Poster: I Know What Crypto You Got Last Summer: A Study on Web3 Wallet Security and Privacy

Weihong Wang
DistriNet, KU Leuven
Leuven, Belgium
weihong.wang@kuleuven.be

Tom Van Cutsem
DistriNet, KU Leuven
Leuven, Belgium
tom.vancutsem@kuleuven.be

***Abstract*—Web3, also known as the Decentralized Web, is a vision for the next generation of Web applications, supported by blockchain technology, where users have stronger ownership over their data and identity. One of the key components in Web3 is wallets, which hold a user's public and private keys, manage digital tokens, and sign transaction details. Despite their significance in securely managing digital identities, wallets also introduce vulnerabilities that, if overlooked, can compromise users' privacy and security, particularly during data exchange with network endpoints. We investigate how popular wallets like MetaMask can inadvertently expose sensitive information to RPC endpoints, even when no transactions are made. Additionally, we examine the confidentiality risks associated with the registration requirements of major node providers, highlighting how the collection of personal and financial details can further threaten user privacy. We briefly report on ongoing work in analyzing the characteristics of wallets across various blockchain networks to identify key security and privacy features that can be integrated into new wallet designs. This research aims to address the challenges inherent in wallet security and privacy within Web3.**

***Index Terms*—Blockchain Wallets, RPC Endpoints, Node-as-a-Service, User Privacy**

I. Introduction

Blockchain networks enable transactions without intermediaries, with the wallet being a key component. It stores users' public and private keys, allowing them to manage digital assets, sign transactions, and interact with blockchain networks. Among various types, software wallets that are stored within mobile devices or accessible online via web browsers are the most popular due to their ease of use. However, many users may not fully consider how these wallets exchange data with network endpoints.

When a wallet extension connects to a decentralized application (dApp), both the dApp and wallet can independently initiate transactions and requests. For example, a dApp might ask the wallet to sign a transaction, while the wallet may query the latest balance using its own endpoint. Sometimes, the dApp can also use the wallet's endpoint to interact with the blockchain.

These interactions are facilitated by intermediaries known as Node-as-a-Service ("node providers"), which offer permissioned access to endpoints. These endpoints are essentially URLs or interfaces provided by a node provider, allowing applications (including dApps and wallets) to send requests to and receive data from the blockchain network. This reliance arises because running a "full node" requires substantial computational and storage resources, making it impractical for most users or developers.

Typically, a wallet or dApp comes with a developer-configured default API endpoint, though users can opt to set up their own. However, this reliance on external endpoint services poses significant risks. Connections to these node providers involve an API key, which authenticates users and allows providers to monitor and charge for usage. Obtaining an API key usually requires a registration process, often involving the sharing of sensitive personal or financial information.

Moreover, all wallet requests and transactions are sent through these endpoints, exposing a significant amount of privacy-related data about end users such as IP addresses, browser fingerprinting, and request details. It also allows adversaries to potentially trace and track end-user activities across different public addresses, a consequence of queries sent from wallets that end users are fully unaware of.

A major concern with this setup is the vulnerability of wallets to unauthorized access and data breaches, which could compromise users' sensitive information. Since wallets are lightweight applications that interact with the blockchain through these endpoints, the security and privacy of these interactions are crucial.

II. Analysis of Sensitive Data Leakage

The convenience of using wallets and centralized node providers comes with significant trade-offs, particularly in data security and user privacy. This section delves into the privacy risks posed by unintended information leaks in blockchain wallets and how these leaks can be exploited during the Web2 registration processes of node providers.

A. Sensitive Information Leakage through Wallets

Surprisingly, wallets, as a widely used third-party application, provide a node provider with far more information than one might expect [1, 2].

