Is Your Wallet Snitching On You?
An Analysis on the Privacy Implications of Web3

Christof Ferreira Torres        Fiona Willi        Shweta Shinde
What is Web3?

Web 2.0

• Data is **centralized across a small group** of companies

Web 3.0

• Data is **decentralized through blockchain technology**

• +1,000 Decentralized Applications (DApps)\(^1\)
• Market capitalization estimated at **US $3 billion**\(^2\)

---

\(^1\) dappradar.com
\(^2\) futuremarketinsights.com
Interacting with Web3

User → Visit DApp → app.uniswap.org → Web2-Enabled Browser → Request page → Display page → app.uniswap.org Webserver
Interacting with Web3

User interacting with Web3 using MetaMask, which has over 10 million users.

Web3 Web2-Enabled Browser
Interacting with Web3

User

Connect wallet

Web3 Web2-Enabled Browser

Connect to Account 1 (0xef7...44d5)

Allow this site to:

- See address, account balance, activity and suggest transactions to approve

Only connect with sites you trust. Learn more

Cancel Connect
Interacting with Web3

DApp can now access user specific information (e.g., wallet address)

0xEF7d…44D5

Web3 Web2-Enabled Browser
Interacting with Web3

User

Web3 Web2-Enabled Browser

Retrieve blockchain data (e.g., wallet balance)

Blockchain Client

0.00123 ETH
What about Privacy?

Web3 introduces sensible user information:
- Wallet address
- Transactions
- Balance
- ...

Web3 technology is based on Web2 technology
- DApps may include 3rd party scripts
- Traffic is routed via TCP/IP

Is the privacy of Web3 users at risk?
Contributions

• First large-scale study on wallet address leakage across DApps and wallet extensions

• First measurement study on the prevalence of web3-based browser fingerprinting

• Analysis on the efficacy of popular blocklists against web3-based online tracking
Threat Model

User

3rd Party Scripts (e.g., Advertisers)

Browser

Website

Wallet Extension

3rd Party Blockchain Providers (e.g., Infura)
Problem 1: Wallet Address Leakage

- Your wallet address is **unique**
- Wallet address accessible via MetaMask object

3rd party scripts can read wallet address via JavaScript* and send it to their backend

*Assuming DApp is connected with user’s wallet
Problem 2: Web3-Based Browser Fingerprinting

- Browser fingerprinting is a well-known problem on the web
- Web3 further **augments** this problem

MetaMask injects a JavaScript object into every website a user visits (i.e., `window.ethereum`)

3rd parties can read this JavaScript object to:
- Check which cryptocurrency user owns
- Check which wallet user has installed
- Augment user’s browser fingerprint
Framework Overview

- Websites
- Extensions
- JSON Log File

- Wallet Simulator
- MetaMask Automator

- Wallet APIs
- Leakage Detector

- Tracker Radar Collector
- Request Interceptor

- Puppeteer

- Chrome DevTools Protocol

https://github.com/christofortres/Web3-Privacy
Measuring Wallet Address Leakage

**Crawled 616 DApps automatically**

- Found **211** DApps leaking the user’s wallet address to at least one 3rd party
- Analyzed privacy policy of top 3rd parties: **95%** collect your IP address

---

Wallet address leaked via HTTP GET request to google-analytics.com on the degens.farm DApp

```
https://www.google-analytics.com/collect?v=1&v=j99&a=1044933369&t=event&ni=0_&a=1&d=https%3A%2F%2Fdegens.farm%2Fwallet&ul=en-us&de=UTF-8&dt=degens%2F24%2F0Farm%3A%20Wallet&sd=30-bit&sr=1512x982&vp=1512x749&je=0&ec=WalletConnected&ea=4&ab&d=0x7e4ab63a7c8314cc43883473684f292&el=labelForWalletConnect&ev=7.2899959041511e%2B47&_u=aADAAEABAACAA1-_&id=&cid=437541385.1675387202&tid=UA-201259489-1&_gid=196110698.1675387202&gaid=2ug2105PC6982&jid=1338733511
```
Measuring Leakage Across Wallet Extensions

- **None** of the analyzed wallet extensions **leak your password** or **browser history**
- **13** extensions **leak your wallet address** to third-parties (e.g., blockchain providers, advertisers)
Measuring Web3-Based Browser Fingerprinting

- Found **878** scripts across **1,099** websites leveraging wallet information to perform browser fingerprinting
- Most websites preforming Web3-based browser fingerprinting are related to **Pornography & Sexuality**

Crawled Top 100K Tranco websites

Intercepted JavaScript calls to popular wallet APIs (e.g., `window.ethereum`)

https://static-lvl.xhcdn.com/xh-shared/js/v1d487c898d.ext-detect
Do Blocklists Improve Your Privacy?

• Analyzed efficacy of 5 **popular** Ad blockers:
  – **Whotracks.me** provides **best protection** (43%)
  – **Disconnect** provides **weakest protection** (12%)

• Installing **multiple Ad blockers** improves privacy
  – **Combination** of all blocks 56% of third-parties

<table>
<thead>
<tr>
<th>Ad Blocker</th>
<th>Blocked</th>
<th>Not Blocked</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disconnect</td>
<td>13</td>
<td>95</td>
</tr>
<tr>
<td>DuckDuckGo</td>
<td>38</td>
<td>70</td>
</tr>
<tr>
<td>EasyList</td>
<td>16</td>
<td>92</td>
</tr>
<tr>
<td>EasyPrivacy</td>
<td>33</td>
<td>75</td>
</tr>
<tr>
<td>Whotracks.me</td>
<td>46</td>
<td>62</td>
</tr>
<tr>
<td>Combined</td>
<td>60</td>
<td>48</td>
</tr>
</tbody>
</table>
Conclusion

• **Web3 wallet extensions pose a serious threat** to user’s privacy
  – Found **evidence of popular websites** performing web3-based browser fingerprinting
  – **34% of connected DApps leak the user’s wallet address** to third-parties
  – **44% of the third-parties are not blocked** by popular Ad blockers

• **New solutions** need to be developed **to preserve user’s privacy**
Questions?

christof.torres@inf.ethz.ch

https://github.com/christoftorres/Web3-Privacy