usenix
THE ADVANCED COMPUTING SYSTEMS ASSOCIATION

Is Your Wallet Snitching On You?

An Analysis on the Privacy Implications of Web3

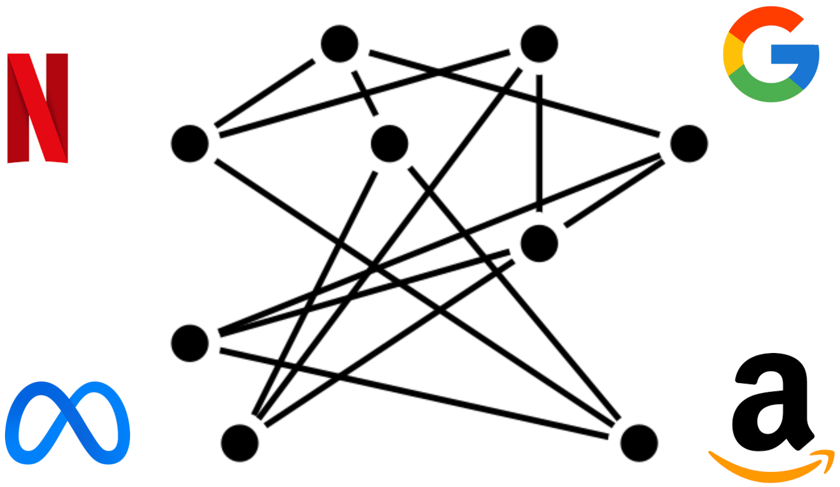
Christof Ferreira Torres Fiona Willi Shweta Shinde

ETH zürich

What is Web3?

