ZENDETSU

Trustless Escrow Infrastructure for the On-Chain Economy

Whitepaper v0.3

Zendetsu Team | Built in Nigeria. For the world.

Abstract

Trust is the most expensive thing in commerce. Lawyers charge thousands to hold it. Banks charge fees to enforce it. Both take days, report everything, and know your business better than you want them to.

Zendetsu is a trustless escrow protocol built on Solana. It replaces lawyers, banks, and blind trust with a smart contract that holds funds, enforces conditions, and releases automatically when both parties agree, or routes to a hybrid AI and human dispute system when they do not.

Four escrow modes cover every use case from a small freelance payment to a nine-figure private deal. One SDK lets any developer integrate in 30 minutes. Fees start at 1.0% and scale down as transaction size grows. No membership required. No paperwork. No middlemen who know your business.

Built in Nigeria, Zendetsu is designed from the ground up for markets where trust infrastructure is most broken and the need is most urgent, starting with West Africa and scaling globally.

---

1. The Problem

Two parties want to transact. Neither trusts the other completely. Their current options are:

Blind trust

Send money and hope. The most common choice and the most dangerous one. Scams, ghosting, and non-delivery are the inevitable results.

Lawyers

A lawyer handling a $10,000 deal can charge more than the deal is worth. They take weeks. They generate paperwork. They know everything about your transaction whether you want them to or not.

Banks

They report to governments, freeze accounts without warning, charge layered fees, and were never designed for peer-to-peer commerce in the first place.

Existing escrow services

Built for one use case, poorly documented, often centralized, and almost always require identity verification that defeats the purpose for privacy-conscious users.

None of these work for the freelancer in Lagos getting paid by a client in London. None of them work for the developer building a peer-to-peer gaming platform on Solana. None of them work for the businessman who needs a large deal settled privately and quickly.

Zendetsu works for all three.

---

2. The Solution

Zendetsu is a Solana smart contract protocol built around five core pillars:

- The Contract: Holds funds in Program Derived Accounts, enforces conditions, and executes releases automatically. Fully on-chain. Open source. Audited before mainnet.
- The Dispute Layer: A hybrid system where AI handles objective cases instantly and a panel of vetted human jurors handles subjective ones. No single point of failure. No bias from a centralized authority.
- The SDK: A TypeScript package any developer can install in one command and have working escrow in 30 minutes. Four modes, full TypeScript types, clean error messages in both English and Nigerian Pidgin.
- The Privacy Layer: Burner IDs so counterparties never see each other's real wallets. Routing options for additional separation. Dashboard privacy for users who do not want their activity in public analytics.
- African Market Infrastructure: Purpose-built features for West Africa and emerging markets, the Ajo rotating savings system, trustless P2P currency exchange, Web2 invisible mode with mobile money integration, and a Deadman Trigger for crypto inheritance.

---

3. How It Works

Every Zendetsu escrow follows the same core flow:

- Step 1: Depositor creates the escrow. Funds split into two vaults immediately. Vault A holds the funds designated for the recipient. Vault B holds the platform fee, separated upfront.
- Step 2: Recipient confirms participation. The timelock begins based on transaction size. Both parties receive burner IDs for the transaction.
- Step 3: Both parties can mutually agree to speed up the transaction to Express or Instant at any point. One party cannot force this on the other.
- Step 4: Either party can send a liveness ping at any time to reset the inactivity clock.
- Step 5: Delivery happens off-chain.
- Step 6: Both parties confirm. Instant release regardless of timelock remaining. Vault A goes to the recipient. Vault B goes to the Zendetsu treasury.
- Step 7 (if silent): Timelock expires and the waiting party can claim. If 180 days pass with no activity, funds return automatically to the depositor.
- Step 8 (if disputed): Escrow freezes immediately. AI evaluates the case first. Objective cases resolve instantly. Subjective cases go to the founding juror panel. The verdict executes automatically on-chain.

Contract Architecture

Each escrow initializes two Program Derived Accounts on Solana. The Vault holds the principal amount and is seeded with [escrow, depositor, escrow_id]. The Fee Vault holds the platform fee and is seeded with [fee_vault, escrow_key]. Every escrow address is fully deterministic and independently verifiable on-chain from just the depositor wallet and escrow ID.

Funds never sit in a shared pool. The escrow account stores both parties, the mode, status, timelock, speed preference, milestone list, and dispute state in a single account sized at initialization. Account space is calculated deterministically from the number of parties and milestones so there are no resize transactions after creation.

The program is deployed at GuDNhDbxfmpAt3zDg9TSPdzAYvARifeFTqUhQRtsmjuC on Solana devnet. The full source is open on GitHub and all 17 tests pass against the live deployment.

---

4. Escrow Modes

Simple 1v1

The simplest way to transact with someone you do not fully trust yet. One party locks funds, the other delivers, both confirm and the money moves. If the deal falls apart before the other side joins, cancelling returns everything with no fee charged.

Milestone

When a project is too large to pay all at once but too important to pay blindly upfront. The full amount locks at the start and releases in stages as each milestone gets approved. Each milestone has a name, a percentage of the total, and a deadline. If a client keeps rejecting the same milestone without a legitimate dispute, the system escalates automatically after three rejections.

