

# Other World Projex Whitepaper

Sep 29, 2026 · @OWProjex

This is a living document. It will be revised as the project changes, and every material revision will be logged at the end rather than silently edited away.

## Executive summary

Other World Projex (OWP) is a Solana-based project built by Other World Asset Company around \$RIBBIT, a fixed-supply, 35%-burned Token-2022 asset; a suite of in-house, tiered-risk on-chain tools; a liquidity-provision operation moving toward transparent, backtested community intelligence; and the Otherworld Reserve, a real-asset rewards vault with an honest, database-first custody model. The project is small and deliberately so: roughly 200 community members and 400 legitimate holders, run by a small executive team and a volunteer moderator group.

OWP has also made real mistakes — a careless liquidity-pool configuration, a phishing incident, and a September 2026 platform compromise — documented in full in this whitepaper rather than omitted. Its guiding design principle, adopted directly because of those mistakes, is architectural rather than aspirational: no single key or account should ever hold more than one narrow privilege, users sign their own transactions and OWP never custodies a private key on their behalf, and irreversible actions are deliberately the last thing built, not the first.

## Origins and philosophy

OWP was started by people frustrated with a corner of crypto where projects hide their mistakes, custody funds nobody asked them to hold, and market outcomes to their community as guarantees. The founding thesis was that a project could instead prove itself by how it operates — open about failure, conservative about custody, and slow about anything irreversible — rather than by marketing claims alone.

That thesis was tested early and expensively, by the project's own hand. A liquidity-pool misconfiguration and a phishing incident (§ Security incident history) cost the team real money before the community had grown large enough to be exposed to the same risk. Roughly 90% of the capital at risk in the project's early mistakes belonged to the founding team, not the community. That is not offered as an excuse for the mistakes; it is offered as the reason the community members who were present for them are, today, among the project's most committed holders — they watched the team absorb the cost and make affected people whole, rather than the reverse.

\$RIBBIT was deliberately kept a microcap: cheap enough to join without meaningful financial risk, and small enough that the team's own incentives stay aligned with a broad, engaged base rather than a handful of large holders. Every product decision documented in this whitepaper is meant to be read against that origin: this project has already been careless once, been attacked once, and has since tried to build the kind of structural caution that doesn't rely on nobody ever making a mistake again.

## Token specification: \$RIBBIT

| Field                     | Value                                                                                              |
|---------------------------|----------------------------------------------------------------------------------------------------|
| Standard                  | SPL Token-2022                                                                                     |
| Mint address              | EVHtwfyWoHmUM5RHi3td31sNKCC8f83XKT44ZDqn pump                                                      |
| Metadata storage          | Native Token-2022 metadata extension (on the mint account itself, not a separate Metaplex account) |
| Mint authority            | Revoked (null) — supply is permanently fixed, no further tokens can ever be minted                 |
| Freeze authority          | Revoked (null) — no token account can ever be frozen                                               |
| Metadata update authority | Revoked (null) — name, symbol, and image are permanently immutable on-chain                        |
| Supply permanently burned | ~35% of total supply                                                                               |

All three authorities being independently revoked and verifiable on-chain means no party — including the OWP team — can mint additional supply, freeze a holder's tokens, or alter the token's on-chain identity. That immutability held through the September 2026 compromise (§ Security incident history): even with administrative and treasury access, the attacker could not touch the mint itself.

One consequence of permanent metadata immutability: a planned rename from \$RIBBIT to a new ticker (OWX) cannot be applied to this mint at all — there is no transaction that could change it, and no key that could sign one. That rename is accordingly on hold pending a full migration to a new mint rather than a cosmetic update (§ Roadmap summary).

## Security incident history

This section is the technical record. A narrative version, written for a general audience, is published as a companion article; nothing here contradicts it, and this version carries more detail for anyone who wants it.

### Incident 1 — liquidity pool misconfiguration (early)

OWP created and locked a liquidity pool for \$RIBBIT itself. Locking was correct — it removed the team's own ability to pull liquidity out from under holders — but the pool's own parameters were set carelessly, and that error, not any external action, caused an early price decline. The record is on-chain and independently verifiable.

### Incident 2 — burn-tool phishing (later, after partial recovery)

While attempting to burn a large portion of token supply, the team navigated to what was believed to be the legitimate burn tool through a link surfaced inside Phantom wallet's built-in explorer. The page

was a pixel-identical clone of the real tool, and the interaction that followed was a phishing loss, not a burn-tool bug. This incident, together with Incident 3, is the direct motivation for the in-house Tools Suite (§ Product: the Solana Tools Suite) and for treating lookalike-site risk as a first-class design constraint across every product OWP has built since.