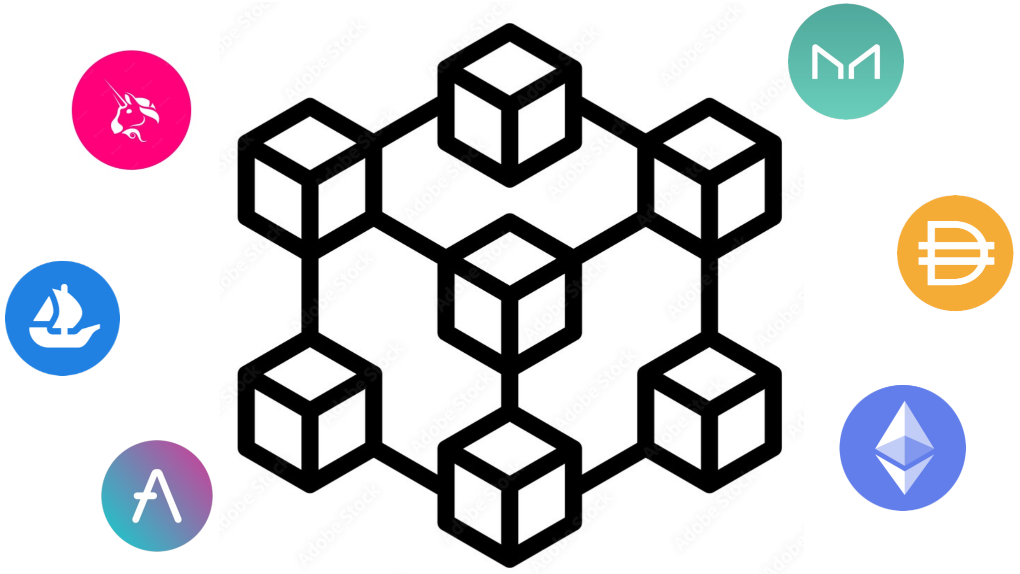
Web 2.0

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



Web 3.0

- Data is **decentralized through blockchain technology**

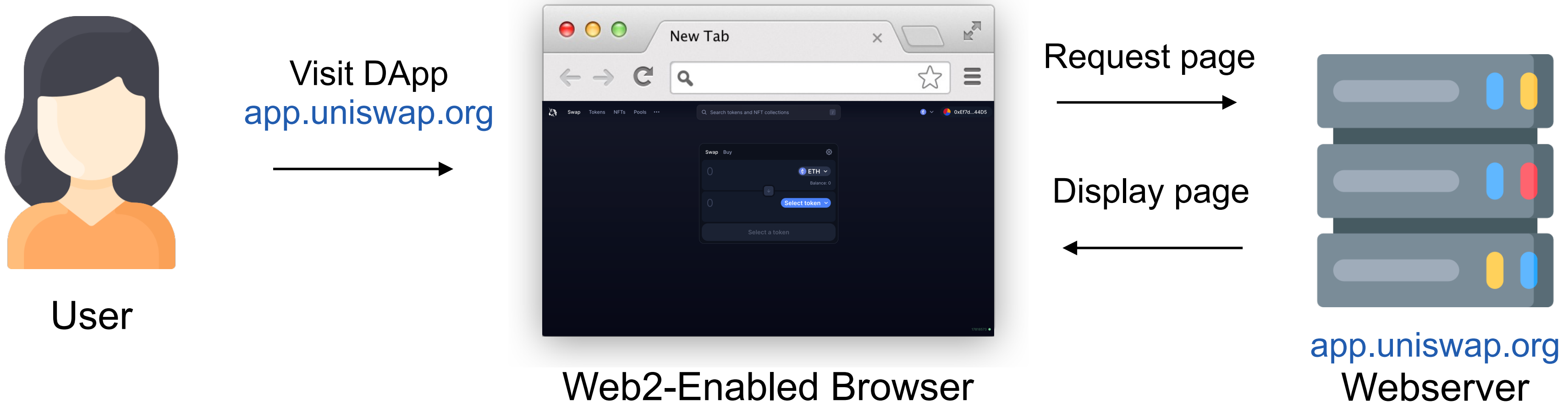


- **+1,000** Decentralized Applications (DApps)[1]
- Market capitalization estimated at **US $3 billion**[2]

