Walletbeat

In action: Main page

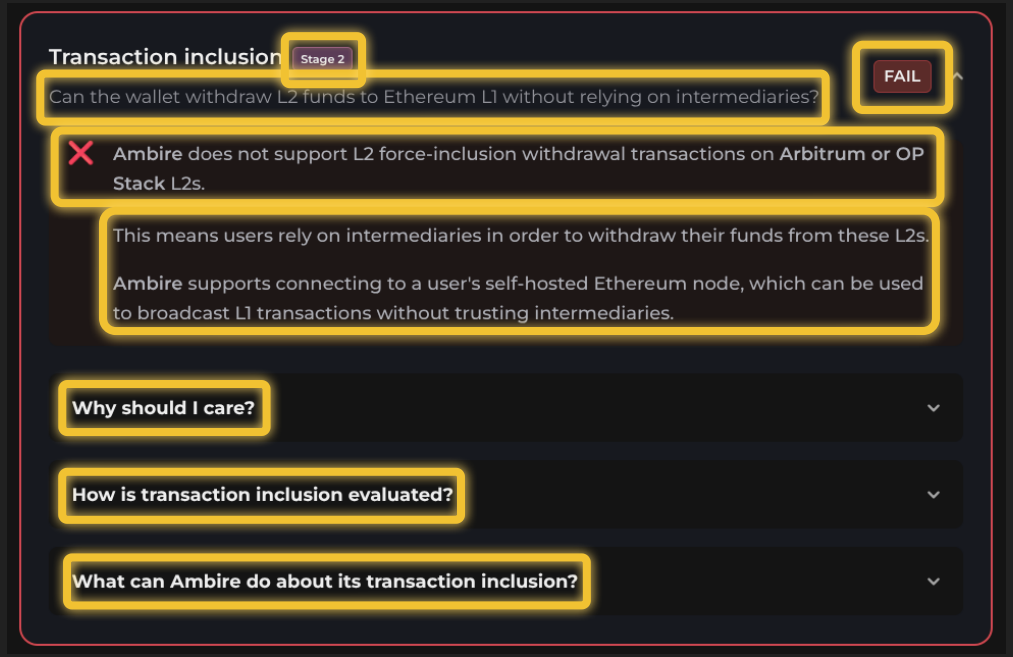
`beta.walletbeat.eth.limo`

In action: Wallet page

`beta.walletbeat.eth.limo/ambire`

In action: Wallet attribute

`beta.walletbeat.eth.limo/ambire`

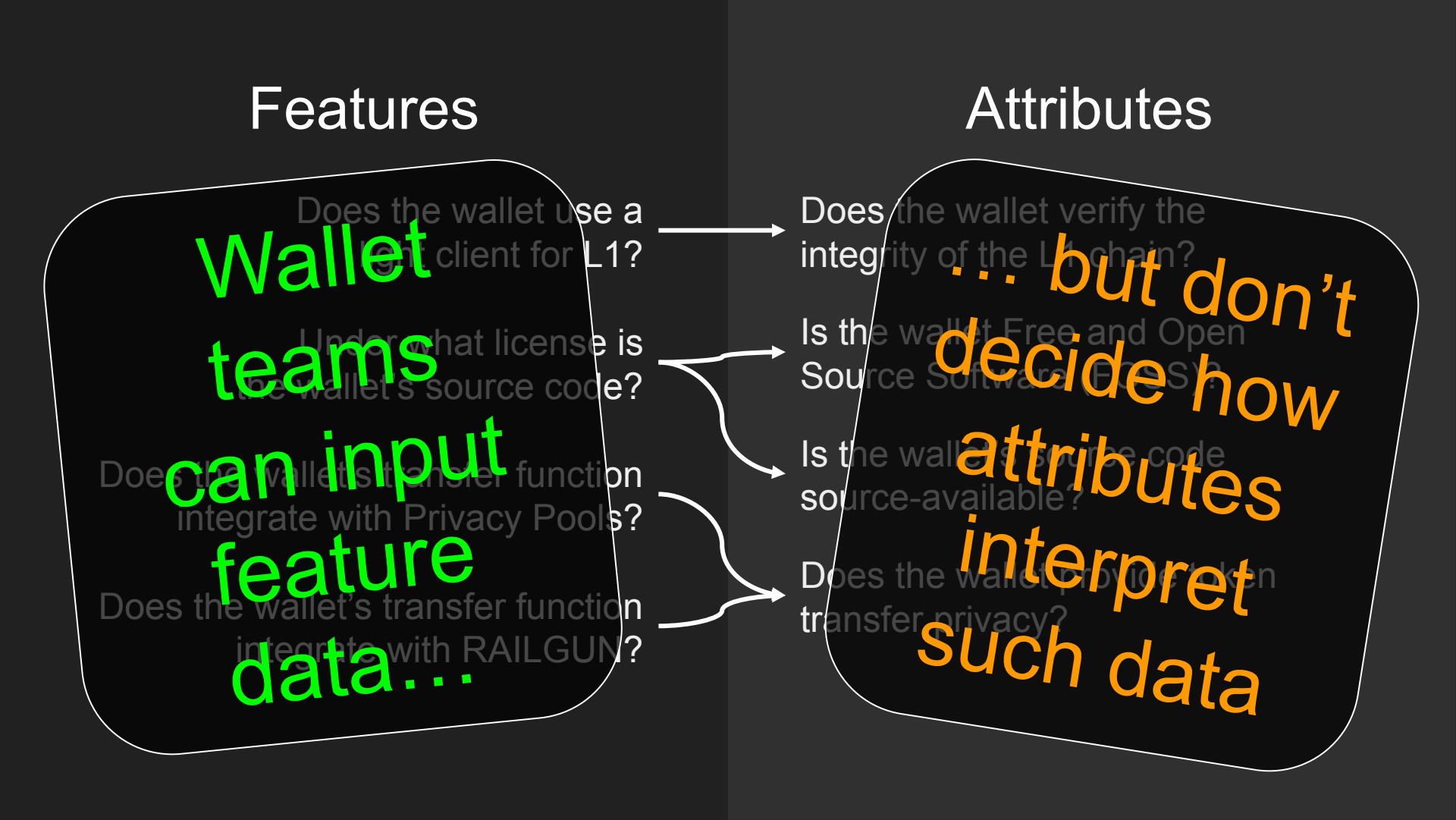


Wallet rating philosophy

- **Align with Ethereum values**:
  - 🔒 Security | 🫆 Privacy | 🏰 Self-sovereignty | 🪟 Transparency | 🐝 Ecosystem
  - Inspiration: V's "*Making Ethereum alignment legible*" & "*What I would like to see in a wallet*"
- **Base all evaluations on verifiable behavior**:
  - Example: Network traffic analysis >> Reading privacy policies
  - *(If it's not verifiable, it violates the Transparency value in the first place)*
- **Don't pick winners**:
  - Rate based on **effective outcome for the user**, not on specific standards
  - Example: **Private transfers**
  - *Important exception:* ***Wallet interoperability standards*** **:)**
- **Limit to what's *technically feasible* in the present**:
  - Can't ask browser extension wallets to do things browser extensions can't do
  - The bar will rise as the tech progresses (Example: light clients for L2s)
- **Put the bar high first**:
  - Easier to adjust downwards later than the other way around

Walletbeat structure in a nutshell

- Wallet **feature**: observable *piece of information* about a wallet
  - “Does it display transaction fees by default?”
  - “What license is the source code under?”
- **Attribute**: Function to evaluate a wallet about a *specific thing*.
  - Input: **features**.
    - Example: The license the source code is under.
  - Output: **rating**. (`PASS`, `PARTIAL`, `FAIL`)
    - Example: If license is FOSS: `PASS`; if not FOSS: `FAIL`.
- Why the decoupling?
  - Allows complex rating logic, eg. Vitalik’s “Walkaway Test”
  - Yet still keeps wallet feature data easy to understand.