Hopr's DERP tool [3] shows that MetaMask, which by default sends data to Infura, discloses significant metadata to RPC endpoints even without transactions. Our testing revealed MetaMask made about 110 calls in 10 minutes, mainly for chain ID and block number updates. To display tokens for

TABLE I: Comparison of Features and Registration Requirements of Node Providers

Node Provider	Free Public Service	Login	Sign-up			Pricing Plan		Freemium Node Service	Payment		Notes
	No registration	Support wallets	Email address	Full name	Organization name	Based on call type	Tiered plans number	Monthly free usage	Credit card	Crypto	
Alchemy	-	-	●	-	-	●	4	300 million compute units	●	-	-
Infura	-	-	●	●	-	-	5	3 million requests	●	-	-
Quicknode	-	-	●	●	●	●	5	50 million API credits	●	-	can't use before giving address
Ankr	●	●	◐	-	-	-	4	1 million requests	●	-	-
Chainstack	-	-	●	●	●	●	4	3 million request units	●	●	-
Blockdaemon	-	-	●	●	-	●	1	3 million compute units	●	-	-
Getblock.io	-	●	◐	-	-	-	3	1.2 million requests	●	●	-
Nownodes	-	-	●	-	-	-	6	100k requests	●	-	-

● = indicates that the property is provided; in the Sign-up column, it means the property is required.;
◐ = indicates that property is not necessarily required; - = does not provide property.
In the column of Monthly free usage, these metrics (compute units, requests, API credits, etc.) represent the amount of computational work and resource usage as defined by different node providers. All the data was collected before February 2024.

an address, MetaMask sent an $ethCall$, exposing all wallet-controlled addresses to the RPC provider.

This leakage of metadata includes:

- **Linkability of addresses.** This compromises privacy by enabling anyone with access to trace transactions and activities across different addresses, even if separate addresses are used for different purposes.
- **IP address.** Revealing IP addresses can compromise user anonymity and expose their physical location.
- **Browser fingerprint.** Details about the user's browser fingerprint, including system information and other identifiers, can be used to track and identify users across different websites.

B. Confidential information involved when registering at a node provider

We examined 8 well-known Web3 node providers, detailed in Table I, focusing on their API key application processes.

We assessed if services could be accessed without registration. Ankr offers free, no-registration access with 300 requests per minute, while Quicknode requires home addresses and credit card details, increasing entry barriers.

Ankr and Getblock.io allow wallet-based identity, letting users access services with just their wallet address, whereas others require at least an email address.

We reviewed free monthly requests and pricing models; while all offer free daily usage, half charge based on call types.

Lastly, 6 out of 8 providers accept only credit cards. Overall, accessing a blockchain network still requires registration, enabling providers to build user profiles.

III. Ongoing Work

Torres *et. al* [1] conducted a large-scale study on wallet privacy issues, investigating how browser fingerprinting and sensitive wallet address leakage occur when a wallet interacts with decentralized applications (DApps).

Building on that, we will focus on a comprehensive analysis of wallets as independent, lightweight Web3 applications used across various networks, comparing their characteristics from multiple security and privacy perspectives. Specifically, we will address the following questions:

- How much information is sent to an external node provider by a wallet, and how might it be exploited?
- When a wallet connects to a DApp using a permissions model like EIP-2255 [4], are all requested permissions necessary, or does the DApp request more data than needed? Does the DApp use granted permissions for additional actions?
- What data security and privacy features do modern wallets claim?

Through this investigation, we aim to identify key security features and privacy-enhancing measures that can be integrated into the design of a new wallet application.

Acknowledgement

This research is partially funded by the Research Fund KU Leuven.

References

[1] C. F. Torres, F. Willi, and S. Shinde, "Is your wallet snitching on you? an analysis on the privacy implications of web3," in *Proceedings of the 32nd USENIX Conference on Security Symposium*, ser. SEC '23. USA: USENIX Association, 2023.

[2] Y. Erinle, Y. Kethepalli, Y. Feng, and J. Xu, "Sok: Design, vulnerabilities, and security measures of cryptocurrency wallets," 2023.

[3] H. Team. (2024) Derp dumb ethereum rpc provider. [Online]. [Online]. Available: https://derp.hoprnet.org/

[4] (2024) Eip-2255: Wallet permissions system: An interface to restrict access to sensitive methods. [Online]. [Online]. Available: https://eips.ethereum.org/EIPS/eip-2255