Multi-Party

For deals involving more than two people. Up to 5 parties can participate in a single escrow. Odd numbers support majority or unanimous release. Even numbers like 2v2 or 4v4 require unanimous agreement to prevent deadlock.

Timed Release

Lock until a specific date and time. Both parties can confirm early for instant release if the work is done ahead of schedule. If the date arrives and nobody has acted, funds release automatically to the recipient.

---

5. Fee Structure

Fees are calculated by the Zendetsu SDK before the transaction is sent. The user sees exactly what they will be charged before their wallet popup appears. There is no minimum transaction amount.

Deal Size	Fee
$0 to $1,000	1.0%
$1,000 to $10,000	0.8%
$10,000 to $100,000	0.6%
$100,000 to $10M	0.45%
$10M to $100M	0.3%
$100M+	0.15%

Fee Distribution

Recipient	Cut	Purpose
Protocol Treasury	0.2%	Development and running costs
$ABE Burn	0.15%	Deflationary pressure on token
Juror Pool	0.1%	Distributed to case jurors
Senior Council	0.05%	Reserved for major disputes only

Cancel Policy

Cancelled escrows return both vaults in full to the depositor. The platform fee is only earned when a deal completes. No deal, no fee.

---

6. The Dispute System

Step One: AI Triage

Every dispute hits the AI layer first. The system checks whether the case can be resolved objectively from on-chain data and submitted evidence.

Cases the AI resolves: deadline passed with no delivery, on-chain data showing whether a milestone was marked complete, a wallet with a clear pattern of bad faith, a demonstrable breach of conditions both parties agreed to in writing.

Cases the AI does not touch: quality of creative work, anything delivered off-chain, disagreements that come down to one person's word against another's. These go straight to the juror panel.

Step Two: Founding Jurors

A panel of 20 to 50 vetted community members who review cases and vote. Three, five, or seven jurors are assigned per case depending on the stakes. Votes stay hidden until everyone has submitted so no juror can be influenced by seeing how others voted. Majority wins. Partial payment verdicts are supported.

Jurors earn from the 0.1% juror pool of each disputed transaction they adjudicate.

Evidence System

Both parties can upload files, screenshots, contracts, and any relevant documentation via IPFS. The content hash is stored on-chain as immutable evidence that cannot be deleted or altered after submission.

Why Hybrid

Pure AI gets gamed on anything subjective. Pure human panels get slow and expensive as volume grows. The hybrid model uses each where it actually works. AI handles speed on the clear cases. Humans handle judgment on the hard ones.

---

7. Privacy

Zendetsu is built on a public blockchain. All transactions are visible on-chain. We do not claim otherwise. What Zendetsu provides is practical privacy, the kind that matters for real use cases.

- Burner IDs: Every party gets a generated identity that exists only for that transaction. Both sides communicate and confirm using these IDs without ever exposing their real wallets. When the transaction closes the IDs expire permanently.
- Wallet separation: In Private mode, funds route through intermediate accounts so on-chain observers cannot directly connect sender and recipient wallets.
- Lit Protocol encryption: Deal terms, amounts, and party identities are encrypted. Only the two wallets involved can decrypt and read the details.
- Dashboard privacy: Transactions do not appear in public Zendetsu analytics unless the user chooses to opt in.

Ghost Transactions

Ghost mode combines the full privacy layer with dedicated human oversight. A ghost transaction routes through intermediate accounts, encrypts terms via Lit Protocol, uses a private dispute channel if needed, and never appears in any public statistics or dashboards.

Sovereign Ghost is the highest tier. Everything in Ghost mode plus a personal NDA from Zendetsu, 1 hour guaranteed dispute resolution, dedicated senior council access, and a private communication channel for the duration of the deal.

---

8. Security Model

Two Vault Architecture

The platform fee separates into its own vault the moment funds are deposited. User funds and platform fees never sit together. A bug affecting one cannot reach the other.

Timelock Scaling

Amount	Timelock
Under $100	1 hour

Amount	Timelock
$100 to $1,000	6 hours
$1,000 to $10,000	24 hours
Above $10,000	72 hours

Additional Protections

- Liveness ping: Either party resets the inactivity clock at any time for only the Solana network fee.
- Inactivity timeout: 180 days with no activity returns funds automatically to the depositor. No funds are ever permanently locked.
- Milestone abuse protection: Three rejections of the same milestone triggers automatic escalation. Neither party can hold the other hostage indefinitely.
- Overflow protection: All arithmetic uses checked operations throughout the program. Overflow is a known exploit vector in smart contracts and is handled at every calculation.
- Open source: The smart contract is publicly readable. Security through obscurity is not security.
- Audit before mainnet: No real funds until a third party security firm has reviewed the contract.

---

9. The SDK

The Zendetsu SDK is a TypeScript package published to npm as @zende/sdk. It handles all protocol interactions. Developers install it with one command and have working escrow in 30 minutes.

