ZAKAT COIN

The "HyFi" Hybrid-Finance Donation & Distribution Protocol

Where Every Transaction Becomes an Act of Giving

Symbol: ZKTC

Network: BNB Smart Chain (BEP-20)

FinCEN MSB: 31000302240755

USPTO Patent: 19/640,087

PCT International: Filed

Shariah Review: Reviewed by Board of Scholars (v2 under review)

501(c)(3) EIN: 39-4624928 (Zakat Coin Organization Inc.)

Whitepaper Version: 2.0

Zakat Coin Inc. DBA ZakPay · A Delaware C-Corporation

Utility Token Declaration

ZKTC is a consumptive utility token. It is the unit consumed to use the network: each payment instruction settled through the FUSE engine consumes ZKTC (a Settlement Instruction Record is created and the corresponding token is burned at settlement), and ZKTC powers the platform actions a user performs in ZakPay — sending, spending, holding, and triggering the Giving Contracts. Users acquire ZKTC to access and consume these services, not as an investment. The token confers no equity, no dividend, no profit share, no interest, and no claim on the proceeds or assets of any entity. Its value is functional — it is spent to operate the network. No expectation of profit from token price is created or intended.

Important Distinction

While Zakat Coin carries the sacred term *"zakat"* in its name, we fully affirm that acquiring or using ZKTC does not itself constitute a zakat payment, nor does it fulfill the religious obligation of zakat (*fard*). The divine command of zakat remains a personal, spiritual duty upon each eligible Muslim, requiring clear *niyyah* (intention), calculation after one lunar year (*hawl*), and distribution to the eight Quranic categories (*asnaf*).

Zakat Coin serves as technological infrastructure — a bridge between traditional Islamic obligations and modern financial systems. The platform provides tools for accurate calculation, transparent distribution, and verified charity selection, while preserving the spiritual essence and personal responsibility of zakat.

Table of Contents

Technical Protocol Appendix — for auditors, integrators, and reviewers requiring architectural detail

Executive Summary

ZakPay is a Shariah-compliant payment and remittance platform built for the global Muslim community and for any individual or institution committed to transparent charitable giving. The platform combines domestic and international payments, card spending, and structural charity routing into a single application, addressing a market gap that no existing financial infrastructure serves as a unified product.

What ZakPay Does

Every primary user action on ZakPay — acquiring tokens, donating, sending money domestically or internationally, or tapping the card at a merchant — triggers a charitable consequence by structural design. A defined portion of every transaction routes to verified nonprofit destinations through smart-contract enforced Giving Contracts. Charity is not a feature toggled on; it is a structural property of the protocol.

The Four Layers

ZakPay	The consumer-facing application and operating ecosystem. Mobile and web. Domestic and international payments, card spending, charitable giving, and Zakat / Sadaqah calculation tools.
FUSE	The patent-protected settlement orchestration engine. Routes payment instructions across regulated banking and payment counterparties, capable of orchestrating 1–3 second end-to-end delivery in any country where the ZakPay application is accessible to users and where licensed counterparty institutions are aligned. FUSE orchestrates; licensed counterparties execute jurisdiction-specific settlement.
ZKTC	The utility token implementation used within the ZakPay ecosystem (BEP-20 on BNB Smart Chain). Every ZakPay transaction creates a Settlement Instruction Record (SIR) backed by ZKTC; every completed transaction permanently consumes the associated ZKTC. Utility demand is tied to platform usage, not speculation.
ZUSD	A stable token backed 1:1 by USDC, used for charitable disbursement and stable-value settlement. All distributions to verified charities are denominated in ZUSD — recipients receive predictable value, not exposure to token volatility.

How the Business Generates Revenue

Zakat Coin Inc. earns revenue from commerce processed through ZakPay — transaction fees (targeted 1.5–2.5% per transfer), foreign-exchange margin, and card interchange. This platform commerce revenue is the operating company's primary income stream. Token-acquisition proceeds are kept structurally separate from corporate revenue: they route to the liquidity pool, the Team Liquidity Pool, and operating token infrastructure (the full allocation is detailed in Section 8). Corporate success is tied to platform usage, not token market dynamics.

