



Wallet capability for mempool transactions

jistro.eth, ariutokintumi.eth

Last update: May 25, 2024

ABSTRACT

The objective of this research what wallet can be useful for mempool transactions.

Keywords: EVM, Blockchain

CONTENTS

1	Wallet Criteria	2
2	Hot Wallets for Web Browser / Desktop	2
2.1	Metamask	2
2.2	Trust Wallet	3
2.3	Rainbow Wallet	3
2.4	Zerion	3
2.5	Bitget wallet	3
2.6	OKX wallet	3
2.7	Token Poket	3
2.8	Exodus	3
2.9	MEW wallet / Enkrypt wallet	4
2.10	Onto wallet	4
2.11	Math wallet	4
2.12	Internet Money wallet	4
2.13	Coin97	4
2.14	Frontier	4
2.15	Brave Wallet	4
2.16	Opera Crypto Wallet	4
2.17	Cypher	5
2.18	Rabby wallet	5
2.19	Block wallet	5
2.20	SAFE	5
2.21	Core wallet	5
2.22	Taho	5
2.23	Frame	5
2.24	Coinbase wallet	6
2.25	Phantom wallet	6
2.26	One Key	6
2.27	Oisy wallet	6
2.28	Infinity wallet	6

3	Hot Wallets for Mobile devices	6
3.1	Metamask	6
3.2	Trust Wallet	6
3.3	Rainbow wallet	7
3.4	Uniswap wallet	7
3.5	Zerion Wallet	7
3.6	imToken Wallet	7
3.7	Spot wallet	7
3.8	Bitdet wallet	7
3.9	Crypto.com wallet	7
3.10	OKX wallet	8
3.11	Token Poket	8
3.12	Frontier	8
3.13	Omni web3 wallet	8
3.14	1inch wallet	8
3.15	Exodus	8
3.16	Coinbase Wallet	8
3.17	Alpha wallet	9
3.18	ONTO wallet	9
3.19	Obvious Smart Wallet	9
	References	10

1 WALLET CRITERIA

To assess the suitability of a wallet for integration within the protocol, the following criteria have been established:

- Custom Nonce and Gas Fee Configuration
 - Users should have the capability to set a custom nonce and gas fee directly from the wallet interface.
 - Alternatively, the wallet should support the configuration of nonce and gas fees through a decentralized application (DApp).

This criterion ensures the flexibility of the wallet in adjusting transaction parameters, providing users with direct control or enabling configuration through our protocol.

To identify wallets meeting these criteria, we compiled a list from various sources [1], evaluating their compatibility with our established criteria.

For the DApp, we implemented two versions: one utilizing WalletConnect and Ethers.js, and the other solely relying on Web3.js. This approach allows us to explore different integration methods and assess their respective advantages within the context of our criteria.

2 HOT WALLETS FOR WEB BROWSER / DESKTOP

2.1 Metamask

Usability: **Cannot be used**

- ✗ Custom Nonce
- ✓ Custom Gas Fee Configuration

Despite Metamask allowing users to configure custom gas fees, it currently lacks the functionality for setting a custom nonce directly from the wallet interface. The DApp approach, as observed, generates an incorrect nonce, even if the number is registered in the transaction header. This issue has been reported since 2023 by Ariutokintumi [2].

2.2 Trust Wallet

Usability: **Cannot be used**

- ✓ Custom Nonce
- ✓ Custom Gas Fee Configuration

While Trust Wallet provides the functionality to set a custom nonce and configure gas fees, it cannot be used for our purposes. During testing on the testnet, the configured settings did not reflect accurately. Furthermore, on the mainnet, even when the configuration is displayed correctly, confirming the transaction results in an error message stating `x` is not a valid digit for number system with base 10. This issue renders Trust Wallet unsuitable for our intended use.

2.3 Rainbow Wallet

Usability: **Cannot be used**

- ✗ Custom Nonce
- ✗ Custom Gas Fee Configuration

While Rainbow Wallet offers a user-friendly interface for the average user, it lacks the capability to manually or programmatically set features such as custom networks, custom nonce, and gas fee configurations. This limitation makes Rainbow Wallet unsuitable for our intended use.

2.4 Zerion

Usability: **Cannot be used**

- ✗ Custom Nonce
- ✗ Custom Gas Fee Configuration

While Rainbow Wallet offers a user-friendly interface for the average user, it lacks the capability to manually or programmatically set features such as custom networks, custom nonce, and gas fee configurations. This limitation makes Rainbow Wallet unsuitable for our intended use.

