

IUNUA / PROJECT FOUNDATIONS

IUNUA Whitepaper

Version 0.6 - Project Draft - 10 September 2026

World-authenticated payments, an XMR treasury and verifiable IUNUA records.

IUNUA combines an available wallet app with a proposed trust-currency system. This whitepaper describes the project's purpose, current implementation, private accounting design, eligibility, optional public settlement, economics, privacy and governance. It distinguishes dated evidence from capabilities that remain planned or locked. Practical launch budgeting and operating guidance are provided in the separate System & Launch Guide. The 10 September revision specifies the intended World-authenticated XMR treasury payment and Solana audit receipt, with explicit verification, privacy and recovery boundaries. It also records native Apple wallet source for iPhone Swap, public-address QR scan and on-device IUNUA service records with a separate value rail. Those client surfaces do not enable production fills.

Target design: World App sign-in, explicitly authorized XMR payments, IUNUA verification and Solana audit receipts. Wallet apps exist, but this complete production flow remains unimplemented. XMR redemption rights for IUNUA tokens are undecided.

[Read the matching website edition](#)

The project's technical foundation

This paper explains the project and its evidence. The separate System & Launch Guide provides practical capability explanations, launch cost estimates, preparation steps and post-launch repair options.

In this paper

- 01 Purpose: recognize useful contributions
- 02 Current implementation: wallet apps and network support
- 03 Intended architecture: identity, treasury, verification and receipts
- 04 Connect with World: a human check and an account are different
- 05 The first complete transaction: sign in, pay, verify, record
- 06 What an on-chain receipt can prove
- 07 The XMR treasury: control, accounting and recovery
- 08 The token today: a public Devnet record
- 09 Economics: test issuance is not tokenomics
- 10 Privacy and security: who can see what
- 11 Readiness gates for the full trust service
- 12 Release evidence: identify the exact files
- 13 Glossary: the words behind the idea
- 14 References and evidence dates

01 / IUNUA WHITEPAPER

Purpose: recognize useful contributions

Sign in, authorize a payment from an XMR treasury, verify its outcome and keep an auditable IUNUA record.

IUNUA is intended to coordinate authenticated payments and accountable records. The first end-to-end target is an IUNUA Wallet user signed in through World App, an explicitly authorized XMR payment from a Monero treasury, verification by IUNUA, and a public audit receipt on Solana. This is a target architecture, not an implemented production service. Wallet apps now expose a test composition of that design: IUNUA records the named service, and a selected rail may move value. The wider trust-currency purpose remains recognizing useful contributions under reviewable rules.

Imagine a community paying for maintenance of a shared solar installation. An authorized operator signs in, reviews an invoice and approves its recipient, XMR amount and fee. The treasury signer applies the spending policy and sends XMR. IUNUA checks payment evidence and confirmations, records the result privately, and publishes a receipt commitment on Solana. A permitted reviewer can compare the receipt with the evidence. The example creates no reward rate, treasury funding claim or token-holder entitlement.



Concept illustration: adults working together. This is an example of the intended purpose, not evidence of a live reward program.

What the example does not establish

Software cannot decide by itself whether work was honest, valuable or fairly rewarded. A production system needs credible event sources, eligibility rules, dispute handling and accountable operators. A digital signature can authenticate an approved message; it cannot make a false claim true. The solar example and the demonstration rewards are illustrative, not a commitment to a particular reward rate.

This revision is for adult beginners, contributors and developers. It separates the dated Devnet token evidence, reviewed wallet packages, later native Apple source for iPhone Swap, public-address QR scan and agreement receipts, and the planned authenticated treasury-payment service. An IUNUA token balance is not an XMR balance or a claim on treasury assets.

Sources: [IUNUA intended architecture](#); [IUNUA Trust Lab](#)

02 / IUNUA WHITEPAPER

Current implementation: wallet apps and network support

Wallet apps are available. The current IUNUA token runs on Solana Devnet; the full trust system is not yet a production service.

Implementation evidence remains dated: wallet package review 8 September 2026 and World website preparation/configuration review 9 September 2026. Native Apple wallet source reviewed 10 September 2026 adds iPhone navigation, a public-address QR scanner, locked Swap estimates and on-device agreement composition. Those source changes do not silently upgrade the published 0.8.4 archives. The complete World-authenticated XMR treasury payment with IUNUA verification and a Solana receipt is Planned. This document revision does not add production signing, deploy a receipt program, fund a treasury or establish an end-to-end production payment test.

The wallet is installed software with implemented account and asset features. It is distinct from the website simulation, which uses modeled balances. The current network restrictions describe which actions the wallet can execute; they do not mean the whole application is imaginary or that every displayed asset is a test asset. Public holdings and market estimates are read-only where indicated.

How to read status labels

Label	Meaning
Available	Present in the reviewed release; network access, fees or ordinary account setup may still be needed.
Requires setup	Depends on configured services, credentials or funded test accounts; not certified live on every network.
Simulation	Uses modeled records or demonstration units, separate from chain balances.
Planned	Unfinished capability or target design.
Locked	Intentionally disabled; a visible screen or estimate does not enable execution.

Native macOS and Electron: reviewed 8 September 2026

Capability	Native macOS 0.8.4	Electron 0.8.4
Solana Devnet balances and transfers	Available: Keychain-backed test wallet.	Available: reviewed transfers and account-bound receipts.
Assets and named accounts	Available: Solana accounts and public holdings.	Available: accounts and holdings across supported test networks.

Native macOS and Electron: reviewed 8 September 2026		
Capability	Native macOS 0.8.4	Electron 0.8.4
Existing test key imports	Planned: no equivalent Electron import workflow.	Available: network-specific imports; no shared universal seed.
Monero Stagenet	Planned: limited native interface.	Requires setup: node and wallet RPC.
World Chain Sepolia	Planned: no equivalent creation/signing flow.	Requires setup: test account and TEST ETH; TEST WLD unverified.
RENDER public holdings	Planned: guidance only.	Available: read-only address lookup.
Market estimates	Available: informational estimates.	Available: informational estimates.
Executable swaps	Locked.	Locked: no approved executable route.
World ID eligibility	Requires setup: staging guidance; production verification unfinished.	Requires setup: staging/backend configuration; production verification unfinished.
Private trust loop and Pantheon	Simulation.	Simulation.
Complete game payments	Planned.	Planned.
Production signing	Locked.	Locked.