Why the Architecture Is Differentiated

The combination ZakPay offers is underserved in the market: **(1)** consumer-grade payment app with seconds-finality international remittance, **(2)** structural charity routing on every transaction class, **(3)** on-chain tax-deductible receipts via ZKT-Badge soulbound NFTs from a U.S. 501(c)(3) fiscal sponsor, and **(4)** Shariah-compliant by design with absolute

ZCBS (Zakat Coin Board of Scholars) veto authority. Existing payment, remittance, and charitable-giving categories address subsets of this capability; none integrate all four.

Why the Structure Is Sustainable

The protocol's economics are bounded by smart-contract-level commitments: a 14.25 billion operational supply hard cap, a bounded ZPP settlement reserve, and hard-coded caps on every economic mechanism. The FUSE patent is held by the Inventor, who has granted Zakat Coin Inc. an executed, irrevocable, perpetual, royalty-free license structured to survive any change of control — so ecosystem access to FUSE does not depend on who holds the patent.

PART I — IMPORTANT DISCLOSURES

Read before anything else

Section 1 — Important Notice & Plain-Language Summary

Read this first

Important Notice

This whitepaper has not been reviewed or approved by any competent regulatory authority in any jurisdiction.

ZKTC is a utility token intended for consumptive use within the ZakPay ecosystem. It is not a share, security, financial instrument, deposit, or investment product, and it is not offered as one. ZKTC confers no ownership interest, no equity, no dividend, no profit share, no interest, and no claim on the assets, revenue, or proceeds of Zakat Coin Inc. or any other entity. It carries no entitlement to any return.

Acquiring or using ZKTC involves risk, including the risk that the token may lose value in part or in full, and the risk that particular features may not be available in a given jurisdiction or at a given time. ZKTC is not covered by any investor-compensation scheme or deposit-guarantee scheme. Zakat Coin Inc. does not guarantee any future value, price, return, liquidity, or availability of the token or of any ZakPay feature.

Nothing in this document constitutes investment, financial, legal, accounting, or tax advice, or a recommendation to acquire or use ZKTC. Prospective participants should assess the risks independently and, where appropriate, obtain their own professional advice before acquiring or using ZKTC. Participation may be restricted or prohibited in certain jurisdictions; it is the responsibility of each prospective participant to determine whether they are legally permitted to acquire or use ZKTC in their jurisdiction and to comply with any applicable laws.

Statements in this document about intended design, functionality, or development reflect present intentions only. They are not guarantees, actual outcomes may differ, and Zakat Coin Inc. is not obligated to update them except as required by law.

Plain-Language Summary

ZakPay is a Shariah-compliant payment and charitable-giving platform for the global Muslim community and for anyone committed to transparent giving. Within ZakPay, ZKTC is a utility token that is consumed to settle transactions: each payment creates an on-chain Settlement Instruction Record (SIR), and the associated ZKTC is burned when the transaction settles. ZKTC confers no profit, dividend, equity, ownership, or entitlement to returns of any kind; its value to a user is functional — it is spent to operate the network and to access reduced fees and platform features. A defined portion of activity routes to verified charities through smart-contract Giving Contracts, making charitable giving a structural property of the system rather than an optional feature. ZUSD, used for stable-value settlement and charitable disbursement, is a stable token backed 1:1 by USDC. This document describes what ZKTC is, what it is not, how it works, the mechanisms that support it, and the risks involved.

Section 2 — Persons Responsible & Entity Structure

Who is behind ZKTC, and who is responsible for this document

Three distinct entities participate in the Zakat Coin ecosystem, each with a separate and clearly bounded role.

Entity	Role
Zakat Coin Inc. (DBA ZakPay)	The offeror of ZKTC and the entity responsible for this whitepaper. Operates the ZakPay platform and is the counterparty for the ZKTC utility described in this document.
Zakat Coin Organization Inc.	A U.S. 501(c)(3) nonprofit entity (EIN 39-4624928). Operates the charitable-custody wallets that receive the charitable contributions arising from ZakPay and ZKTC activity. Firewalled from operating capital.