[1] dappradar.com

[2] futuremarketinsights.com

Interacting with Web3



User

Visit DApp app.uniswap.org

Web2-Enabled Browser

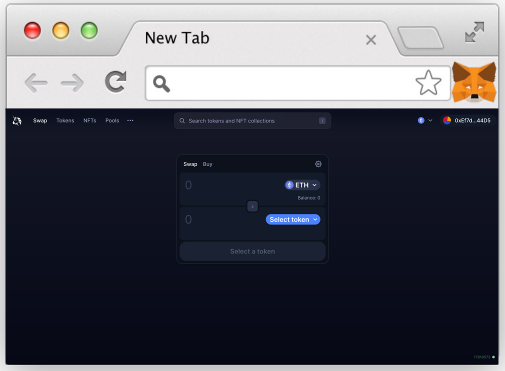
Request page

Display page

app.uniswap.org Webserver

Interacting with Web3

User



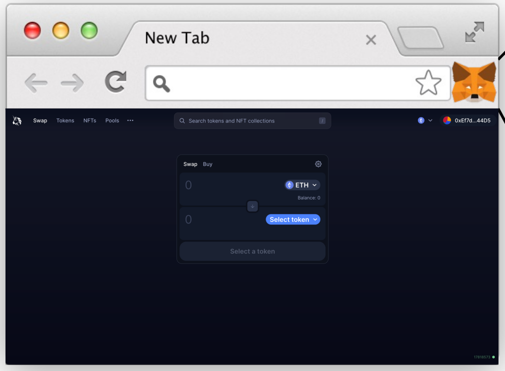
Web3 ~~Web2~~-Enabled Browser

MetaMask
+ 10 million Users

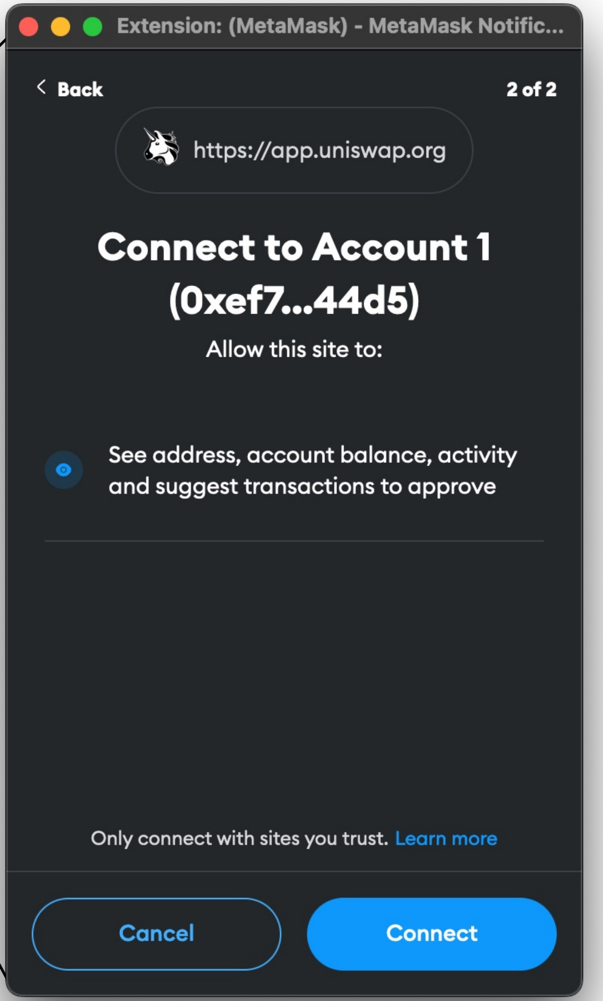
Interacting with Web3

User

Connect wallet



Web3 ~~Web2~~-Enabled Browser



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

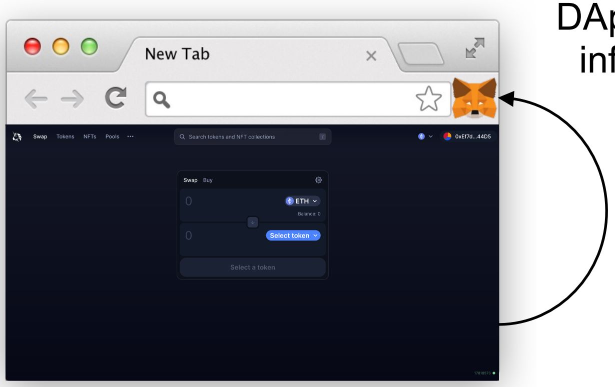
Allow this site to:

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

Only connect with sites you trust. Learn more

Interacting with Web3

User



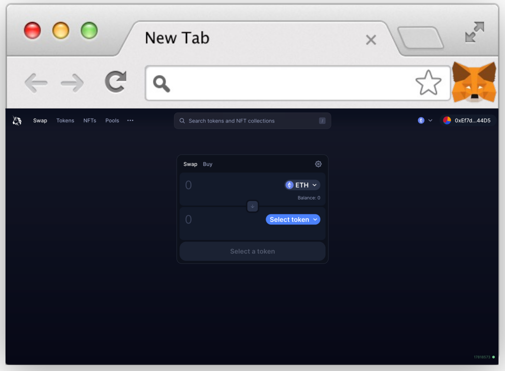
Web3 ~~Web2~~-Enabled Browser

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

0xEf7d…44D5

Interacting with Web3

User

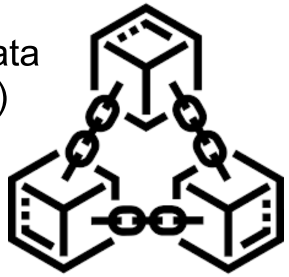


Web3 ~~Web2~~-Enabled Browser

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

→

0.00123 ETH



Blockchain
Client

What about Privacy?

Web3 introduces sensible user information:

- Wallet address
- Transactions
- Balance
- …

Web3 technology is based on Web2 technology

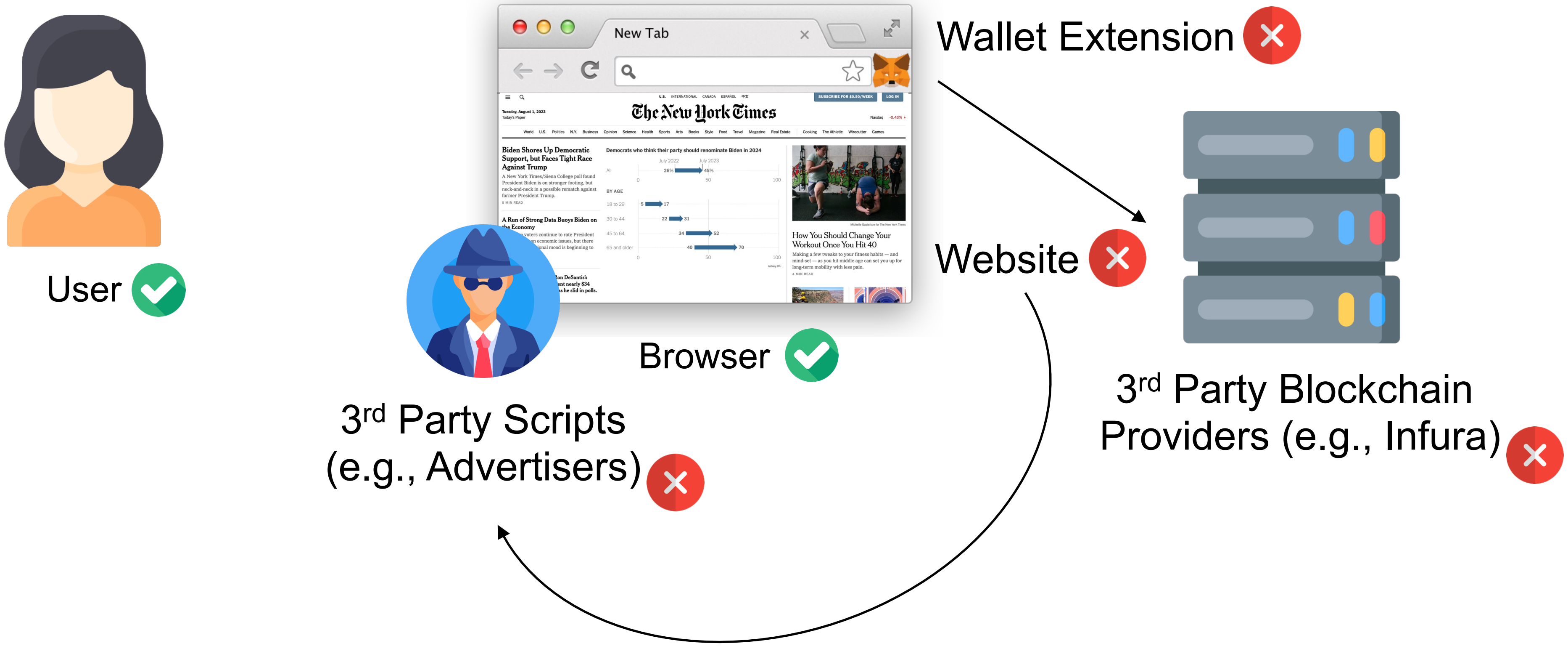
- DApps may include 3rd party scripts
- Traffic is routed via TCP/IP