This matrix summarizes package/source review, not a new end-to-end network certification. A Solana account, a Monero wallet and an EVM account are different custody systems. Import and recovery support must be checked for the particular client and network. Do not assume that one phrase or backup restores every account.

Release and installation boundaries

Both macOS clients are version 0.8.4, but they are different applications. The reviewed Electron release is Developer ID signed, has a stapled notarization ticket and passed Gatekeeper. The native release is Apple Development signed, passes signature verification, and was rejected by Gatekeeper; it is a development distribution. These signing results identify distribution checks, not a financial or protocol security audit.

The iOS download is source version 0.8.4 requiring Xcode and the user's own signing. The browser extension remains version 0.7.0 and requires manual developer installation. The testnet setup kit is version 0.8.4. Exact archive identities are recorded in the whitepaper's release appendix and the linked release manifest; later source changes do not silently upgrade those files.

Native Apple iPhone source, 10 September 2026

The native Apple app is one target for Mac and iPhone. The 10 September source is a later client revision than the reviewed 0.8.4 packages. It does not enable production signing, a Jupiter fill, a hosted fiat partner, an XMR venue or an on-device Monero spend secret.

Native Apple wallet source: reviewed 10 September 2026		
Capability	iPhone	Mac
Primary navigation	Available: Wallet, Assets, Scan, Swap and More. Scan is the middle tab. Wallet Lab and Agreements live under More.	Available: sidebar keeps Wallet Lab, Agreements and Swap first-class.
Receive address	Available: generated QR and share of the public Devnet address only.	Available: generated QR and share of the public Devnet address only.
Scan a recipient	Available: camera scan of a public Solana or Monero address. Wrong-network QRs are rejected. A Monero QR is never written to an IUNUA public receipt.	Locked: paste only. No camera in this source.
Solana Devnet IUNUA-T send	Available: Keychain test wallet; two-phone send with a scanned or pasted address.	Available: Keychain test wallet.
Swap estimates	Available: informational XMR, SOL, IUNUA, EUR and USD. IUNUA has no represented market price.	Available: the same informational estimates.
Executable swaps	Locked: no Jupiter fill, hosted fiat checkout or XMR venue.	Locked: no approved executable route.
Agreement composition	Available: on-device receipt with purpose, amount, optional fee note and settlement asset. Optional Devnet IUNUA-T public ref.	Available: the same composition from the sidebar.
Stagenet XMR value rail	Requires setup: iPhone is a wallet-rpc client. Spend keys stay on the RPC host. The app does not spawn monerod.	Requires setup: owner-started Stagenet daemon 38081 and wallet RPC 38083.
Production signing	Locked.	Locked.

Separate systems, separate limits

The website Trust Lab has seven simulated steps: create an alias, model eligibility, receive a reward, transfer, choose a settlement path, manage disclosure and model an upgrade. Its balances and receipts are local demonstration data. Progress survives internal navigation for the current session and resets on reload or explicit reset. The setup guide stores safe local preferences; it is not proof that the required services were installed or are healthy.

The local Game API, MCP bridge and Electron Wallet Lab now share one file-backed private ledger in the loopback runtime. That ledger is still a simulated local authority: it is not a production wallet, does not hold a private key and does not post a chain transaction. Apple, iOS and browser-extension demo stores

remain separate. Newer game-link code in a checkout is not evidence that a downloadable wallet can approve and settle complete game payments.

Electron offers an optional contained local Solana validator workflow requiring Docker and explicit setup. A local node does not join mainnet automatically. Monero Stagenet is the intended treasury test rail: an authorized Stagenet send is the private-value movement, and IUNUA records the authorized debit on its private ledger and, when visibility is public, may send a separate Devnet IUNUA-T public reference. That record is not a public IUNUA mint, not a wrapped-XMR program and not a substitute for a later, separately previewed production receipt. World ID is an eligibility-proof reference, distinct from the World Chain network. RENDER holdings do not provide Render compute jobs, node operation, billing or token transfers. Estimates for established assets are informational; IUNUA has no represented market price.

Sources: [IUNUA token and wallet capability status](#); [IUNUA release manifest](#); [IUNUA downloads and installation evidence](#); [IUNUA developer integration guide](#); [IUNUA Trust Lab](#); [World ID documentation: overview](#)

03 / IUNUA WHITEPAPER

Intended architecture: identity, treasury, verification and receipts

World authenticates; Monero settles XMR; IUNUA checks and records; Solana anchors the audit receipt.

Four responsibilities in the proposed system

World / identity	World App wallet-account authentication establishes the application session. World ID is a separate human-credential check where policy requires it.
Monero / funds	XMR is the intended principal treasury asset and payment asset for the initial reference flow. Monero establishes the actual payment state.
IUNUA / controls	A policy-controlled signer authorizes spending. Services verify payment evidence and maintain a private, durable accounting and audit record.
Solana / public receipt	A finalized receipt transaction anchors a commitment and verifier attestation. This records evidence about a payment; it does not move the XMR.

Planned architecture. The World network, Monero network and Solana network do not form one atomic transaction. No deployed bridge or cross-chain proof verifier is established here.

Private accounting and network truth

The private ledger records approved instructions, reservations, fees, receipts and adjustments. It must reconcile with the actual Monero wallet and chain. A database credit does not create spendable XMR, and a ledger state cannot override a failed or unconfirmed network payment. Private database updates can be atomic internally; World authentication, Monero settlement and Solana publication cannot be made atomic by a database transaction.

Authentication, eligibility and spending authority are separate. A World account session identifies an authenticated participant. A human credential, a skill credential, an invoice and evidence that work occurred answer different questions. Each must have a defined purpose, issuer, expiry and policy. An authenticated user receives only the treasury roles explicitly assigned to that account.

Mandatory receipt for the first audited-payment product

For the proposed audited treasury-payment flow, receipt publication is a required completion step disclosed before approval. The amount of information disclosed is minimized by policy. Other future private-ledger activities may have different publication rules; the earlier general idea of optional public settlement must not hide a missing receipt for a payment sold as audited. A Monero payment can be confirmed while its Solana receipt is still pending.