Features
Attributes
Does the wallet use a light client for L1?
Under what license is the wallet's source code?
Does the wallet's transfer function integrate with Privacy Pools?
Does the wallet's transfer function integrate with RAILGUN?
Wallet teams can input feature data…
Does the wallet verify the integrity of the L1 chain?
Is the wallet Free and Open Source Software (FOSS)?
Is the wallet's source code source-available?
Does the wallet protect token transfer privacy?
… but don't decide how attributes interpret such data

Walletbeat attributes

Walletbeat attributes: 🔒 Security 1/2

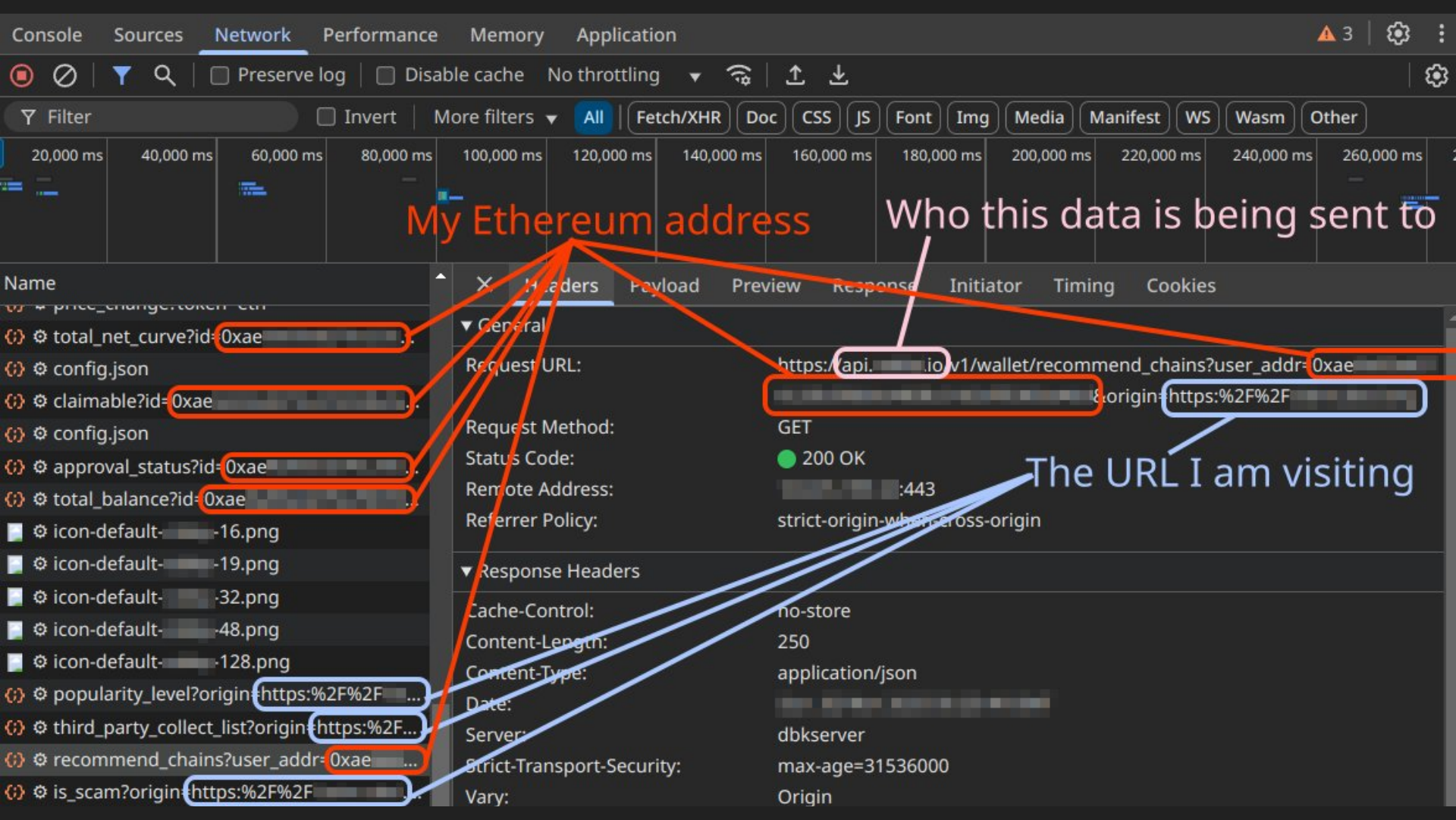
- 🚨 **Scam prevention**: Common privacy-preserving scam checks
  - Examples: Address whitelisting, check against known-scam contract databases...
  - **Why**: Keep users safe.
- ⚓ **Chain verification**: Verify integrity of L1.
  - **Why**: Remove trust dependency on Infura
  - [secondary: enable RPC provider independence]
- 📟 **Hardware wallet support**: Support at least 1 hardware wallet.
  - **Why**: Enables users to airgap their keys.
- 🛟 **Account recovery**: Can you recover your account if you lose one of your devices/seed phrases?
  - **Why**: Prevent lost funds.