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 ✓

Browser ✓

Wallet Extension ✗

Website ✗

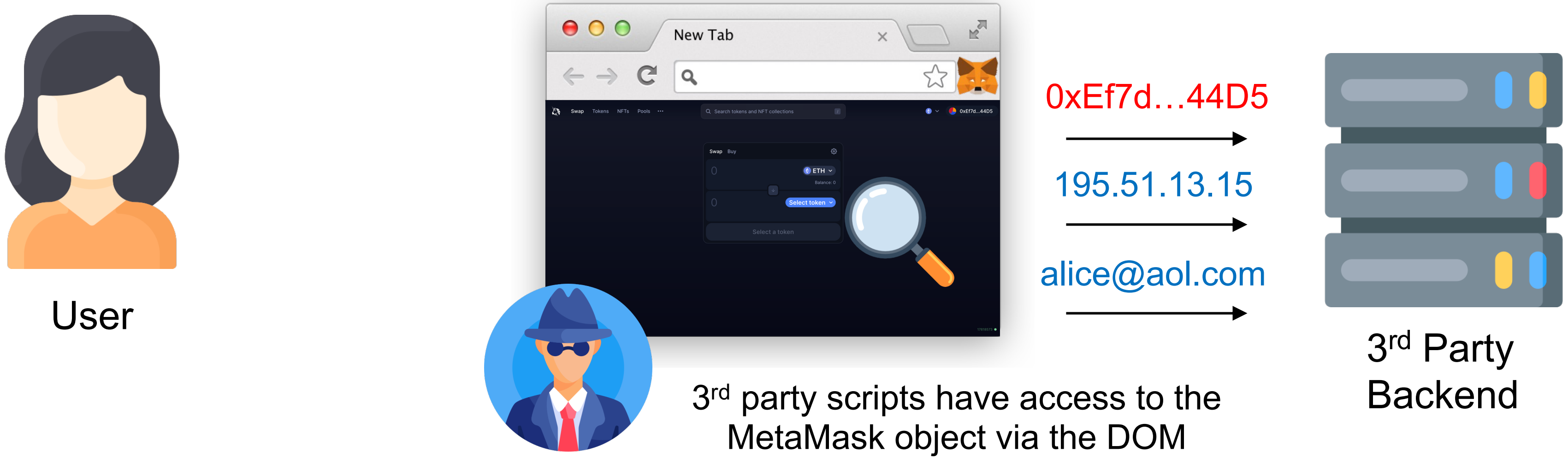
3rd Party Scripts (e.g., Advertisers) ✗

3rd Party Blockchain Providers (e.g., Infura) ✗

Problem 1: Wallet Address Leakage

- Your wallet address is **<u>unique</u>**
- Wallet address accessible via MetaMask object

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



3rd party scripts have access to the MetaMask object via the DOM

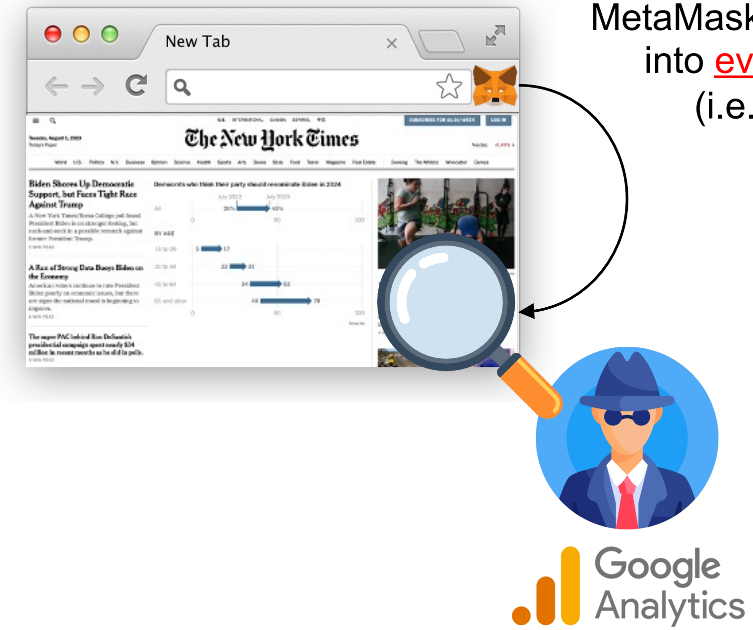
Wallet address can be linked to other personal information (e.g., IP address, email, etc.)

*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

User



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

3rd parties can read this JavaScript object to:

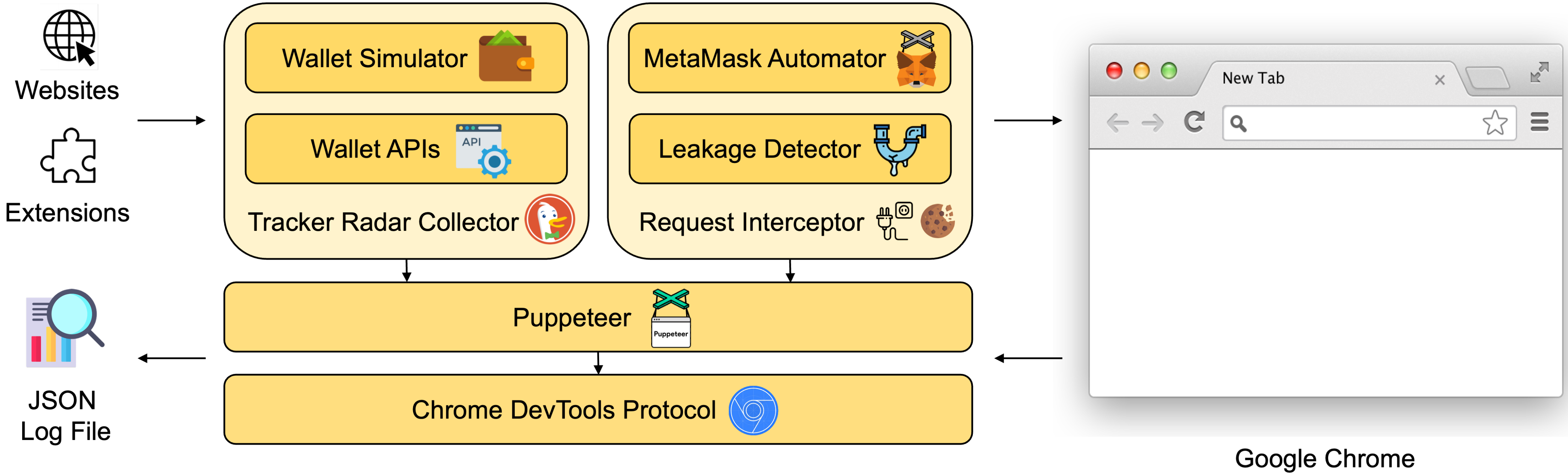
- Check which cryptocurrency user owns
- Check which wallet user has installed
- Augment user’s browser fingerprint