Governance and extensions

Pantheon remains the planned framework for changing spending policy, signer membership, verifier authority and disclosure rules. Proposals, review periods, emergency pauses and controlled activation need an adopted policy. An identity-provider outage may pause new ordinary payment requests; any emergency treasury path must use separate, disclosed authorization and leave an audit record.

The ordinary IUNUA Solana token, the XMR treasury and the receipt mechanism are separate components. Token issuance alone creates neither treasury custody nor payment verification. A receipt can be anchored without transferring an IUNUA token. Any later token utility, redemption, bridge or autonomous on-chain verification requires an additional specification and implementation.

Service record and value rail

IUNUA is a Token-2022 token on Solana. It is not a chain that hosts Monero as contract code. The wallet's test composition records a named service (purpose, amount, optional fee note and settlement asset) on the device and, when visibility is public, may send a Devnet IUNUA-T public reference. The selected value rail is separate: Stagenet XMR through owner-started wallet RPC, or an IUNUA-T-only record. Production SOL and IUNUA fills stay locked. Wrapped XMR, a homemade XMR-SOL bridge and putting a Monero address in the public IUNUA receipt are disallowed.

Wallet test composition

Scan or paste	A public Solana or Monero receive address. The scanner never accepts a key.
IUNUA record	Purpose, amount, optional fee and chosen rail. Optional Devnet IUNUA-T public ref.
Value rail	Stagenet XMR via wallet RPC, or IUNUA-T only. SOL stays locked.
Not a bridge	The two networks stay separate. An on-device agreement is not a legal deed.

Available as a test composition in native Apple source. World App sign-in, mainnet IUNUA and a production XMR payout remain Planned or Locked.

Sources: World App wallet authentication; Monero wallet RPC: payment and reserve proofs; Solana transactions and instruction execution; IUNUA intended architecture

04 / IUNUA WHITEPAPER

Connect with World: a human check and an account are different

World App account sign-in is required for the intended IUNUA treasury-payment flow; a World ID human check is a distinct policy condition.

World ID can supply a privacy-preserving human credential check for IUNUA. World App wallet authentication separately proves control of a World/EVM account. World Chain is a separate blockchain. None of these automatically creates, moves or signs an IUNUA token on Solana.

For this first payment product, World App wallet-account authentication is a required application step, followed by server-verified account linking and separate payment approval. The prepared website QR flow proves a human credential only and does not satisfy that wallet-account sign-in requirement. The exact desktop/mobile World App handoff and supported authentication transport still need implementation and end-to-end validation.

The intended connection journey

1. Ask in IUNUA	The user starts a human check. A server creates a short-lived request, and the official World IDKit displays its QR code or app link.
2. Approve in World	The user scans and approves the requested credential proof. Staging uses a simulator; production requires the real supported credential.
3. Verify and link	The server validates the proof and original request. Linking a Solana account additionally needs proof of wallet-key ownership and explicit consent.

Integration design. A scanned QR or a successful client callback alone is not authentication, token ownership or payment approval.

World connection: implementation and remaining work

Part	Current position
Website QR flow	Requires setup: official IDKit UI and a server verification/session module are prepared. As reviewed on 9 September 2026, no World app ID, RP ID, signing key or database is configured on the site. No real proof was exercised.
Released wallet apps	Requires setup / Planned: reviewed native and Electron 0.8.4 packages provide staging configuration guidance. They do not include the new website QR flow or a completed World login.
Browser human-check session	Prepared code: nonce, signal, browser, environment and action binding; server verification; replay/expiry rejection; 15-minute session. Activation and end-to-end review remain required.
World App wallet sign-in	Planned and required for the treasury-payment target: World App wallet authentication with server-side verification, account linking and a reviewed desktop/mobile handoff. The prepared QR human check does not implement this.
Link to a Solana wallet	Planned: wallet-created challenge, explicit message signature, secure single-use handoff, linking consent and recovery/unlink rules. A pasted address is insufficient.
Token eligibility and rewards	Planned: application or settlement services enforce approved rules. Human verification grants no automatic IUNUA tokens, payments, signing permission or voting rights.

Activation steps

- Register IUNUA and its relying party in the World Developer Portal. Choose the credential and a dedicated human-check action; decide how repeat login differs from a one-time reward claim.
- Configure app ID, RP ID, action and signing-key secret only on the server. Provision the verification-session database. Begin in staging; keep the site access restriction unchanged.

- Test the official QR flow with the simulator, including success, cancellation, expiry, replay, wrong browser and logout. Confirm the result on the server.
- Complete account-linking and recovery design, rate limits, retention/deletion, monitoring and independent review before production identity use.
- Configure World production credentials and test with an eligible real user. Separately integrate wallet handoff and the required World App wallet-account authentication. Solana mainnet remains a separate release decision.

The prepared reference uses an Orb legacy credential proof through IDKit and World's v4 verification endpoint. It stores only short-lived session records, a normalized nullifier and a hashed browser token; raw proof bodies are not retained. The backend accepts only the configured credential shape and must be updated and tested when the selected protocol or credential changes. Production retention cleanup and abuse controls remain launch requirements.

Privacy limit: linking a person identifier to a Solana address creates an association inside IUNUA. Public Solana accounts and transfers remain visible. World ID does not make ordinary token transfers private, provide skill certification or prove every contribution was valuable.

Sources: [World IDKit integration](#); [World React QR widget](#); [World v4 server verification API](#); [World App wallet authentication](#); [World Chain overview](#)

05 / IUNUA WHITEPAPER

The first complete transaction: sign in, pay, verify, record

Working reference: the recipient receives XMR; IUNUA coordinates the process and publishes a Solana receipt. Token redemption remains undecided.

The reference flow below assumes payment directly in XMR. This is a drafting assumption that makes the requested transaction concrete; it does not decide whether a future IUNUA token will represent a redeemable treasury claim. No actual treasury balance, address, recipient, amount or production transaction has been verified for this revision.

Wallet test composition versus production target

Native Apple source now lets two phones share a receive QR, scan a public address, record an agreement with purpose, amount, optional fee note and settlement asset, optionally send Devnet IUNUA-T as a public service record, and optionally spend Stagenet XMR through owner-started wallet RPC. That is a test composition. It is not a legal deed, not a deployed Monero contract on Solana, and not the production World App to XMR treasury flow specified in this paper.