- Calculates and displays exact fees before any wallet popup appears
- Wraps all 10 program instructions with full TypeScript types
- Handles PDA derivation, milestone validation, and transaction building
- Surfaces clean human-readable error messages in both English and Nigerian Pidgin
- IDL bundled inside the package, zero configuration beyond the provider

```
npm install @zende/sdk
```

The pidgin error system is a first for any Solana SDK. Developers building for African users can initialize the client with lang: 'pidgin' and every error message surfaces in Nigerian Pidgin English automatically.

---

10. Built for Africa

Zendetsu is built in Nigeria and designed specifically for the problems African commerce faces. Beyond the core protocol, several features are built exclusively for the African market and the 1.4 billion people across the continent who need better financial infrastructure.

Ajo System

Ajo is a Nigerian rotating savings system. A group contributes money regularly and one person gets the full pot each round. Zendetsu automates this trustlessly on-chain. The smart contract holds everyone's contributions and releases to the correct person at the correct time based on the agreed schedule. No organizer to trust. No human who can run with the money. Fully verifiable on Solana.

This is culturally resonant for Nigeria and West Africa and completely unserved in Web3. Every Yoruba, Igbo, and Hausa person knows what an ajo is. Building it on-chain for them is both product and community.

P2P Currency Exchange

Person A has USDC and wants Naira. Person B has Naira and wants USDC. Both sides lock into a Zendetsu escrow simultaneously. Both confirm. The swap executes atomically. Nobody can run. No centralized exchange. No KYC unless fiat rails require it.

Binance P2P has centralized risk and charges fees. The Zendetsu version is trustless, cheaper, and requires no account with a centralized party. This serves Nigeria, Ghana, Kenya, and every market where people constantly convert between crypto and local currency.

Web2 Invisible Mode

A web2 user signs up with email or phone. Zendetsu creates a custodial wallet silently in the background. They fund it via bank transfer, card, or mobile money, Opay, Palmpay, Flutterwave, M-Pesa, MTN MoMo. They create or join an escrow. It looks like a normal payment app.

When the deal completes funds hit their bank account or mobile money wallet automatically. They never see a wallet address. They never hold SOL. They never know it is blockchain. The Solana program is the settlement rail. Like how people use WhatsApp without knowing it runs on AWS.

Deadman Trigger

If a wallet goes completely inactive for a user-defined period, funds automatically transfer to a pre-designated beneficiary wallet. This is a crypto will and inheritance system. Nobody has built this cleanly on Solana.

The use case is serious. Someone dies or becomes incapacitated. Their SOL does not get locked forever in an inaccessible wallet. It goes to whoever they designated, automatically, trustlessly, verified by on-chain inactivity.

---

11. Roadmap

Version	What	Timeline
V1 Foundation	Core protocol, 4 escrow modes, SDK, demo site, 17/17 tests passing	Complete
V1.1 Developer Experience	Mainnet deployment, full docs site, SDK polish, ecosystem outreach	Month 1
V1.2 Privacy Layer	Burner IDs, Lit Protocol encryption, private routing	Month 2 to 3
V1.3 Speed Control	Express and Instant settlement UI fully surfaced	Month 3
V2 Dispute System	AI triage, founding juror panel, evidence via IPFS	Month 4 to 7
V2.1 Ghost Transactions	Full confidentiality mode, Sovereign Ghost tier	Month 7 to 8
V2.2 Tipping	Payment links, QR codes, zende.xyz/pay/handle	Month 8
V2.3 Deadman Trigger	Crypto will and inheritance system	Month 9
V3 Payment Infrastructure	Recurring payments, splits, SPL tokens, invoices	Month 10 to 14
V3.1 Web2 Invisible Mode	Fiat onramp, custodial wallets, mobile money integration	Month 12 to 15
V3.2 P2P Currency Exchange	Trustless Binance P2P for African markets	Month 14 to 16
V3.3 Ajo System	Rotating savings on-chain	Month 15 to 17
V4 Ecosystem	Audit, REST API, cross-chain, $ABE token, white label	Month 18+

---

12. Supported Assets

V1 supports SOL only. Tokens with freeze authority are automatically rejected at the SDK level before any transaction is sent. USDC and additional SPL token support arrives in V3 alongside the full payment infrastructure layer.

---

13. The $ABE Token

$ABE is the protocol governance and utility token. Stakers receive a 20% discount across all fee tiers. A portion of all protocol fees goes to token burn and the juror reward pool. Token holders participate in governance over juror selection and protocol upgrades.

Token launch is planned alongside V4 after the protocol has meaningful mainnet transaction history and a verified reputation system.

---

14. The Moat

The code is open source. Anyone can fork it. The moat is not the code.

The moat is the reputation system with real transaction history on mainnet. The moat is the founding juror community, trusted humans who cannot be copied overnight. The moat is African market penetration where the problem is most acute and alternatives are worst. The moat is the cultural identity, the language, the brand, the community that forms around something built specifically for them.

Zendetsu is infrastructure. The goal is to become the trust layer for African commerce and Solana-based agreements the same way Stripe became the payment layer for the internet, invisible, essential, everywhere.