Entity	Role
The Inventor	Holds the FUSE patent (see the Underlying Technology section). Has granted Zakat Coin Inc. an executed, irrevocable, perpetual, royalty-free license to the FUSE patent.

Responsibility Statement

Zakat Coin Inc. is responsible for the information contained in this whitepaper. To the best of its knowledge, the information is accurate and no material information has been omitted. This document is issued by Zakat Coin Inc. as the offeror of ZKTC.

PART II — THE ASSET & ITS UTILITY

What ZKTC is, what it is not, and what it does

Section 3 — The Two-Token Utility Model

A dynamic engine token, and a stable settlement rail

The Zakat Coin ecosystem is powered by a dual-token design that separates utility (ZKTC) from stable value (ZUSD). This model provides both a dynamic engine token to drive on-chain smart contracts and a stable settlement rail to deliver predictable, real-world value to charities and end users.

ZKTC — Utility Engine Token

Blockchain	BNB Smart Chain (BEP-20)
Primary Function	Ecosystem utility, charitable automation, and commerce-driven supply activation
Operational Supply	14,250,000,000 ZKTC (hard-capped)
Settlement Role	SIR placeholder for every ZakPay transaction; minted at payment instruction, burned at settlement confirmation
Giving Layer	Powers the Giving Contracts on every acquire, hold, or sell action
Liquidity Architecture	Integrates with FLIP and FLOP to maintain pool depth and settlement health
What ZKTC Is NOT	A security, an investment vehicle, or a standalone payment instrument

ZUSD — Stable Value Rail

Type	A stable token backed 1:1 by USDC
Islamic Compliance	Non-interest bearing, halal by design
Settlement Speed	1–3 seconds to fiat via FUSE orchestration and partner settlement counterparties
Charity Disbursement	All distributions to verified NGOs executed in ZUSD — charities are shielded from volatility
Global Payments	Stable value for international commerce and charity across the global corridors where the ZakPay application and licensed counterparty institutions are aligned
Backing Guarantee	Strict 1:1 USDC backing; reserve held by the regulated issuer of record under a Stablecoin-as-a-Service model

Why Two Tokens, Not One

A single-token system forces a difficult tradeoff: either the token absorbs all the volatility (terrible for charitable recipients planning real-world disbursement), or it tries to be artificially stable (which sacrifices the utility incentives that make commerce-driven supply activation work). The dual-token architecture lets each token do what it does best: ZKTC powers utility consumption and represents real protocol activity; ZUSD delivers stable, predictable value to charities, merchants, and recipients who need to plan in dollars.

Section 4 — Utility & Rights

What ZKTC does — every benefit is accessed by using the token, never by holding it

Primary Utility: Consumptive Settlement Fuel

ZKTC is consumed to do work. The ZakPay SIR wallet uses ZKTC to settle transactions: when a payment instruction is created, a Settlement Instruction Record (SIR) is generated, and the associated ZKTC is burned at settlement. The token is spent performing the network's core function — it is fuel consumed in the act of settlement, not an asset held for appreciation. Utility demand is therefore tied directly to platform usage: the more transactions ZakPay settles, the more ZKTC is consumed.

Secondary Utility: Access Through Use

Using ZKTC within ZakPay unlocks functional benefits, each accessed by spending or consuming the token in a transaction:

- **Reduced transaction fees** — transacting with ZKTC lowers the fee on eligible ZakPay transactions.
- **Platform discounts** — spending ZKTC provides access to discounts on eligible platform services.
- **Zakat-360 access** — using ZKTC unlocks access to Zakat-360 subscription features and associated discounts.

Each of these is obtained by using ZKTC in a transaction. None is granted for holding or owning the token, and none constitutes a financial return, yield, or profit.

PART III — PURPOSE & ECOSYSTEM

Why ZKTC exists and how the ecosystem operates

Section 5 — The Giving Contracts (Unified Concept)

Every action triggers a charitable consequence. The destination, not the giving, is the choice.

At the heart of the Zakat Coin ecosystem is a family of smart contracts collectively called the **Giving Contracts**. These contracts route ZUSD to verified charitable destinations based on user actions within the ZakPay platform. Rather than presenting users with a dozen distinct giving programs to evaluate and select, the protocol uses a single conceptual model: *any acquire, hold, or sell action involving ZKTC can trigger a corresponding charitable flow*.