What the wallet can compose today

Part	Required behavior / boundary
Public service record	IUNUA-T on Solana Devnet may carry purpose, amount and fee as an on-device composition plus an optional explorer signature. The public ref must not contain a Monero address.
Selected value rail	Stagenet XMR via wallet RPC, or IUNUA-T only. Production SOL and IUNUA fills stay locked until mint, pool, signing review and a live venue exist.
iPhone custody	Spend keys stay on the wallet-rpc host. Scanning a QR does not import a key and does not authorize a later spend.
Production target	World App sign-in, a licensed or reviewed XMR payout and a mainnet IUNUA mint remain Planned or Locked. Swap execute stays locked.

An end-to-end payment request

Part	Required behavior / boundary
1. Authenticate	Complete World App wallet authentication and server verification using a fresh challenge. If the adopted policy also requires World ID, verify that credential separately. Bind the resulting session to the IUNUA account.
2. Review	Show the source treasury, Monero network, recipient, XMR amount, estimated fee, purpose and public disclosure policy. Show XMR directly; any fiat estimate must carry its rate and time.
3. Authorize	Require an explicit payment approval bound to the exact instruction and a unique request ID. Enforce role, amount limits, required co-approvals, expiry and available unlocked funds at the signing service.
4. Submit	Reserve the accounting amount and fee budget. Construct, approve and submit the Monero transaction through protected signing infrastructure. Persist the transaction reference before automatic retries can create duplicate payments.
5. Verify settlement	Use Monero wallet/chain observations and suitable transaction proof to verify destination, received amount and confirmation policy. Pending, unknown and failed outcomes remain distinct. Never accept a screenshot or client success flag as settlement.
6. Record evidence	Commit the payment result, actual fees, evidence reference, policy version and verification outcome to a durable private record. Store proofs and identity links under explicit access controls.
7. Publish and display	Publish the approved receipt commitment and attestation on Solana. After its transaction is finalized, show both Monero payment status and Solana receipt status, with the permitted evidence and appropriate explorer references.

A receipt failure must not send the money again

Assign one durable payment ID to the original request and separate IDs to settlement and publication attempts. Reconcile an unknown Monero submission before creating another transfer. If XMR settles but Solana publication fails, retain Payment confirmed / Receipt pending and retry only publication. An idempotency key must prevent duplicate economic effects, not merely duplicate HTTP responses.

Failure and correction behavior	
Part	Required behavior / boundary
Authentication or approval fails	Stop before signing. No authorization is inferred from an earlier QR scan or an expired session.
Fee or funds unavailable	Reject or obtain approval for a revised quote. Do not silently change the amount, recipient or fee ceiling.
Submission outcome unknown	Inspect the existing wallet transaction and chain state. Preserve the original request; do not assume failure and resubmit a new payment.
Payment confirmed, receipt unavailable	Retry receipt publication with the same payment identity. Display the partial completion honestly; keep durable evidence available.
Confirmation becomes insufficient	Mark the receipt as superseded or under review through a new append-only record, and apply the documented confirmation/reorganization policy.
Wrong confirmed recipient or amount	A confirmed payment is not undone by editing the ledger or receipt. A refund or compensating transfer is a separately approved transaction; recovery is not guaranteed.

First demonstration acceptance criteria

- Rehearse with isolated Monero Stagenet funds and Solana Devnet receipts before any real treasury payment; use an explicitly labeled World staging flow for that rehearsal.
- Demonstrate one successful authorized payment and a rejected unauthenticated request. Observe the exact wallet build, not just source code.
- Demonstrate timeout recovery, duplicate-request rejection and Solana publication failure after Monero confirmation without a second XMR payment.
- Have an authorized reviewer verify the selected Monero payment proof and recompute the receipt commitment from the disclosed evidence.
- Before any small mainnet pilot, approve custody, networks, real recipient and amount, fees, evidence disclosure, monitoring, recovery and independent review. No production activation is implied by this paper.

Sources: [Monero wallet RPC: payment and reserve proofs](#); [Solana transactions and instruction execution](#); [World App wallet authentication](#)

06 / IUNUA WHITEPAPER

What an on-chain receipt can prove

A public fingerprint proves consistency with disclosed evidence. Payment verification requires the evidence and the verification procedure.

A finalized Solana record establishes that its recorded bytes were included in that chain. A receipt commitment lets a reviewer check that a later-disclosed evidence package matches those bytes. Neither fact by itself establishes that the claimed XMR payment occurred. The initial design relies on identified IUNUA verifier attestations plus independently checkable Monero evidence for authorized reviewers.

Proposed visibility and evidence	
Part	Required behavior / boundary
Public Solana receipt	An opaque receipt ID, schema and policy versions, commitment, verifier identity/signature, claimed verification outcome and a supersession reference when applicable. Exact encoding, storage and access rules remain to be implemented.
Restricted evidence	The payment instruction, consent and approvals, Monero transaction reference, destination, received amount, relevant payment proof, confirmation observations, timestamps and actual fee/accounting data.
Kept out of public receipts	World login payloads, person identifiers/nullifiers, treasury view/spend keys, recovery secrets and raw evidence. Monero transaction IDs and amounts should not be public by default; disclosure requires a deliberate policy.
Payment proof	Monero <code>get_tx_proof/check_tx_proof</code> can verify a payment for a supplied destination and report received amount, confirmations and pool state. Recheck against a trustworthy synchronized node and the adopted confirmation policy.
Treasury reserve evidence	A payment receipt does not prove the total reserve or solvency. Monero reserve proofs concern particular funds at verification; liabilities, other obligations, custody and later spending need separate accounting and review.

Commitments, signatures and trust

Specify canonical serialization, schema version, domain separation and a fresh high-entropy random salt before calculating the evidence commitment. Publish only the commitment; retain the salt with the protected evidence. A bare hash of predictable amounts or addresses can invite guessing. The verifier signature must bind the commitment, receipt ID, network, policy version and outcome. A signing key authenticates the verifier statement; it cannot make a false statement true.

The verification service must check that the proof corresponds to the expected request, recipient and amount; distinguish sender/spend evidence from recipient-payment evidence; check confirmation state;

and reject invalid or reused evidence where policy forbids reuse. Linking a valid payment to an unrelated invoice must fail. The service must not claim that a human-credential check proves an invoice was legitimate.