2.5 Bitget wallet

Usability: **Cannot be used**

- ✓ Custom Nonce
- ✓ Custom Gas Fee Configuration

While it is possible to manually set up a custom nonce or gas fee configuration, the inability to set up these features programmatically renders Bitget Wallet unsuitable for our purposes.

2.6 OKX wallet

Usability: **Cannot be used**

- ✗ Custom Nonce
- ✗ Custom Gas Fee Configuration

No additional comments are necessary. The wallet does not offer the functionality we are seeking and is therefore unsuitable for our purposes.

2.7 Token Poket

Usability: **Cannot be used**

- ✗ Custom Nonce
- ✗ Custom Gas Fee Configuration

No additional comments are necessary. The wallet does not offer the functionality we are seeking and is therefore unsuitable for our purposes.

2.8 Exodus

Usability: **Cannot be used**

- ✗ Custom Nonce
- ✗ Custom Gas Fee Configuration

Exodus is notably restrictive in its customization options, lacking the ability to configure custom nonce and gas fees. Even for custom ERC20 tokens, the wallet remains inflexible. As such, it is not suitable for our requirements.

2.9 MEW wallet / Enkrypt wallet

Usability: **Cannot be used**

- ✗ Custom Nonce
- ✗ Custom Gas Fee Configuration

No additional comments are necessary. The wallet does not offer the functionality we are seeking and is therefore unsuitable for our purposes.

2.10 Onto wallet

Usability: **Cannot be used**

- ✗ Custom Nonce
- ✗ Custom Gas Fee Configuration

No additional comments are necessary. The wallet does not offer the functionality we are seeking and is therefore unsuitable for our purposes.

2.11 Math wallet

Usability: **Cannot be used**

- ✗ Custom Nonce
- ✗ Custom Gas Fee Configuration

The interface of Math Wallet is overly complex and confusing, limiting transaction options to only three types of transaction fees. As it does not provide the functionality for custom nonce and gas fee configuration, it is not suitable for our requirements.

2.12 Internet Money wallet

Usability: **Cannot be used**

- ✗ Custom Nonce
- ✓ Custom Gas Fee Configuration

No additional comments are necessary. The wallet does not offer the functionality we are seeking and is therefore unsuitable for our purposes.

2.13 Coin97

Usability: **Cannot be used**

- ✗ Custom Nonce
- ✓ Custom Gas Fee Configuration

No additional comments are necessary. The wallet does not offer the functionality we are seeking and is therefore unsuitable for our purposes.

2.14 Frontier

Usability: **Cannot be used**

- ✗ Custom Nonce
- ✗ Custom Gas Fee Configuration

No additional comments are necessary. The wallet does not offer the functionality we are seeking and is therefore unsuitable for our purposes.

2.15 Brave Wallet

Usability: **Cannot be used**

- ✗ Custom Nonce
- ✓ Custom Gas Fee Configuration

While the Brave Wallet, integrated within the Brave browser, allows for custom gas fee configuration, it lacks the functionality to set a custom nonce programmatically. This limitation renders it unsuitable for our purposes.

2.16 Opera Crypto Wallet

Usability: **Cannot be used**

- ✗ Custom Nonce
- ✗ Custom Gas Fee Configuration

Similar to the Brave Wallet but in opera, this wallet lacks the ability to set custom nonce and gas fee configurations. Additionally, its interface is confusing and overly limited in functionality. As a result, it is not suitable for our requirements.

2.17 Cypher

Usability: **Cannot be used**

- ✗ Custom Nonce
- ✗ Custom Gas Fee Configuration

No additional comments are necessary. The wallet does not offer the functionality we are seeking and is therefore unsuitable for our purposes.

2.18 Rabby wallet

Usability: **Cannot be used**

- ✗ Custom Nonce
- ✗ Custom Gas Fee Configuration

While Rabby Wallet incorporates safety precautions for typical users, it lacks the functionality we require. Therefore, it is unsuitable for our purposes.

2.19 Block wallet

Usability: **Cannot be used**

- ✗ Custom Nonce
- ✗ Custom Gas Fee Configuration

No additional comments are necessary. The wallet does not offer the functionality we are seeking and is therefore unsuitable for our purposes.

2.20 SAFE

Usability: **Cannot be used**

- ✗ Custom Nonce
- ✗ Custom Gas Fee Configuration

No additional comments are necessary. The wallet does not offer the functionality we are seeking and is therefore unsuitable for our purposes.