### **Incident 3 — platform compromise, 24–27 September 2026**

**Mechanism.** An actor with access to the project's hosting platform added a wallet under their control to the application's administrator allowlist on 24 September. Using that access, they reduced the in-house casino games' burn share from 50% to 5% and raised the maximum wager roughly a thousandfold, redirecting the large majority of purchase flow to the treasury wallet instead of the burn address. Two days later, on 26–27 September, the same operation: drained the treasury wallet across three separate on-chain swaps (roughly 31,350 \$RIBBIT sold for a combined ~0.038 SOL); emptied a separate operational wallet of approximately 10 SOL through address-poisoning-style transfers; fabricated roughly 5,000,000 in-game credits across two privileged accounts; and altered prize-eligibility parameters.

**Root cause.** A single wallet held both treasury-signing authority and administrative authority simultaneously. Compromising one function compromised both. This is the architectural lesson OWP treats as central, and it is the reason every system built since separates signing authority from administrative authority, and separates every privileged role from every other one, by design (§ Security architecture).

**Data exposure, quantified rather than assumed.** A full database export was reviewed row by row against an earlier, less careful public statement, which this document corrects: 232 email addresses (231 waitlist sign-ups, 1 tournament sign-up); wallet addresses and gameplay history tied to 8 registered accounts; zero postal addresses (none were ever collected); zero passwords (the platform authenticates by wallet signature only, and stores no password of any kind).

**Fairness integrity.** All provably-fair server seeds were, for the exposure window, readable by the same access. Every seed was rotated and publicly revealed immediately on discovery, which allows any player to independently verify the fairness of rounds already played. One affected community member, whose results could not be certified in either direction because of the exposure, was identified, contacted directly, and compensated beyond the value in question.

**Remediation.** Data was recovered via a temporary export mechanism (since deleted) because the production database platform itself was never under OWP's direct administrative control; a clean database was stood up from the project's own migration history and verified row-for-row and table-for-table against the export; every credential connected to the incident was rotated; the compromised administrative access was revoked; and the site was verified live on the clean database within the same day the compromise was discovered.

### **Related item — former-developer code exposure**

A former developer maintains a public copy of an earlier version of the codebase on a personal account, unrelated to Incident 3. A full history audit of that public repository found no credentials, API keys, database URLs, or private key material anywhere in it. OWP's working assumption is that this code is permanently public and irrecoverable, and that security must therefore rest on access control and

credential rotation, never on source code staying secret — which is the same principle the rest of this document applies throughout.

## Security architecture

Every product OWP has shipped since its early incidents follows the same set of rules, applied without exception:

1. **The user signs; OWP never holds a key.** No server-side signing, no custodial convenience, no exceptions for any tool at any tier.
2. **No single key or account holds more than one privileged role.** The root cause of the September 2026 compromise was one wallet serving as both treasury signer and administrator. Every system built since assigns a freshly generated, narrowly scoped key to each distinct privileged function, so that a single leak has a contained, predictable blast radius rather than a compounding one.
3. **Simulate before signing.** Every transaction a tool builds is simulated against the live chain first, and the user is shown the simulation's actual result — not a description of it — before a sign button becomes available.
4. **Risk-tiered build order.** Tools and features are classified by what a bug in them could cost — nothing, recoverable-to-the-signer-only, recoverable-but-real-value, or irreversible — and are built in that order, so the pattern is proven on low-stakes tools before it's trusted with high-stakes ones. Irreversible actions require a confirmation flow that states plainly, in advance, what becomes permanently impossible.
5. **Integer money, always.** Token amounts and balances are handled as exact integers throughout, never floating-point, to remove an entire class of rounding and precision bugs from anything that moves value.
6. **Read the account before acting on it.** No instruction is built from a form value alone; the actual on-chain state is fetched and confirmed immediately before use, since state can change between when a user loads a page and when they sign.

These are treated as invariants, not aspirations: they constrain what gets built, and in at least one documented case (§ Product: the Solana Tools Suite, Tier 4) they mean a feature is deliberately not shipped yet, even though it is technically straightforward, because its confirmation flow isn't ready.