A chosen Solana memo or a dedicated receipt program could anchor the record. A memo alone cannot enforce authorization, uniqueness or verification semantics. A program with approved verifier keys can enforce receipt-submission rules, but still trusts those verifiers for Monero facts unless a separately designed and reviewed cross-chain verification mechanism is implemented. The receipt mechanism has not been selected or deployed.

Disclosure and corrections

Publicly releasing destination, transaction proof and transaction reference can allow others to verify the associated payment and amount, reducing the privacy of that payment. Keep access purpose-bound and disclose only the needed evidence. Revoking access cannot erase copies already obtained. Public receipts should be append-only: corrections point to the prior record and preserve who changed the claim and why.

Sources: Monero wallet RPC: payment and reserve proofs; Monero privacy and wallet keys; Solana transactions and instruction execution

07 / IUNUA WHITEPAPER

The XMR treasury: control, accounting and recovery

XMR is the intended principal reserve asset. Who owns and can spend it must be settled before funding a production treasury.

The design places the main treasury funds in Monero/XMR. It does not claim that a production treasury already exists or is funded. The recorded Solana Devnet game treasury in this paper is a different test asset/account. A small separate SOL fee budget is needed for public Solana receipts; owning XMR does not pay Solana fees.

Required treasury decisions	
Part	Required behavior / boundary
Ownership and custody	Identify the treasury owner, beneficial interests, authorized operators and applicable obligations. Decide whether funds are project-owned, user-owned or held on behalf of users; a shared custody arrangement must not be implied silently.
Spending control	Use a selected, tested signing/custody design with spending limits, independent approvals where required and separation of online coordination from secret keys. Evaluate Monero-specific signing and recovery capabilities; Solana multisig code does not secure XMR.

Required treasury decisions	
Part	Required behavior / boundary
World sign-in boundary	The treasury signer must validate the authenticated payment authorization and policy. A login-only screen cannot enforce spending restrictions against another client that holds the spend key. Self-custody users retain external spending ability.
Accounting	Distinguish total and unlocked funds, reserved outgoing payments, fees, liabilities and pending reconciliation. Reconcile outgoing spends with appropriate evidence; a view-only wallet is not automatically a complete outgoing-spend ledger.
Recovery	Test protected backups, authorized recovery, signer replacement, key compromise response and provider outages. Revoke application sessions after account recovery; require separate approval to relink a World account to treasury roles.
Reserve risk	Holding treasury funds in XMR does not create a stable fiat value. Treasury coverage depends on asset price, liquidity, fees and obligations. The reference flow sets no exchange rate or guaranteed conversion.

Human login, identity verification and treasury key custody must remain separate. Never place XMR spend keys, view keys, World signing secrets or recovery material in the public paper, browser storage or on-chain receipts. The iPhone wallet is a client of owner-started Stagenet wallet RPC; it does not hold a Monero spend secret and does not spawn monerod. For a real pilot, expose only a small explicitly approved operating amount after the signing and recovery design has been validated.

Sources: [Monero wallet RPC: payment and reserve proofs](#); [Monero privacy and wallet keys](#); [World App wallet authentication](#)

08 / IUNUA WHITEPAPER

The token today: a public Devnet record

The current IUNUA mint exists on Solana Devnet. Production currency issuance is a separate milestone.

Finalized read-only verification on 2026-09-09T09:24:23.195685+00:00. Devnet mint slot 495559004 and treasury-balance slot 495559005. Mainnet genesis was verified; this Devnet mint address returned no account on mainnet at slot 445576054. That checks this address, not every possible IUNUA-named mint. Faucet health was not reverified.

Recorded Devnet state	
Field	Snapshot
Network and program	Solana Devnet; Token-2022
Mint	9UePLTf7PRfbZUDzRq8f4sVo3CE7DsZvEtY7ypYZprk

Recorded Devnet state	
Field	Snapshot
Issued supply	42,000,000 IUNUA (test tokens)
Base units and precision	420000000000000000 base units; 9 decimals
Game treasury token account	8NcU2LK62iNV2ySjHZKgKf72r4yP7tP8dELREZvyr1nW
Game treasury balance	41,999,000 IUNUA (test tokens)
Mint and freeze authority	EixVckoyE92vZTVvA2YYkANenrvJdYDW1rTN5ZP8U43W
Pause state	Unpaused at verification; pause authority retained.
Metadata controls	Metadata pointer and update authorities retained.
Observed extensions	metadataPointer, pausableConfig, tokenMetadata

42 million is issued supply, not an enforced cap. The mint authority is still assigned, so the recorded number must not be advertised as immutable scarcity. The same authority address is recorded for minting, freezing, pausing and metadata control. This snapshot does not establish multisignature custody, decentralized control or governed authority execution.

The game treasury is separate from a faucet reserve. Neither is an individual player balance, and the difference between total issuance and this treasury is not an allocation schedule or proof of adoption. This edition makes no claim that the faucet is funded, reachable or ready to issue tokens.

A Solana mint identifies a token and records shared properties such as supply, decimals and controlling authorities. Creating that mint does not deploy a private ledger, proof verifier, game entitlement system or Pantheon settlement program. The observed extensions provide metadata and pause-related state; they do not establish private transfers or verified eligibility.

What registering or publishing means

The Devnet mint is already publicly inspectable on its network. Publishing a website or metadata does not turn it into a mainnet asset, establish a market or create enforceable economic rights. A future mainnet mint would be a separate issuance. No automatic conversion of Devnet balances, migration entitlement or redemption promise is established by this draft.

The current Devnet IUNUA is a test asset with no represented monetary value, redemption right or verified exchange rate. This describes the Devnet asset, not every capability of the wallet or the intended scope of IUNUA. Solana Devnet is distinct from mainnet and its state can be reset. The successful read-only checks used here did not issue, transfer, freeze or authorize any tokens.

Creating a mainnet token would establish a production-network mint, but it would not automatically enable this wallet to sign mainnet transactions or complete the trust-currency system. The configured production mint and RPC endpoint are currently unset and production signing is disabled. Custody and recovery, network configuration, reviewed signing and confirmation, security validation and explicit

activation are still required for a production wallet flow. Private accounting, eligibility verification and governed settlement have additional implementation requirements.