What varies between Giving Contracts is not whether charity occurs — charity occurs structurally on triggered events — but the trigger condition, the rate, and the routing destination. The user experiences this as a unified, predictable behavior: their participation in the protocol carries a charitable consequence by design.

The Three Trigger Categories

Trigger Category	What It Means	Example User Action
ACQUIRE	Charitable routing triggers when a user acquires ZKTC tokens or initiates a ZakPay transaction	Purchasing ZKTC through the ZakPay platform; sending money internationally via Zak-It; spending with the ZakPay Card

Trigger Category	What It Means	Example User Action
HOLD	Charitable routing triggers based on duration or characteristics of token holding	Tokens held in a vault for a defined period generate charitable distributions; wallets above nisab receive annual zakat prompts
SELL	Charitable routing triggers when a user sells or converts ZKTC	A defined portion of a conversion routes to charity automatically

Acquisition Giving (UTG) — The Contribution on Acquisition

The ACQUIRE trigger is implemented through **Acquisition Giving** (referred to in Shariah documentation as User-Triggered Giving, or UTG). When a user acquires ZKTC, a charitable contribution is routed through the Giving Contracts and settled in ZUSD. For acquisitions up to $1,000, the contribution is 2.5%. For acquisitions above $1,000, the user sets the rate using the **Donation Slider**, from 1% to 10%. The applicable rate and the receiving charity are disclosed to the user at the point of acquisition, and participation follows from the user's choice to acquire and use ZKTC within the ecosystem.

By default, this contribution is a voluntary charitable gift (*sadaqah*) and is routed to the Sadaqah Charity Wallet (SCW); by default it does not constitute zakat. The user's charitable intent is set separately through the Intent Toggle described below — the Donation Slider sets only the amount, never the religious character of the gift.

Hold-to-Give (HTG) — Charity From Reserves While Holding

Hold-to-Give (HTG) implements the HOLD trigger. While a user holds ZKTC under the defined holding conditions, the protocol releases a charitable distribution *from its own charity reserves* to the appropriate charitable wallet. The user is not required to stake, lock, lend, or transfer any tokens, and the user's own token balance is never reduced or incremented; the holding period functions only as a qualifying condition for the protocol to give from its reserves.

Distributions under Hold-to-Give are released in **ZUSD (backed 1:1 by USDC)** as a fixed-value charitable amount — not as a quantity of ZKTC scaled to token price. The benefit accrues exclusively to charitable recipients, never to the holder as monetary gain. Hold-to-Give is therefore a time-conditioned charitable commitment by the protocol, and is not staking, yield, APR, rewards, or passive income of any kind.

How Hold-to-Give Stays Funded

Hold-to-Give distributions are paid from the HTG Piggy Bank (HPB), a reserve held in real USDC. The HPB is funded from multiple streams rather than a single source: a share of token-purchase proceeds, deposits from FLOP operations at the liquidity ceiling, a portion of ZakPay card interchange, and ZakPay transaction revenue. Each of these contributes USDC to the HPB over time.

Critically, a Hold-to-Give match fires only when the HPB already holds the USDC to back it. The distribution is paced by the reserve's actual balance, not by a fixed calendar: if the reserve holds sufficient USDC, qualifying matches are released; if it does not, they queue without expiry until the reserve is funded. This means Hold-to-Give can never distribute more than it holds — the mechanism is solvent by construction, because it pays only from USDC already collected. A match, when it fires, is a real charitable distribution backed by real USDC, and the corresponding ZKTC is burned on the event. The protocol makes no promise as to when any individual match will fire; it promises only that no match is paid that is not already fully backed.