## Product: the Solana Tools Suite

Live at the Tools page on our main site. Built in-house, on our own domain, specifically so community members never have to search for a third-party wallet-hygiene tool and risk landing on a clone — the exact mechanism behind Security Incident 2.

| Tier | Tools                                                                       | Status | What a bug can cost                           |
|------|-----------------------------------------------------------------------------|--------|-----------------------------------------------|
| 1    | Epoch countdown, read-only wallet inspector, read-only stake-account reader | Live   | Nothing — no connection or signature involved |

| Tier | Tools                                                                                       | Status                                | What a bug can cost                                 |
|------|---------------------------------------------------------------------------------------------|---------------------------------------|-----------------------------------------------------|
| 2    | Revoke Approvals, Rent Reclaim                                                              | Live                                  | Limited to the signer's own wallet, and recoverable |
| 3    | Stake merge/split, partial withdrawal, token metadata update                                | Reader live; acting tools in progress | Moves real value, but recoverable                   |
| 4    | Revoke mint authority, revoke freeze authority, make token immutable, create/lock liquidity | Deliberately not built yet            | Irreversible — no recovery path exists once run     |

The page itself carries anti-clone measures: it states its own canonical URL in full, commits to never sending that link over direct message, and compares the browser's address bar against the URL baked into the build at compile time, surfacing a warning when they disagree. This catches a straightforward scrape-and-clone; it does not catch a clone rebuilt from source with its own URL substituted, which is a known limitation stated on the page itself rather than left implicit.

Every tool in every tier follows the security architecture above without exception: the user signs, nothing is simulated-and-hidden, and Tier 4 will not ship until it has a confirmation flow that resists being clicked through by someone in a hurry — the same state the team itself was in during Security Incident 2.

## Product: LP management, intelligence, and community signal-following

OWP operates its own liquidity-provision book across Solana venues (currently Meteora DLMM and PumpSwap), monitored through an in-house dashboard secured with password and two-factor authentication, hosted read-only on dedicated infrastructure rather than personal hardware. The dashboard surfaces position health scoring, wallet-reputation signals, and market scanning — all advisory, none of it executing a trade on its own.

**Capital discipline.** No automated strategy is given meaningful capital until it has been backtested against real historical on-chain data and shown to be net-positive after costs. Execution, where it exists at all, sits behind hard position and loss limits and a kill switch a human can flip instantly — the same tiered-risk logic applied throughout this whitepaper, applied here to trading specifically.

**The community signal-following model (designed, not yet released).** OWP intends to make a version of this intelligence — wallet reputation, pool health, market scanning — available to the wider community, gated by \$RIBBIT holdings. The non-negotiable design constraint is stated here in full because it is the load-bearing legal and security fact of the whole feature: **OWP's service would be a signal source, and never an execution service, for anyone else's funds.** No community member's private key would ever reach OWP's infrastructure; a member who opts in runs a local client on their own machine, holding their own key, applying their own risk parameters to signals published in relative (percentage-of-portfolio) terms rather than absolute dollar amounts. This is not released to anyone outside the

founding team today, and will not be, until it has had a real legal review of the questions it raises around publishing information that others may act on financially.

## **Product: the Otherworld Reserve**

The Otherworld Reserve is a holding of real, physical assets — bullion coins and rounds initially — bought and custodied by the project, awarded through bounties and puzzles, and available for direct acquisition.

**Custody model.** The project's own append-only ledger is the sole authoritative record of who holds a claim to each item; a mirrored NFT, where one exists, is a public, tradeable view of that ledger record and never a substitute for it. This was a deliberate design choice: an NFT cannot itself be legal or practical title to a physical object in a vault, and building the relationship the other way around — as many "redeemable NFT" projects do — creates ambiguity about who the custodian actually owes the object to.

**Pricing.** Bullion is priced from a live spot feed plus a fixed premium (higher for professionally graded pieces than for ungraded), with a checkout price that refuses to quote against stale spot data and holds briefly before re-pricing.

**Trade-in.** \$RIBBIT can be exchanged for Reserve credit at fixed denominations. To prevent a short-lived price spike from being converted into underpriced silver, the exchange rate uses the lower of a live price and a 30-minute time-weighted average, with a circuit breaker if the two diverge sharply, a bounded quote lifetime, and daily caps per wallet and platform-wide.

**Marketplace.** A holder may request physical delivery or list their claim for resale to another member; resale carries a modest, published commission taken from the seller.

**Compliance.** Shipping and sales are blocked to jurisdictions under comprehensive U.S. sanctions, with additional conservative blocks reviewed against current guidance, and screened at account, checkout, and shipping-address level.

## **Governance, compliance, and legal posture**

OWP has drawn an explicit internal line, stated in its own codebase, that governs every benefit ever offered to a holder or staker: a benefit may be access, a fee discount on a member's own transaction, or a status mark — and never a payout, a credit grant funded by house revenue, or better odds in a game of chance. Anything that would cross that line is required to clear legal counsel before it ships, not after.