Sources: IUNUA launch preparation: read-only chain evidence; IUNUA mint on Solana Explorer (Devnet); Game treasury token account on Solana Explorer (Devnet); Solana documentation: create a token mint; Solana documentation: clusters and public RPC endpoints; Solana documentation: token extensions

09 / IUNUA WHITEPAPER

Economics: test issuance is not tokenomics

The test supply is known. Production economic rules still need explicit decisions and validation.

The initial reference payment spends XMR and records an IUNUA audit receipt. It does not mint IUNUA against an XMR deposit or give IUNUA holders a right to withdraw treasury funds. Whether IUNUA becomes redeemable for XMR remains explicitly undecided. The ordinary token is not required merely to anchor a receipt; its eventual utility must be specified separately.

A usable economy needs more than a token count. It needs an account of what can be earned, who funds rewards, which services accept units, what obligations exist and who bears losses when something goes wrong. This draft describes these required decisions without substituting illustrative numbers for an adopted policy.

Economic decisions for a future production system

Topic	Current position / required decision
Supply and issuance	42 million test tokens are recorded on Devnet. Production maximum supply, future issuance powers and enforcement are undecided.
Allocation and vesting	No production allocation percentages, team reserve, investor allocation or vesting schedule is established here.
Reward policy	Useful contributions are the intended basis. Rates, eligibility, budgets, appeals and abuse prevention need approved rules.
Treasury and reserves	XMR is the intended principal treasury asset. Production ownership, custody, funding, spending limits and reporting remain open. No reserve ratio or token backing is established.
Fees and sustainability	XMR payments require Monero fees; Solana receipts require a separate SOL fee budget. Production service fees, subsidies, verifier costs and operating funding remain to be decided.

Economic decisions for a future production system	
Topic	Current position / required decision
Utility and redemption	No guaranteed goods, services, cash redemption, price peg or exchange listing is promised. Real use requires explicit terms and working integrations.
Migration	No automatic test-to-mainnet conversion. Any future migration policy must be separately decided, implemented and communicated.

Questions the next economic design must answer

Can one person claim the same contribution through several accounts? Who resolves conflicting reports of work? What happens when the reward budget runs out? Can administrators change issuance or rewards, and how are participants notified? What happens to outstanding obligations if a service closes? These questions require simulations, operational evidence and governance decisions before real value is involved.

Neither a balance displayed in a demo nor a market estimate for another asset answers these questions. A token holder should not infer ownership of the project, voting rights, profit sharing or a claim on assets from this draft. Any such future rights would require a separate, explicit decision and supporting implementation.

A future redeemable token would need a separately approved exchange-rate rule, reserve coverage and liabilities model, deposit/issuance and burn/redemption rules, liquidity, withdrawal terms, loss allocation, independent controls and appropriate legal review. A payment-proof commitment cannot establish those obligations or make redemption automatic.

Sources: IUNUA launch preparation: read-only chain evidence; IUNUA token and wallet capability status

10 / IUNUA WHITEPAPER

Privacy and security: who can see what

A private intention is not a privacy guarantee. Every boundary needs implementation and review.

For the treasury-payment target, public receipts should expose commitments and attestations, while identity links, XMR recipient/amount and evidence remain restricted by default. Publishing a payment proof can deliberately reveal payment information; a commitment must use a specified salted construction. World account linkage creates a sensitive association within IUNUA. Neither World sign-in nor a Solana receipt adds privacy to a public token transfer.

Visibility boundaries

Private record - planned	Authorized services process the information needed for accounting. Storage, logs and access controls must enforce the boundary.
Scoped review - planned	A named reviewer receives specified information for an authorized purpose. Copies cannot be recalled.
Public chain - visible today	Observers can inspect the mint, public accounts, amounts and transactions. Address reuse and timing can link activity.

Visibility domains require independent controls. The first audited XMR payment requires a minimal Solana receipt; disclosure of its protected evidence remains purpose-bound. Current Devnet transfers do not implement this design.

Principal risks and required controls	
Risk	Required response / present limitation
Compromised signing keys	Protect keys and recovery material; separate client, treasury and upgrade powers. Reviewed signing and Keychain use are not a complete custody audit.
False or replayed claims	Authenticate evidence, bind purpose and policy, enforce expiry and consume unique claim identifiers atomically. Production verification is unfinished.
Ledger inconsistency	Test atomic accounting, durable idempotency, crash recovery and reconciliation. The local JSON simulation is not production persistence.
Operator or governance abuse	Define minimum privileges, approval thresholds, monitored emergency powers and reviewable policy history. These controls are not established by retained Devnet authorities.
Identity and activity linkage	Minimize disclosure and log content; review address reuse, amount and timing correlations. Pseudonyms alone do not guarantee anonymity.
Unavailable or misleading services	Fail closed on unknown proofs, stale network evidence and failed settlement. A pending request or service health response is not payment confirmation.

Public keys and transaction references may be shared as evidence. Private keys, recovery phrases, bearer tokens, identity documents and biometric material must not be placed in the whitepaper, public metadata, demonstration inputs or ordinary logs. An eligibility integration must minimize what it requests and retain only what its justified purpose requires.

The trust model includes wallet software, the user device, event issuers, proof providers, backend operators, RPC providers and authority custodians. A production specification must assign their powers and document the consequences of each compromise. Cryptographic claims need a defined construction, adversary model, implementation review and tests; the current conceptual illustrations and simulated checks provide none of those guarantees.

Reference concepts associated with Monero, World ID or Solana are not partnerships, endorsements or evidence of inherited security. Production legal and privacy requirements must be assessed against the actual system, operating locations and intended use before launch; this technical draft does not establish a legal classification.

Sources: IUNUA intended architecture; IUNUA developer integration guide; IUNUA token and wallet capability status; World ID documentation: overview

11 / IUNUA WHITEPAPER

Readiness gates for the full trust service

These additional gates apply to the complete trust-currency service. A basic token and wallet pilot has a narrower scope.

Additional gates for the first audited treasury payment

Part	Required behavior / boundary
World authentication	A real server-verified World App account session, tested wallet handoff and explicit treasury role mapping. Human verification is checked separately when policy requires it.
XMR custody and signer	Approved owner, funding source, signing design, limits, co-approval rules, backup/recovery and monitored Monero infrastructure.
Payment verification	Expected-recipient/amount proof checks, trustworthy confirmation observations, durable request binding, replay prevention and reconciliation.
Solana receipt mechanism	Adopted schema and commitment construction, authorized verifier keys, durable publication, finalized-status checks and append-only correction rules.
End-to-end acceptance	A test-network rehearsal including partial failures and no double payment, independent review, then a separately authorized small real payment in the exact released app.