Walletbeat attributes: 🔒 Security 2/2

- 🪩 **Transaction simulation** (in a privacy-preserving manner)
  - **Why**: Critical security feature to understand transaction outcome.
- 🔍 **Transaction legibility**: Is it clear what you are signing?
  - **Why**: Bybit hack.
- 🔏 **Security audit**: Independent security audit within the last year
  - **Why**: Delegate the security work to experts whose job is on the line.
- 🐛 **Bug bounty program**: Independent security audit within last year
  - **Why**: Align incentives for exploits to be disclosed rather than exploited.
- Probably more to come; Coinspect partnership TBD.

Walletbeat attributes: 🫆 Privacy

- 📨 **Private transfers**: Are token sends privacy-preserving by default?
  - **Why**: Wallets without private transfers are like browsers without HTTPS.
- 🏝️ **App isolation**: Does the wallet isolate per-dapp addresses by default?
  - **Why**: Address reuse creates a public, indelible dataset for tracking you across time & dapps.
- 🖇️ **Multi-address privacy**: Does any external entity ever learn that 2 of your addresses belong to the same person?
  - **Why**: Defeats the purpose of using separate addresses for privacy.
- 🔗 **Address privacy**: Does any external entity ever learn one of your addresses **+** another piece of personal information about yourself? (including IP)
  - **Why**: Now that entity knows who the address belongs to and can track it across time.
  - And, because, well:


Console
Sources
Network
Performance
Memory
Application
Preserve log
Disable cache
No throttling
Filter
Invert
More filters
All
Fetch/XHR
Doc
CSS
JS
Font
Img
Media
Manifest
WS
Wasm
Other
20,000 ms
40,000 ms
60,000 ms
80,000 ms
100,000 ms
120,000 ms
140,000 ms
160,000 ms
180,000 ms
200,000 ms
220,000 ms
240,000 ms
260,000 ms
My Ethereum address
Who this data is being sent to
Name
total_net_curve?id=0xae
config.json
claimable?id=0xae
config.json
approval_status?id=0xae
total_balance?id=0xae
icon-default-16.png
icon-default-19.png
icon-default-32.png
icon-default-48.png
icon-default-128.png
popularity_level?origin=https:%2F%2F
third_party_collect_list?origin=https:%2F
recommend_chains?user_addr=0xae
is_scam?origin=https:%2F%2F
Headers
Payload
Preview
Response
Initiator
Timing
Cookies
General
Request URL:
https://api. .io/v1/wallet/recommend_chains?user_addr=0xae
&origin=https:%2F%2F
Request Method:
GET
Status Code:
200 OK
Remote Address:
:443
Referrer Policy:
strict-origin-when-cross-origin
The URL I am visiting
Response Headers
Cache-Control:
no-store
Content-Length:
250
Content-Type:
application/json
Date:
Server:
dbkserver
Strict-Transport-Security:
max-age=31536000
Vary:
Origin

