Abstract

We propose Lido consider support Tor Wallet by their Grants program. TorWallet wishes to equip Grantors and Grantees with a robust set of tools to simplify, streamline, and increase transparency for participants in the grants process.

Tor Wallet is a first EVM compatible privacy focused wallet with built-in TOR. Earn TOR tokens on every transactions you made.

Problem Statement

When relying on conventional wallets, your IP address is transmitted to various third-party services. These services may also have visibility into multiple wallet addresses associated with you. This exposes you to potential tracking and surveillance, as well as the risk of transaction censorship. Tor Wallet, on the other hand, eliminates these concerns by integrating the Tor protocol, ensuring that your IP address and wallet-related information remain confidential and secure, protecting you from unwanted tracking and transaction censorship.

Solution

Tor Wallet goes beyond just preventing such privacy risks; it offers advanced features to enhance both privacy and security. By integrating the Tor protocol, Tor Wallet ensures that your IP address is shielded, preventing any potential tracking or surveillance associated with your wallet activities.

Moreover, Tor Wallet incorporates additional layers of privacy and security measures, providing users with a comprehensive solution that goes above and beyond traditional wallets. Experience a new level of confidence in your blockchain interactions with Tor Wallet’s robust privacy and security features.

Technical Framework

Torwallet is compatibility with EVM, and its compatible blockchains has greatly improvised our project, due to the added features of high decentralization, and scalability.

- Circuit Management

We establish and manage a pool of dormant Tor circuits.

Upon necessity, we select a circuit at random and withdraw it from the pool.

We eliminate the need to wait for circuit creation by directly selecting one from the pool. Simultaneously, the pool seamlessly generates additional circuits in the background.

- IP Address Collision

Typically, we make diligent efforts to ensure that the two sets of circuits do not overlap. However, it is important to note that there exists a low, albeit possible, probability that a wallet may utilize a TOR exit node that has been employed by another wallet in the past.

- Evil RPC

While there is a chance that the two wallets share the same IP address, suggesting potential control by the same individual, absolute certainty is challenging due to the widespread reuse of IP addresses by numerous users.

Risks & challenges

- The Tor network

Our commitment extends beyond just leveraging the Tor network; we plan to enhance its capabilities by introducing WebTor and persistently contributing to its development. Having already addressed security issues within Tor, we are dedicated to a future that not only safeguards privacy but also strengthens the Tor network for everyone.

- Project side

Yet, our journey is far from concluded. Our ongoing commitment revolves around crafting an unparalleled user experience while upholding our principle of “zero-cost privacy.” This presents a substantial challenge, especially considering that many traditional wallets grapple with UX complexities without being encumbered by the same privacy and security constraints that define our wallet. Nevertheless, we’re determined to overcome these challenges and set new standards in user-friendly, private, and secure wallet experiences.

** Specifications**

We propose Lido augment the existing grants program by integrating TorWallet for processing grant applications from members of the Lido community.

TorWallet will be able to continue disbursal of grant funds via the Lido "Grant