Required milestones and acceptance evidence

Milestone	Evidence required before real-value use
Specify policy and economic rights	Versioned decisions for issuance, rewards, fees, treasury, migration and any user obligations or rights.
Implement the private service	Authenticated access, durable transactional accounting, scoped authorization, recovery, reconciliation and privacy-aware logging.
Verify eligibility	Real provider and event adapters; adversarial tests for replay, wrong purpose, expired proofs, duplicate claims and invalid evidence.

Required milestones and acceptance evidence	
Milestone	Evidence required before real-value use
Complete wallet and game flows	Explicit account linking and approval; correct network and amount; actual signing, confirmation, failure handling and recovery in exact release packages.
Implement settlement and authority controls	Reviewed programs/adapters, constrained custody, supply accounting, pause behavior, governed upgrades and preserved historical policy references.
Validate safety independently	Security and cryptographic review, resolved critical findings, reproducible builds and realistic end-to-end testing.
Prepare operations and governance	Monitoring, backups with restore drills, incident ownership, key rotation, dispute handling and approved change procedures.
Approve a bounded production launch	Applicable legal/privacy assessment, published user terms, explicit governance authorization and defined rollout limits.

These are prerequisites for the complete production trust service, not a requirement to finish every future feature before issuing a basic token. The initial token-and-wallet pilot must satisfy its own custody, signing, distribution and operational checks and clearly exclude unfinished capabilities.

Executable swaps need a separately verified route and failure handling. Complete game payments need explicit wallet approval and reconciliation. These can be delivered after a bounded token launch, but must not be presented as available beforehand.

Writing or publishing this paper changes documentation only. It does not activate a signing route, remove authorities, issue a mainnet token, establish token-holder rights or change the website's private access policy.

Sources: [IUNUA token and wallet capability status](#); [IUNUA downloads and installation evidence](#); [IUNUA developer integration guide](#)

12 / IUNUA WHITEPAPER

Release evidence: identify the exact files

[Versions describe releases; hashes identify bytes. This appendix pins the packages discussed in this edition.](#)

Package and signing assessment: 8 September 2026. Manifest generated at 17:14:46 UTC that day. The website release process compared the macOS archives against the installed bundles and recorded signing checks. This paper reuses that dated assessment rather than claiming a fresh signing audit or live test of every capability.

macOS - 0.8.4

Field	Value
Version	0.8.4
Archive	/downloads/IUNUA-Wallet-macOS.zip
Size in bytes	13715290
SHA-256	511e1d065f1a2fb8c6ed31b2b05e719af866e9639962aa505f69b86825e27e91
Requirements	macOS 14 or later

Electron macOS - 0.8.4

Field	Value
Version	0.8.4
Archive	/downloads/IUNUA-Wallet-Electron-macOS.zip
Size in bytes	133738590
SHA-256	9b59b05eeca72ad748184ece8c1c1305ffcf0eede2d200aeb690af597fc6a55d
Requirements	macOS 14 or later · Apple silicon

iOS source - 0.8.4

Field	Value
Version	0.8.4
Archive	/downloads/IUNUA-Wallet-iOS-Source.zip
Size in bytes	20104647
SHA-256	a5739fb9d231a9b3288aefc7a5a83802b240bb8ea50ea2ac2f2a0fd8c65a92d
Requirements	Xcode 16 · iOS 17 simulator

Browser extension - 0.7.0

Field	Value
Version	0.7.0
Archive	/downloads/IUNUA-Wallet-Browser-Extension.zip
Size in bytes	3203743
SHA-256	c25774682e2a91870638a00a0e371493ab5ac9cb6a28c11de0b4253a834bee83

Browser extension - 0.7.0

Field	Value
Requirements	Chrome or Edge 121+

Testnet setup kit - 0.8.4

Field	Value
Version	0.8.4
Archive	/downloads/IUNUA-Testnet-Setup-Kit.zip
Size in bytes	37857
SHA-256	bd9298badd10a9ad01aac4a9b3d32ce324571f470ef0fbd43095cc516c6d847a
Requirements	macOS 14 or later · Node.js 22.13+

A matching SHA-256 confirms that a download matches this recorded artifact. It does not prove the application is safe, audited or suitable for real money. If a release is replaced, publish a new manifest and revalidate its capabilities; do not carry forward evidence solely because its version label is unchanged.

Sources: [IUNUA release manifest](#); [IUNUA downloads and installation evidence](#)

13 / IUNUA WHITEPAPER

Glossary: the words behind the idea

Everyday definitions for the terms used in this draft.

Key terms

Term	Meaning
Trust currency	The project's proposed system for recording qualifying contributions and permitted uses under shared rules.
IUNUA	The ecosystem and proposed mainnet token name/symbol.
Mint	The network account defining a token and its shared properties.
Mint authority	The authority permitted to issue additional tokens. Retaining it is different from enforcing a fixed cap.
Devnet / mainnet	Separate testing and production networks. A Devnet balance is not a mainnet balance.

Key terms	
Term	Meaning
Token-2022	Solana's token program supporting extensions. Only enabled extensions apply to a particular mint.
Private ledger	The proposed authoritative accounting record, with access limited by implemented controls.
Commitment	A cryptographic representation intended to bind a value while concealing it under stated assumptions. No production construction is established here.
Nullifier	A unique marker intended to prevent reusing the same permitted claim or spend.
Eligibility proof	Evidence checked for a specific condition; it is not automatically evidence that useful work occurred.
Settlement	Completion and reconciliation of a value transfer under its applicable rules.
Audit grant	Proposed permission to disclose specified information to a named reviewer for a defined purpose.
Pantheon	The proposed framework for reviewing and authorizing policy or program changes.
Timelock	A required delay between approval and activation; the production duration is undecided.
BFF / MCP	Backend for frontend / Model Context Protocol. Here, proposed backend architecture and a separate local simulation integration respectively.
Notarization / checksum	Distribution review evidence / a file identity check. Neither establishes protocol or financial readiness.
XMR treasury	The intended Monero funds account or custody system; separate from the recorded Solana Devnet game treasury.
Service record	The IUNUA/Solana record of a named service: purpose, amount, optional fee and chosen rail. It does not by itself move XMR.
Value rail	The network that actually moves funds. In the wallet test composition this is Stagenet XMR or IUNUA-T only; production SOL stays locked.
Swap estimates	Informational mid-market quotes. A visible estimate does not enable execution.
Wallet-rpc client	The iPhone talks to owner-started Monero wallet RPC. Spend keys stay on that host.
Receipt commitment	A salted cryptographic fingerprint of defined evidence; matching bytes alone do not establish the truth of the claim.
Verifier attestation	A signed statement by an identified verifier; its trust assumptions must be disclosed.