2.21 Core wallet

Usability: **Cannot be used**

- ✗ Custom Nonce
- ✗ Custom Gas Fee Configuration

The official wallet for Avalanche c-chain, the Core Wallet does not provide the functionality we require. However, in a conversation on February 2nd 2024, we discussed this issue with the Avalanche team. They have expressed interest in discussing a potential future implementation to address our requirements with the development team behind the wallet. As of now, it remains unsuitable for our purposes.

2.22 Tahoe

Usability: **Cannot be used**

- ✗ Custom Nonce
- ✗ Custom Gas Fee Configuration

No additional comments are necessary. The wallet does not offer the functionality we are seeking and is therefore unsuitable for our purposes.

2.23 Frame

Usability: **Can be used**

- ✓ Custom Nonce
- ✓ Custom Gas Fee Configuration

Frame offers the functionality we require, allowing users to configure custom nonce and gas fees. However, it is important to note that Frame is a desktop wallet, and its integration with DApps requires the use of a browser extension that facilitates injected connections.

2.24 Coinbase wallet

Usability: **Can be used**

- ✓ Custom Nonce
- ✓ Custom Gas Fee Configuration

Coinbase Wallet provides the functionality we require, enabling users to configure custom nonce and gas fees. However, it is worth noting that the custom nonce feature may appear hidden within the transaction interface. Despite this, the behavior aligns with our expectations.

2.25 Phantom wallet

Usability: **Cannot be used**

- ✗ Custom Nonce
- ✗ Custom Gas Fee Configuration

No additional comments are necessary. The wallet does not offer the functionality we are seeking and is therefore unsuitable for our purposes.

2.26 One Key

Usability: **Cannot be used**

- ✗ Custom Nonce
- ✗ Custom Gas Fee Configuration

Despite being an open-source wallet, One Key does not offer the functionality we are seeking and is therefore unsuitable for our purposes.

2.27 Oisy wallet

Usability: **Cannot be used**

- ✗ Custom Nonce
- ✗ Custom Gas Fee Configuration

Utilizing an Internet Computer Protocol (ICP) canister for the implementation of an Ethereum Virtual Machine (EVM) wallet, Oisy Wallet does not offer the functionality we are seeking and is therefore unsuitable for our purposes.

2.28 Infinity wallet

Usability: **Cannot be used**

- ✗ Custom Nonce
- ✗ Custom Gas Fee Configuration

For desktop only, no additional comments are necessary. The wallet does not offer the functionality we are seeking and is therefore unsuitable for our purposes.

3 HOT WALLETS FOR MOBILE DEVICES

Due to accessibility limitations on Apple devices, the next phase of our investigation will focus on assessing Android applications.

3.1 Metamask

Usability: **Cannot be used**

- ✗ Custom Nonce
- ✗ Custom Gas Fee Configuration

It currently lacks the functionality to set a custom nonce or gas fee programmatically from the wallet interface. Therefore, it is unsuitable for our purposes.

3.2 Trust Wallet

Usability: **Cannot be used**

- ✗ Custom Nonce
- ✗ Custom Gas Fee Configuration

While Trust Wallet provides the functionality to set a custom nonce and configure gas fees, it cannot be used for our purposes. During testing on the testnet, the configured settings did not reflect accurately. Furthermore, on the mainnet, even when the configuration is displayed correctly, confirming the transaction results in an error message stating x is not a valid digit for number system with base 10. This issue renders Trust Wallet unsuitable for our intended use.

3.3 Rainbow wallet

Usability: **Cannot be used**

- ✗ Custom Nonce
- ✗ Custom Gas Fee Configuration

While Rainbow Wallet offers a user-friendly interface for the average user, it lacks the capability to manually or programmatically set features such as custom networks, custom nonce, and gas fee configurations. This limitation makes Rainbow Wallet unsuitable for our intended use.

3.4 Uniswap wallet

Usability: **Cannot be used**

- ✗ Custom Nonce
- ✗ Custom Gas Fee Configuration

No additional comments are necessary. The wallet does not offer the functionality we are seeking and is therefore unsuitable for our purposes.

3.5 Zerion Wallet

Usability: **Cannot be used**

- ✗ Custom Nonce
- ✗ Custom Gas Fee Configuration

No additional comments are necessary. The wallet does not offer the functionality we are seeking and is therefore unsuitable for our purposes.

3.6 imToken Wallet

Usability: **Cannot be used**

- ✗ Custom Nonce
- ✗ Custom Gas Fee Configuration

While imToken Wallet allows for the manual configuration of custom gas fees within the app, it lacks the functionality to programmatically set a custom gas fee. Additionally, it does not offer the ability to set a custom nonce. Therefore, it is unsuitable for our purposes.