Walletbeat attributes: 🏰 Self-sovereignty

- 🏰 **Self-hosted node**: Can you point the L1 RPC provider to your own node?
  - **Why**: Necessary for walkaway test and/or removing trust on RPC provider.
- 🧳 **Account portability**: Does another independent wallet exist that can give you back full control of your account if you import it there?
  - **Why**: Necessary for walkaway test; enforces address derivation standard, smart account lock in risk etc.
- 🪚 **Account unruggability**: Can an external provider unilaterally take over your account?
  - **Why**: Definition of Self-sovereignty. Targets custodial wallets & risky wallet backup structures.
- 📡 **Transaction inclusion**: Can you perform an L2 force-withdrawal transaction on L1 without depending on intermediaries?
  - **Why**: If you can't, you don't have control of your funds. Addresses censorship resistance at both the L2 and L1, since the L1 transaction must also be broadcast with no intermediaries.

Walletbeat attributes: 🪟 Transparency

- 🍝 **Source availability**: Is the wallet's source code public?
  - **Why**: Auditability, build reproducibility.
- 💞️ **Open source**: Is the wallet's source code FOSS-licensed?
  - **Why**: Code reuse, transparency, feasible to transfer maintainership if team walks away.
- 💸 **Fee transparency**: Are fees transparently displayed?
  - **Why**: Transparency on take rates.
- 🗺️ **Orderflow transparency**: Are orderflow handling practices disclosed?
  - **Why**: Similar to TradFi PFOF disclosures. Transparency on take rates.
- 💰 **Funding transparency**: Is it clear how wallet development is funded?
  - **Why**: Transparency on take rates, discourages selling personal data.

Walletbeat attributes: 🐝 Ecosystem

- 💼 **Account Abstraction**: Do you support any form of AA?
  - **Why**: Future-proofing, key rotation, fee sponsorships…
- 🧺 **Transaction batching**: Does the wallet support multiple operations in one transaction approval flow?
  - **Why**: Better UX for token approvals, enables more complex DeFi use-cases.
- 📇 **Address resolution**: Can you send to ENS addresses?
  - **Why**: Make typos less problematic, make Ethereum simpler to use.
- 🌐 **Browser integration**: Does the wallet implement standard browser wallet discovery EIPs?
  - **Why**: Wallet interoperability within apps, competitive wallet ecosystem.
- 🌉 **Chain abstraction**: Is it easy to interact with multiple chains?
  - Cross-chain balances, built-in bridging.
  - **Why**: Smooths over the fragmentation pains of the L2 world.
- 🧩 **HW wallet interop**: Can you use HW wallets from ≥2 manufacturers?
  - **Why**: Wallet interoperability, competitive wallet ecosystem.

[pause for a breather]

That’s a lot.

How to make sense of it all?

The stage system

- Another idea shamelessly stolen from **L2BEAT**.
- ***Cross-cutting*** rating system for wallets.
- **Stage 0**: Table stakes
- **Stage 1**: Significant commitment on all fronts
- **Stage 2**: Full commitment to Ethereum values on all fronts
- **Badges** for significant milestones across each Ethereum value
  - “**Significant investment in security**” badge 🔒
  - “**Privacy is normal**” badge 🫆
  - “**Wartime-ready wallet**” badge 💣
  - “**Built-in-the-open wallet**” badge 🪟
  - “**Fully interoperable**” badge 🌈

Open questions

- What about **hardware wallets**?
- What about **embedded wallets**?
- **Stages** for those?
- How do we **get wallets to care**?
- How do we know how/when to **change the bar**?
- How will governance **avoid capture**?
- **Sustainable funding** for wallet research/updates?

Come contribute!

beta.walletbeat
.eth.limo

github.com/walletbeat

farcaster.xyz/~
/channel/walletbeat

x.com/walletbeat