Key terms

Term	Meaning
Idempotency	A repeated request has no additional economic effect; an unknown payment must be reconciled before another is sent.

Sources: IUNUA intended architecture; IUNUA developer integration guide; Solana documentation: create a token mint; Solana documentation: clusters and public RPC endpoints; Solana documentation: token extensions

14 / IUNUA WHITEPAPER

References and evidence dates

Project evidence establishes project state. External documentation explains reference technology.

The project whitepaper and the separate System & Launch Guide share the same dated technical evidence. The wallet package assessment remains dated 8 September 2026. Mint, treasury and mainnet rent observations are separately dated 9 September 2026. Native Apple wallet source for iPhone navigation, QR scan, locked Swap and agreement composition is dated 10 September 2026. This document separation does not change software, economic policy or chain state.

This edition was revised on 10 September 2026. Current-state statements are limited to the evidence and dates identified here. Source checkout changes, a later explorer view or a different package may show a different state. This is a project draft; unresolved decisions remain unresolved.

Earlier project documents describing only a simulator or stating that no token exists predate the wallet and Devnet milestones. They remain useful historical design notes, but this edition uses the dated package assessment and chain evidence for current-state claims. Planned components in those notes have not been promoted to available functionality.

IUNUA token and wallet capability status

Release review: 8 September 2026. Website figures are separately dated snapshots.

<https://iunua-trust-currency.amun-ra-14th.chatgpt.site/token-status>

IUNUA release manifest

Generated 8 September 2026, 17:14:46 UTC. Exact versions, archive sizes and SHA-256 hashes.

<https://iunua-trust-currency.amun-ra-14th.chatgpt.site/downloads/client-manifest.json>

IUNUA downloads and installation evidence

Package and signing review: 8 September 2026. Version numbers alone do not establish package identity.

<https://iunua-trust-currency.amun-ra-14th.chatgpt.site/downloads>

IUNUA launch preparation: read-only chain evidence

Devnet mint and treasury, mainnet genesis/address absence and rent queries. Checked 2026-09-09T09:24:23.195685+00:00. No transaction submitted.

<https://iunua-trust-currency.amun-ra-14th.chatgpt.site/documents/iunua-mainnet-preparation-evidence-2026-09-09.json>

IUNUA mint on Solana Explorer (Devnet)

Explorer displays current network information, which may differ from the paper snapshot.

<https://explorer.solana.com/address/9UePLTf7PRfbZUDzRq8f4sVo3CE7DsZvEtY7pYZprk?cluster=devnet>

Game treasury token account on Solana Explorer (Devnet)

Public test token account; not an individual player balance.

<https://explorer.solana.com/address/8NcU2LK62iNV2ySjHZKgKf72r4yP7tP8dELREZvyr1nW?cluster=devnet>

IUNUA intended architecture

Project design, not production implementation evidence.

<https://iunua-trust-currency.amun-ra-14th.chatgpt.site/architecture>

IUNUA Trust Lab

Seven-step browser simulation; no real proof verification or settlement.

<https://iunua-trust-currency.amun-ra-14th.chatgpt.site/trust-lab>

IUNUA developer integration guide

Local Game API and MCP simulation boundaries; source presence is not a released payment feature.

<https://iunua-trust-currency.amun-ra-14th.chatgpt.site/developers>

Solana documentation: create a token mint

Accessed 9 September 2026. Mint state, supply, decimals and authorities.

<https://solana.com/docs/tokens/basics/create-mint>

Solana documentation: clusters and public RPC endpoints

Accessed 9 September 2026. Distinct networks and Devnet testing limitations.

<https://solana.com/docs/references/clusters>

Solana documentation: token extensions

Accessed 9 September 2026. General Token-2022 capabilities do not prove an extension is enabled for IUNUA.

<https://solana.com/docs/tokens/extensions>

World ID documentation: overview

Accessed 9 September 2026. Reference concept; no partnership or completed IUNUA production integration is asserted.

<https://docs.world.org/world-id/overview>

World IDKit integration

Reviewed 9 September 2026. Provider documentation establishes the integration mechanism; it does not certify an IUNUA deployment.

<https://docs.world.org/world-id/idkit/integrate>

World React QR widget

Reviewed 9 September 2026. Provider documentation establishes the integration mechanism; it does not certify an IUNUA deployment.

<https://docs.world.org/world-id/idkit/react>

World v4 server verification API

Reviewed 9 September 2026. Provider documentation establishes the integration mechanism; it does not certify an IUNUA deployment.

<https://docs.world.org/api-reference/developer-portal/verify>

World App wallet authentication

Reviewed 9 September 2026. Provider documentation establishes the integration mechanism; it does not certify an IUNUA deployment.

<https://docs.world.org/mini-apps/commands/wallet-auth>

World Chain overview

Reviewed 9 September 2026. Provider documentation establishes the integration mechanism; it does not certify an IUNUA deployment.

<https://docs.world.org/world-chain/index>

Monero wallet RPC: payment and reserve proofs

Reviewed for the 10 September 2026 architecture revision. Provider capabilities do not establish an implemented IUNUA integration.

<https://www.getmonero.org/resources/developer-guides/wallet-rpc.html>

Monero privacy and wallet keys

Reviewed for the 10 September 2026 architecture revision. Provider capabilities do not establish an implemented IUNUA integration.

<https://www.getmonero.org/resources/moneropedia/stealthaddress.html>

Solana transactions and instruction execution

Reviewed for the 10 September 2026 architecture revision. Provider capabilities do not establish an implemented IUNUA integration.

<https://solana.com/docs/core/transactions>