pomo

One book for pump.fun and fomo.

Two launchpads trade the same coins and keep two separate crowds. Prices and balances are already shared — they're on-chain. What's siloed is the map from a wallet to a named trader. This is a technical account of resolving it.

Version	Date	Network	Live at
1.0	2026-08-19	Solana	pomopad.fun

01 The problem

> A memecoin's holders are one set of people. Every app that surfaces the coin shows you a different fraction of them, and none will tell you the rest.

pump.fun and fomo list overlapping markets. A trader active on both appears as two unrelated accounts, and each platform ranks them on only the slice of their record that happened inside that app. Neither can compute a number covering both, because neither can see the other's identities.

The consequence is not cosmetic. If you are trying to work out whether the wallet accumulating a coin is a known trader or an anonymous sniper, the answer exists but is split across two databases that do not talk.

02 The insight

Almost everything people assume is siloed is already public. Balances, prices, supply and transfers are on-chain: identical whichever app you ask, and readable from a neutral RPC. There is nothing to merge.

Exactly one layer is genuinely siloed — the social one. The map from a wallet to a named trader, and the posts those traders publish. So the entire product reduces to a single job:

The job

Resolve many platform identities onto one canonical wallet, and keep the evidence for why we believe each link.

03 Identity resolution

Conceptually this is union-find with wallets as the join key. If a pump.fun handle and a fomo handle both provably control wallet `W`, they are one person and their profiles merge. Everything the product promises — one holders list, one feed, one leaderboard — falls out of getting this right.

Evidence is stored per source rather than as one verdict per pair. Several independent observations can support the same link, and that is what makes weak evidence safe to keep: it can be recorded, scored and later corroborated without ever being mistaken for proof.

Confidence model

SOURCE	SCORE	MEANING
`wallet_signature`	1.00	Ed25519 signature over a server-issued challenge. Cryptographic.
`oauth_link`	0.95	Authorised account link with the platform.
`public_profile`	0.60	The platform itself publishes the association.
`self_declared`	0.50	The wallet's owner says so. Nothing corroborates it.
`heuristic`	0.30	Behavioural correlation. Never sufficient alone.

Two thresholds do the work. **0.60 is the display floor** — below it a link is stored as evidence but never shown as fact. **0.90 is the merge floor** — only cryptographic or platform-authorised evidence may collapse two profiles into one.

That gap is deliberate. A scraped link is good enough to badge a holder "also on fomo". It is not good enough to merge two strangers, because a merge deletes the losing profile and **is not recoverable by re-running ingestion**. The asymmetry between a cosmetic error and an unrecoverable one sets the bar.

> **Why `self_declared` sits at 0.50**
>
> A trader can tell us their fomo handle; we cannot check it. Scoring the claim below the display floor means it appears on the claimant's own profile, labelled unverified, and nowhere else. Score it at 0.60 and impersonating a well-known handle becomes free.

Custodial guard

A wallet carrying more than 25 high-confidence identities is treated as custodial and never merged. This is not hypothetical: an exchange or router wallet appearing in profile data would otherwise transitively merge every trader who touched it into a single profile — and because merging deletes rows, that corruption survives re-ingestion.

04 Data sourcing

Balances come from a neutral RPC, never from a launchpad. That is what makes the holders list complete regardless of which app a holder uses, and it is why the on-chain layer is deliberately kept outside the platform-adapter interface.

On-chain

Top holders resolve in three RPC calls: largest token accounts, their owning wallets, then what program owns each of those wallets. The third call is the one that matters. A user's wallet is owned by the System Program; a bonding curve, AMM pool or vault is a program-derived account. Without that check, the top "holder" of nearly every launchpad coin is the bonding curve holding most of the supply — the single most misleading row a holders table can have.

pump.fun

Read from their public frontend API. Coin discovery returns the deployer wallet and the display name attached to it in the same payload, which is a `public_profile` link at no extra cost — that is the creator pipeline. A second endpoint supplies follower counts and avatars.

fomo — not ingested

fomo (fomo.family) is **not** scraped, and that is a decision rather than a gap. Three independent signals say programmatic access is not on offer: their API returns a WAF block to non-browser clients on every path; their `robots.txt` disallows `/profile/`, `/user`, `/coin` and `/prices/`; and their sitemap publishes only marketing, with trader data behind a login.

