KTH ROYAL INSTITUTE OF TECHNOLOGY

Analysis of the software supply chain of cryptocurrency wallets

Raphina Liu <raphina@kth.se>

Supervised by Sofia Bobadilla, Martin Monperrus and Qinghua Wang
<sofbob@kth.se>, <monperrus@kth.se>, <qinghua.wang@hkr.se>

In blockchain, your assets are connected to a private key.

You lose your key, you lose your assets.

Cryptocurrency wallets keep the user's private keys safe and accessible, allowing them to send and receive cryptocurrencies.

Due to the giant stake involved with crypto-wallets, their software faces a motivated adversarial [1,2,3].

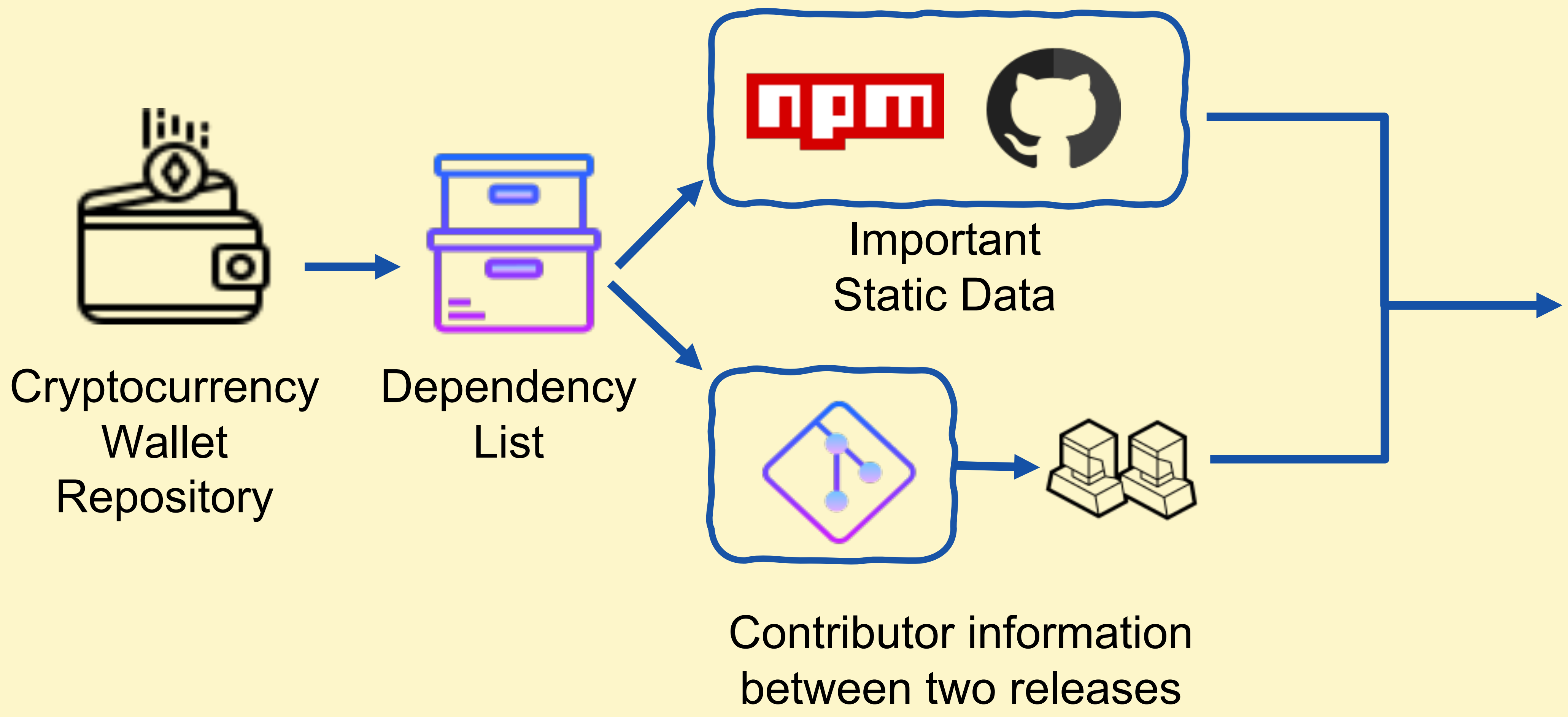
Research on crypto wallets

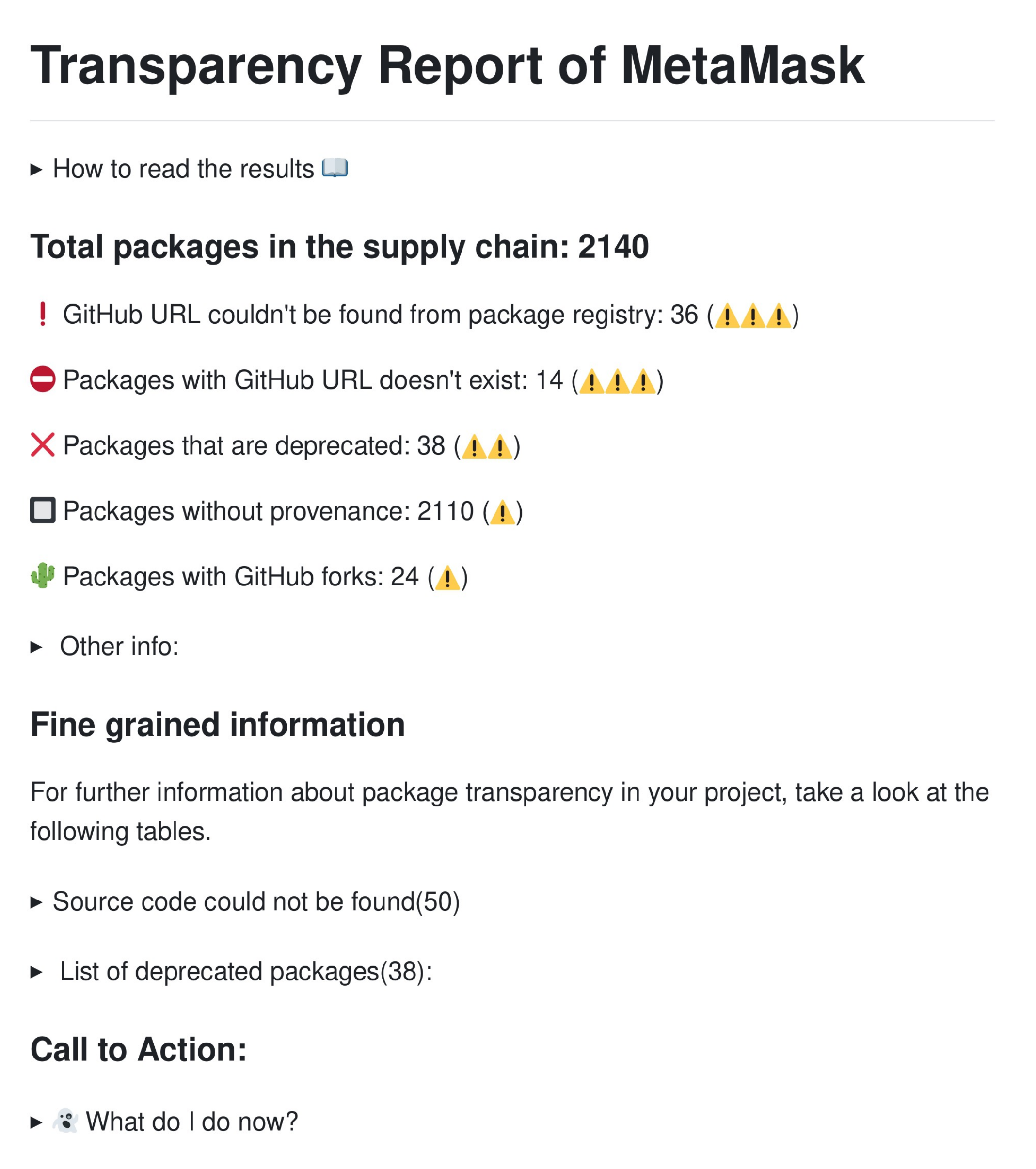
Focuses on exploring general attacks such as network, application, blockchain and authentication threats to wallets[4], **but overlooks at source code provenance and contributors.**

When it comes to the supply chain of your cryptocurrency wallet,
Are you swimming in dirty waters?

Dirty Waters

A tool designed to unveil the transparency status of crypto wallet software dependencies.


Cryptocurrency Wallet Repository
Dependency List
Important Static Data
Contributor information between two releases



Transparency Report of MetaMask

▸ How to read the results 📖

Total packages in the supply chain: 2140

❗ GitHub URL couldn't be found from package registry: 36 (⚠️⚠️⚠️)

⛔ Packages with GitHub URL doesn't exist: 14 (⚠️⚠️⚠️)

❌ Packages that are deprecated: 38 (⚠️⚠️)

□ Packages without provenance: 2110 (⚠️)

🌵 Packages with GitHub forks: 24 (⚠️)

▸ Other info:

Fine grained information

For further information about package transparency in your project, take a look at the following tables.

▸ Source code could not be found(50)

▸ List of deprecated packages(38):

Call to Action:

▸ 👻 What do I do now?

Human-readable report

References:

[1] Tomislav Maljic. Mining for malicious Ruby gems
[2] Ledger. Security Incident Report, December 2023
[3] research!rsc: Timeline of the xz open source attack
[4] Yimika Erinle, Yathin Kethepalli, Yebo Feng, and Jiahua Xu. SoK: Design,Vulnerabilities, and Security Measures of Cryptocurrency Wallets, August 2023. arXiv:2307.12874 [cs].