Framework Overview

ARTIFACT EVALUATED usenix ASSOCIATION AVAILABLE

ARTIFACT EVALUATED usenix ASSOCIATION FUNCTIONAL

ARTIFACT EVALUATED usenix ASSOCIATION REPRODUCED



Websites

Extensions

Wallet Simulator

Wallet APIs

Tracker Radar Collector

MetaMask Automator

Leakage Detector

Request Interceptor

Puppeteer

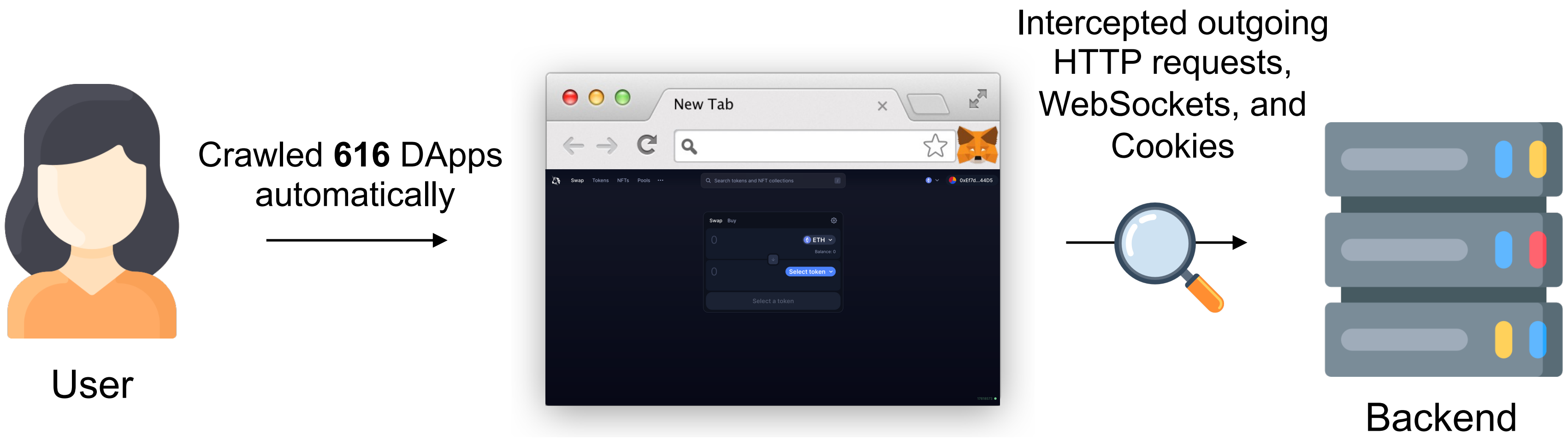
Chrome DevTools Protocol

JSON Log File

Google Chrome

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

Measuring Wallet Address Leakage



User

Crawled **616** DApps automatically

Intercepted outgoing HTTP requests, WebSockets, and Cookies

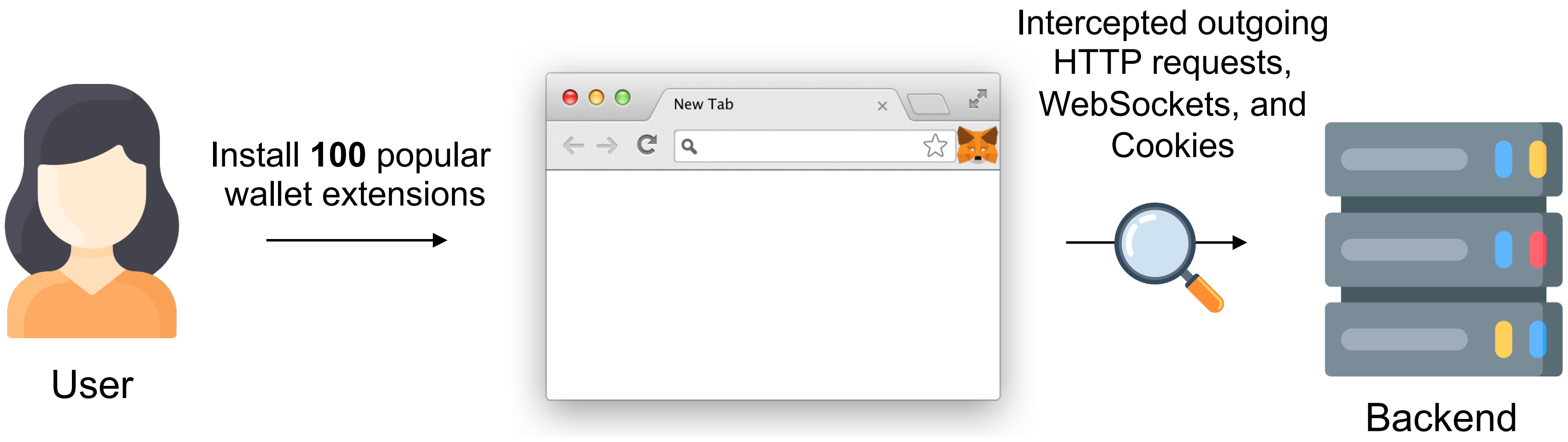
Backend

- 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