Defeating a bot block means forging browser fingerprints to circumvent an access control the operator configured deliberately. That is a different act from reading an open API, it breaks on their next rule change, and it risks the access that does work. The adapter is written against the same interface and

stays inert behind one environment variable until a sanctioned endpoint exists. Nothing downstream can distinguish "fomo returned nothing" from "fomo isn't enabled".

05 Architecture

The system runs on serverless infrastructure, which rules out holding a websocket open. Live data is therefore a relay rather than a passthrough:

Cron polling is the baseline and needs no extra infrastructure. An optional worker holds the websocket for sub-second latency; both producers are safe to run together because publication dedupes on `(mint, event kind)`. Keying on mint alone would swallow a coin's migration after its creation was broadcast.

Server-sent events rather than websockets, because `EventSource` reconnects on its own — which is exactly what is needed when the function backing the stream ends at its duration ceiling. The client replays a cursor so a reconnect resumes instead of repeating.

LAYER	CHOICE	WHY
Record	Postgres (Neon)	Profile merges need real transactions; a half-applied merge orphans every identity it moved.
Ephemeral	Redis (Upstash, REST)	Nonces, cursors, event buffer, rate limits. Flushable without data loss.
Chain	RPC indexer	Balances, token accounts, program ownership.
Auth	Sign-In With Solana	The only evidence that may merge profiles.

Authentication

Connecting a wallet and proving ownership are different things; only the second is worth anything, since an extension can announce any address. The server composes the full signing message rather than returning a bare nonce — if the client assembled it, a malicious page could show the user different text than what is later verified, and the entire guarantee is that the approved string is the checked string. The message binds domain, address and a single-use nonce spent atomically on verification, so replay is impossible rather than merely unlikely.

06 Current state

Measured on the live deployment. Every figure is ingested or on-chain; none is seeded, sampled or estimated.

6,968 coins tracked	**1,612** traders resolved to a name	**91** with 1,000+ followers	**508.7K** largest account
2,193 platform identities	**4,362** wallets indexed	**6,812** holdings recorded	**$5.5B** market cap tracked

Of 2,193 identity links, 2,182 are `public_profile` and 11 are `wallet_signature`. 271 of the indexed wallets are program-owned — pools and bonding curves, excluded from every holder ranking.

07 Limitations

Stated plainly, because a whitepaper that omits them is marketing.

- **No profit and loss.** Neither platform publishes it, so the leaderboard ranks on follower count. Real realised PnL is computable from transaction history and is the obvious next piece of work — it is also the one number neither platform can produce across both books.
- **fomo is not ingested.** Cross-listing counts therefore read zero. The mechanism is built and dormant; the blocker is permission, not code.
- **Thesis ingestion is limited.** pump.fun's replies have no stable public route at present, so the merged feed carries only posts published natively.
- **Holder lists are top-N snapshots**, refreshed on a staleness gate rather than streamed. Balances move faster than the refresh interval.

08 Position

The defensible asset is not the data — most of it is public to anyone who asks the right endpoint. It is **the resolved identity graph and the evidence behind it**: a per-source, per-link record that can be re-scored, corroborated or revoked without rebuilding, and that gets strictly more valuable as sources are added.

That is also why the confidence model is the centre of this document rather than an appendix. Any team can scrape two APIs. The difficulty is knowing which links you are entitled to believe, and being able to show your work when someone asks why two accounts are the same person.

---

pomo · pomopad.fun · Solana · Figures measured 2026-08-19 on the live deployment. Aggregated data is attributed to its source. Not financial advice.