This line is not theoretical; it actively gates real, designed features today:

- An in-house staking platform has been designed (an ICP-based canister holding custody without any person controlling the underlying keys), but its proposed reward structure is paused pending counsel's review, precisely because paying stakers from project revenue is the pattern securities analysis focuses on.
- An automatic transfer-fee-distribution-to-holders feature, built into the token-creation tooling used for any future mint, ships **disabled by default** and requires a named individual's documented sign-off before it can be enabled — a code-level gate, not just a policy statement.

- A planned DAO commitment mechanism will collect non-custodial pledges rather than deposited funds unless and until custody questions are separately resolved with counsel.
- Physical coin sales are planned through a separate legal entity, using payment processing that requires its own business-category approval given restrictions on precious-metals and currency-adjacent sales; approval will be secured before launch, not assumed.
- Sanctioned-jurisdiction screening (§ Product: the Otherworld Reserve) is applied at every relevant transaction point, reviewed against current guidance rather than fixed once.

OWP is not a registered investment adviser, broker-dealer, or money-services business, and nothing in this whitepaper is an offer to sell securities, an invitation to invest, or investment, legal, or tax advice. Where a feature's legal status is unresolved, that is stated plainly in this document and in the roadmap rather than implied to be settled.

## Community tiers and benefits

Membership tier is derived live from a wallet's currently staked \$RIBBIT — there is no separate enrollment step and no snapshot date; unstaking drops the tier on the next check.

| Tier    | Staked \$RIBBIT | Benefit                                                                     |
|---------|-----------------|-----------------------------------------------------------------------------|
| (none)  | Below 250,000   | Standard commission on the member's own Reserve sales                       |
| Keeper  | 250,000+        | Reduced commission on the member's own Reserve sales                        |
| Curator | 1,000,000+      | Further reduced commission; proposed gate for LP-dashboard community access |
| Warden  | 5,000,000+      | Lowest commission tier; proposed gate for OWP-funded AI/advisory features   |

Every benefit at every tier is access or a fee discount on the member's own activity — never a payout, a credit grant, or improved odds — consistent with the governance line above. Thresholds and exact commission figures are tunable by the team without a code deployment and may be adjusted; this table reflects the values in effect as of the date of this document.

## Roadmap summary

A full, visual, status-tagged roadmap is maintained as a companion document: [Other World Projex Roadmap](#). In brief, by phase:

1. **Security & tools** — Tiers 1–2 live; Tier 3 in progress; Tier 4 deliberately delayed.
2. **LP infrastructure & intelligence** — dashboard and monitoring live and advisory-only; automated execution gated behind backtesting.
3. **Otherworld Reserve** — live: listing, redemption, resale, trade-in.

4. **Community access** — membership tiers live; community rigs, wallet-health tools, and signal-following designed and planned, the last pending legal review.
5. **Main site expansion** — airdrop tooling, in-house staking (pending legal review), a full money-path security audit, physical coin sales, and a DAO commitment pool, all planned.
6. **Multi-chain & migration** — an ICP multi-dex integration under review, and the \$RIBBIT → OWX migration on hold pending token unlocks, to be executed as a full new-mint migration rather than a cosmetic rename.

The roadmap document is updated as items ship; this whitepaper's changelog (§ Living document notice) records when a roadmap change is significant enough to also revise this section.

## Risk disclosures

\$RIBBIT is a volatile, microcap digital asset. Its price can fall to zero, and it can be highly illiquid at times. Past burns, past recoveries, and past incident remediation are historical facts, not indicators of future price or project performance.

This document is not financial, legal, or tax advice, and nothing in it should be read as a recommendation to acquire, hold, or dispose of \$RIBBIT or any related asset. Prospective holders should independently verify the on-chain facts stated here and consult their own professional advisors before making any financial decision.

OWP has been compromised once (§ Security incident history) and has made unforced configuration and operational-security errors twice before that. The architectural changes described in this document (§ Security architecture) are designed to reduce the likelihood and blast radius of a future incident; they do not eliminate the possibility of one. No software system, custody design, or organization can guarantee against every future compromise, and this document does not claim otherwise.

Features described as "planned" or "pending legal review" in this document and in the companion roadmap are not committed, may be delayed, may be materially changed by legal review, or may not ship at all.

## Living document notice

This whitepaper is maintained as a living document rather than a fixed snapshot. Material changes — a new product, a resolved legal review, a changed tokenomic parameter, a new incident — will be reflected here and logged below, newest first. Wording or formatting corrections that don't change a fact are not logged.

| Date       | Change               |
|------------|----------------------|
| 2026-09-29 | Initial publication. |

A companion, general-audience article covering this same history is published as [Other World Projex: The Full Story](#).