```
https://www.google-
analytics.com/collect?v=1&_v=j99&a=1044933369&t=event&ni=0&_s=1&dl=https%3A%2F%2Fdegens.fa
rm%2Fwallet& ul=en-us&de=UTF-8&dt=Degen%27%24%20Farm%3A%20Wallet&sd=30-
bit&sr=1512x982&vp=1512x749&je=0&ec=WalletConnected&ea=0x7e4abd
63a7c8314cc28d388303472353d884f292&el=labelForWalletConnect&ev=7.20999590401511e%2B47&_u=a
ADAAEABAAAAACAAI~&jid=&gjid=&ci d=437541385.1675387202&tid=UA-201259489-
1&_gid=196110690.1675387203&gtm=2wg2105PC69BZ&z=1330733511
```

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

Measuring Leakage Across Wallet Extensions



User

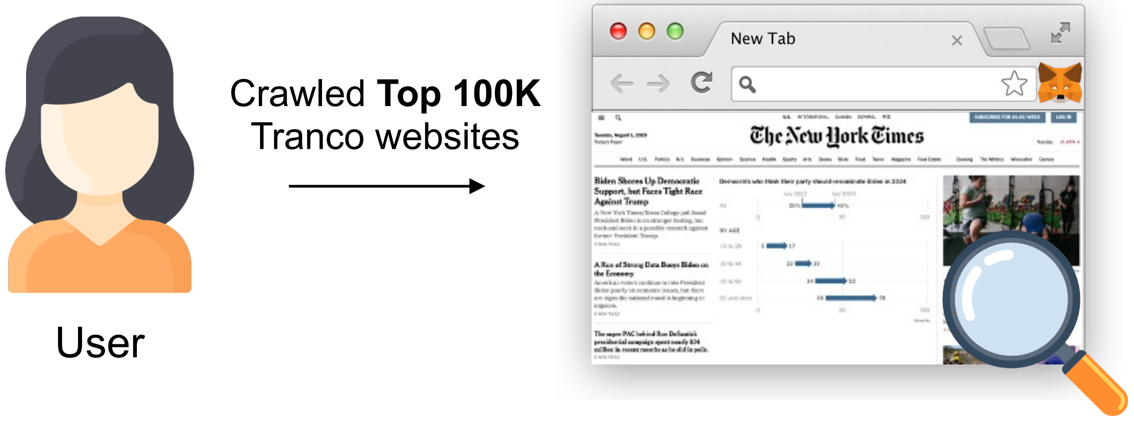
Install **100** popular wallet extensions

