within the Ethereum network. The standard outlines a set of predefined functions and events that enable the transmission and reception of messages, alongside a defined format for structuring these messages.

ERC-4337 not only simplifies communication within the Ethereum network but also plays a pivotal role in Web3 messaging. With its implementation, user-friendly cryptocurrency wallet designs are anticipated to become a reality, revolutionizing the way users interact with the Ethereum ecosystem.

**What is Web3 messaging?**

Web3 messaging is a new way of communicating that refers to the utilization of messaging protocols and standards within decentralized applications. This means that messages are not stored on a central server, and they cannot be censored or intercepted.

By adopting ERC-4337, dApps and other entities can communicate using a uniform format, fostering interoperability and collaboration within the Ethereum ecosystem. This standardized approach paves the way for enhanced innovation and the development of groundbreaking applications.

**How does ERC-4337 operate?**

ERC-4337 encompasses a collection of functions designed for sending and receiving messages between smart contracts and various entities within the Ethereum network. These functions include:

1. send: This function facilitates the transmission of a message to a specific recipient.

2. broadcast: It enables the dissemination of a message to all subscribers within the network.

3. subscribe: By employing this function, entities can subscribe to a specific topic.

4. unsubscribe: Entities can leverage this function to unsubscribe from a particular topic.

In addition to these functions, ERC-4337 also defines a range of events that can be triggered when messages are sent and received. These events encompass:

1. MessageSent: This event occurs when a message is successfully dispatched.

2. MessageReceived: It is emitted when a message is received by the intended recipient.

Messages themselves are constructed using a JSON format, which comprises a topic field, a data field, and a timestamp. Topics serve the purpose of categorizing messages, while the data field can accommodate any form of data that can be serialized into JSON.

**Account Abstraction and ERC-4337**

Account abstraction is a concept closely associated with ERC-4337. This concept aims to improve the Ethereum user experience and smart contract wallet security without altering the blockchain’s consensus protocol. It allows the functionalities of both externally owned accounts (EOA) and smart contract accounts (SCA) within a single account.

EOAs can initiate transactions, while SCAs execute contract codes after receiving transactions from EOAs. Account abstraction simplifies wallet designs, enables social recovery and customization, and brings smart contract functionality to wallets.

ERC-4337 also introduces UserOperations, a pseudo-transaction object that allows bundlers to package multiple transactions together, enhancing transaction efficiency. It addresses the issue of account recovery by providing customizable recovery services. This standard not only enhances the user experience but also has the potential to boost the mass adoption of cryptocurrencies.

The introduction of this innovative technology has brought about an increase in the number of roles involved in transaction processes. These roles consist of:

1. Bundlers: These nodes take on the responsibility of bundling transactions within the blockchain and transmitting them to a bundle marketplace.

2. Aggregators: Helper contracts that play a crucial role in validating and aggregating signatures. Bundlers are tasked with the responsibility of authorizing and listing supported aggregators.

3. Senders: Account contracts designed to send UserOperations, which are a data model utilized to describe transactions sent on behalf of a user.

**Pros and Cons of ERC-4337**

Implementing ERC-4337 brings forth a range of advantages and disadvantages that should be taken into consideration. Let’s examine them.

**Pros:**

* Decentralized Wallet Control: ERC-4337 ensures that control over wallets remains decentralized, avoiding centralization.
* Enhanced Wallet Security: The standard offers improved wallet security by supporting advanced options like 2FA and easier implementation of multi-signatures. It also simplifies wallet development, reducing complexity.
* Simplified Wallet Management: ERC-4337 reduces complexity in wallet management and control, making it more accessible to individuals with limited knowledge of cybersecurity and cryptocurrencies.
* Multi-Chain Support and Interoperability: The standard, based on Solidity and EVM, allows for multi-chain support without altering the consensus protocol, facilitating interoperability between different chains.
* Commission Replacement: ERC-4337 maintains the option to replace commissions by sending a new operation with a higher commission.
* Execution Logic Flexibility: Wallets implementing ERC-4337 can incorporate custom logic into the execution step, such as atomic multi-operations.

**Cons:**

* Slight Increase in DoS Vulnerability: Despite efforts to mitigate risks, the verification logic in ERC-4337 can be slightly more complex than the standard ECDSA verification, leading to a minor increase in DoS vulnerability.
* Gas Overload: Transactions involving ERC-4337 smart contracts may have slightly higher gas overhead compared to normal transactions. However, the overhead can be offset in certain use cases by multi-trade support. It’s important to note that using this feature may result in higher fees.
* Single Transaction Limit: Accounts cannot queue and submit multiple transactions to the mempool simultaneously. However, the ability to perform atomic multi-operations helps mitigate the need for queuing multiple transactions.

**Conclusion**

The advent of ERC-4337 critical milestones within the blockchain and decentralized application landscape. Through the provision of a standardized messaging interface on the [Ethereum](https://cryptotvplus.com/education/eth/) network, ERC-4337 empowers dApps and entities to communicate with one another in a consistent and streamlined manner. This open line of communication will be fundamental to the development of interoperable systems and sets the stage for the evolution of the internet’s next generation.

<https://cryptotvplus.com/2023/07/understanding-erc-4337-the-standard-for-web3-messaging/>