3.7 Spot wallet

Usability: **Cannot be used**

- ✗ Custom Nonce
- ✗ Custom Gas Fee Configuration

Spot Wallet is not suitable for our purposes due to its impending deprecation in January 2024. Even if the app were usable (which it is not), it would become unsafe by February 2024. Therefore, it is unsuitable for our requirements.

3.8 Bitdet wallet

Usability: **Cannot be used**

- ✗ Custom Nonce
- ✗ Custom Gas Fee Configuration

Despite offering the functionality to configure manually custom gas fees, Bitdet Wallet lacks the ability to set custom nonce. Additionally, its confusing custom chain configuration renders it unsuitable for our requirements.

3.9 Crypto.com wallet

Usability: **Cannot be used**

- ✗ Custom Nonce
- ✗ Custom Gas Fee Configuration

No additional comments are necessary. The wallet does not offer the functionality we are seeking and is therefore unsuitable for our purposes.

3.10 OKX wallet

Usability: **Cannot be used**

- ✗ Custom Nonce
- ✗ Custom Gas Fee Configuration

OKX Wallet presents the same limitations as its web extension counterpart, lacking both custom nonce and gas fee configuration. Therefore, it is not suitable for our purposes.

3.11 Token Poket

Usability: **Cannot be used**

- ✗ Custom Nonce
- ✗ Custom Gas Fee Configuration

Despite its well-designed interface as the web extension, Token Pocket does not meet our requirements as it lacks both custom nonce and gas fee configuration capabilities. Therefore, it is not suitable for our purposes.

3.12 Frontier

Usability: **Cannot be used**

- ✗ Custom Nonce
- ✗ Custom Gas Fee Configuration

Frontier app restricts users to using only the chains it was designed for and enforces the use of "safest" gas configurations. This limitation renders it unsuitable for our purposes.

3.13 Omni web3 wallet

Usability: **Cannot be used**

- ✗ Custom Nonce
- ✗ Custom Gas Fee Configuration

No additional comments are necessary. The wallet does not offer the functionality we are seeking and is therefore unsuitable for our purposes.

3.14 1inch wallet

Usability: **Cannot be used**

- ✗ Custom Nonce
- ✓ Custom Gas Fee Configuration

While 1inch Wallet allows for custom gas fee configuration, it lacks the functionality to set custom nonce. Therefore, it is unsuitable for our purposes.

3.15 Exodus

Usability: **Cannot be used**

- ✗ Custom Nonce
- ✗ Custom Gas Fee Configuration

Exodus, like its web extension counterpart, is very limited in functionality. It lacks the ability to set custom nonce and gas fee configuration, making it unsuitable for our purposes. Additionally, even the tokens displayed in the interface are limited. Therefore, it does not meet our requirements.

3.16 Coinbase Wallet

Usability: To be confirm

- ? Custom Nonce
- ✓ Custom Gas Fee Configuration

While it appears that Coinbase Wallet allows for programmable gas fee configuration, the visibility of custom nonce settings is unclear from the interface. Further investigation is required to confirm whether this wallet meets our requirements.

3.17 Alpha wallet

Usability: **Cannot be used**

- ✓ Custom Nonce
- ✗ Custom Gas Fee Configuration

While Alpha Wallet allows for custom nonce configuration, it does not respect custom gas fee configurations. Therefore, it is not suitable for our purposes.

3.18 ONTO wallet

Usability: **Cannot be used**

- ✗ Custom Nonce
- ✗ Custom Gas Fee Configuration

ONTO Wallet requires phone permissions and allows users to send ETH/ERC20 using their linked phone number, which deviates from our requirements. Additionally, it lacks the functionality for custom nonce and gas fee configuration. Therefore, it is unsuitable for our purposes.

3.19 Obvious Smart Wallet

Usability: **Cannot be used**

- ✗ Custom Nonce
- ✗ Custom Gas Fee Configuration

No additional comments are necessary. The wallet does not offer the functionality we are seeking and is therefore unsuitable for our purposes.

REFERENCES

- [1] WalletConnect, “Explorer.” [Online]. Available: <https://explorer.walletconnect.com/?type=wallet>
- [2] ariutokintumi, “Received and Confirmed Custom Nonce is Ignored by the Transaction Constructor,” Sep. 2023. [Online]. Available: <https://github.com/MetaMask/metamask-extension/issues/20784>