Intercepted outgoing HTTP requests, WebSockets, and Cookies

Backend

- **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)

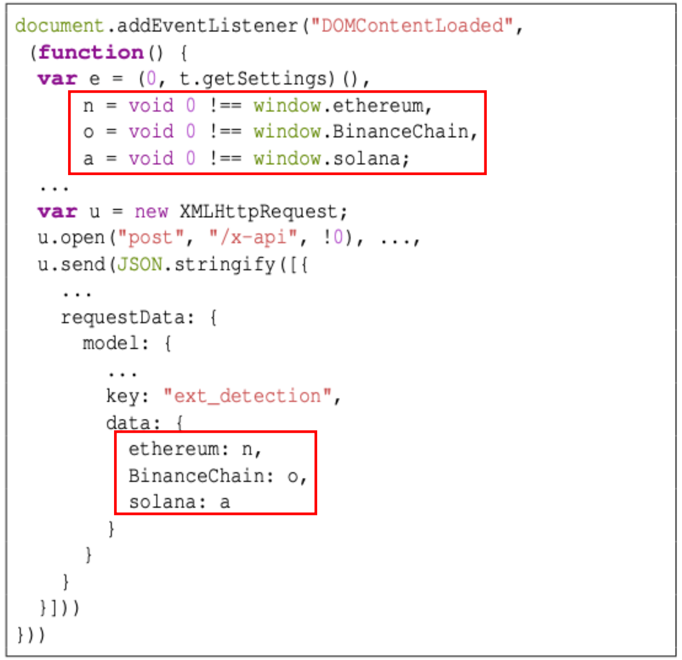
Measuring Web3-Based Browser Fingerprinting



User

Crawled **Top 100K** Tranco websites

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



```
document.addEventListener("DOMContentLoaded",
 (function() {
  var e = (0, t.getSettings)(),
      n = void 0 !== window.ethereum,
      o = void 0 !== window.BinanceChain,
      a = void 0 !== window.solana;
  ...
  var u = new XMLHttpRequest;
  u.open("post", "/x-api", !0), ...,
  u.send(JSON.stringify([{
    ...
    requestData: {
      model: {
        ...
        key: "ext_detection",
        data: {
          ethereum: n,
          BinanceChain: o,
          solana: a
        }
      }
    }
  }]))
}))
```

https://static-lvlt.xhcdn.com/xh-shared/js/v1d487c898d.ext-detect

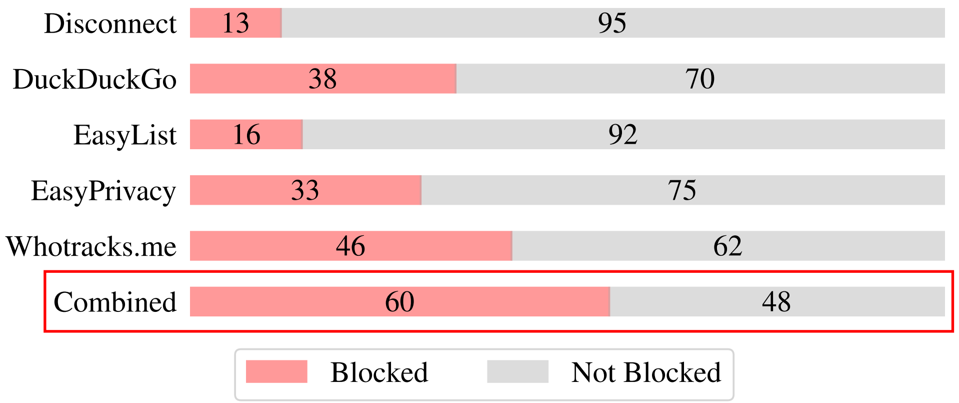
- Found **878** scripts across **1,099** websites leveraging wallet information to perform browser fingerprinting
- Most websites preforming Web3-based browser fingerprinting are related to **Pornography & Sexuality**

ETH zürich

Do Blocklists Improve Your Privacy?

User

- 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



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**

ETH zürich

Questions?

✉ christof.torres@inf.ethz.ch

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