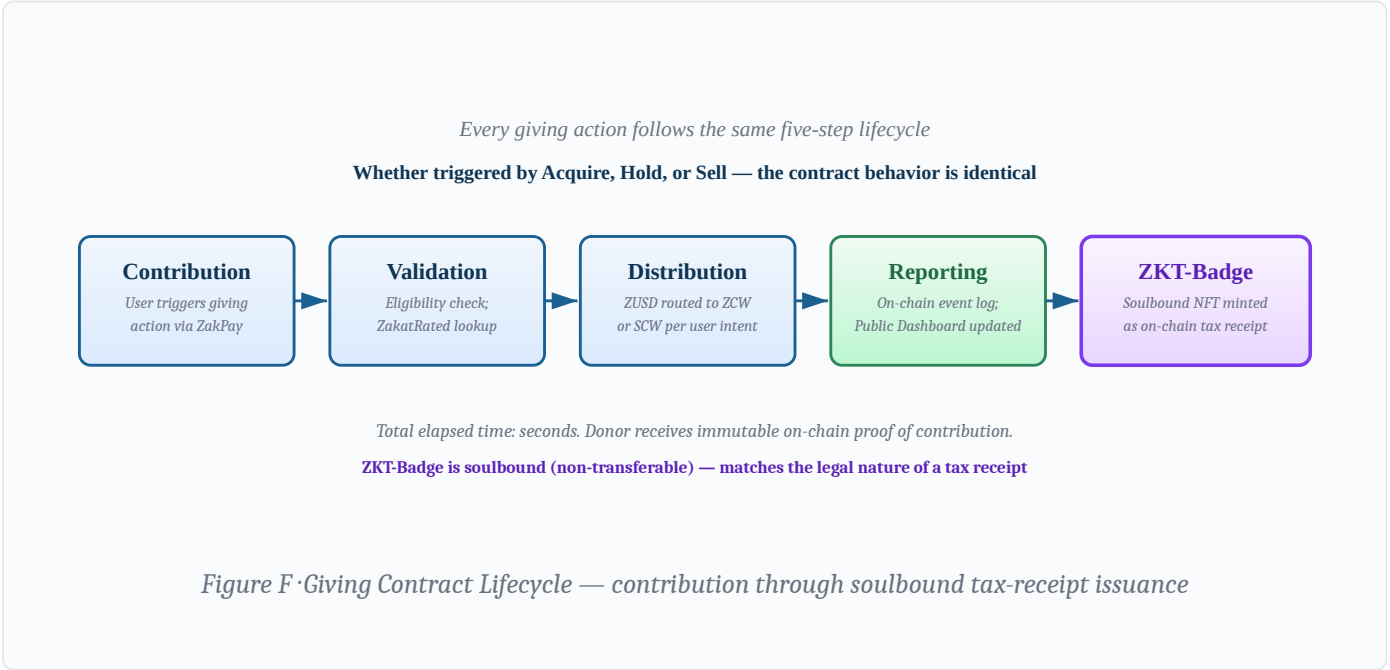

Figure F·Giving Contract Lifecycle — contribution through soulbound tax-receipt issuance

How a Giving Contract Trigger Fires

Each Giving Contract follows the same architectural pattern:

1. **Detection:** The contract detects an eligible trigger event (acquisition, hold-period completion, or sale).
2. **Calculation:** The contract calculates the charitable amount based on the event's parameters (transaction value, hold duration, or profit amount).

3. **Routing decision:** The contract identifies the appropriate charitable destination (Zakat Charity Wallet for zakat-eligible flows; Sadaqah Charity Wallet for voluntary sadaqah).
4. **Distribution:** The contract converts the charitable amount to ZUSD (the stable settlement rail) and routes it to the destination wallet.
5. **Recording:** An immutable on-chain record of the charitable distribution is created, complete with timestamp, amount, source wallet, and destination.

> *Generic Giving Contract Amount*
>
> $$C = E \times r$$
>
> *where C is the charity amount routed, E is the eligible event value (acquisition amount, sale profit, or hold-bound calculation), and r is the applicable rate for that contract.*

```
Giving Contract Trigger (Pseudocode)

function onTriggerEvent(event): if not isEligible(event): return charity_amount =
event.value * applicable_rate destination = event.user.charity_intent # ZCW or SCW
zusd_amount = convertToZUSD(charity_amount) route(zusd_amount, destination) emit
CharityRouted( amount = zusd_amount, destination = destination, trigger_type =
event.type, timestamp = now() )
```

The User Experience

From the user's perspective, the experience is simple: every interaction with ZakPay carries a charitable footprint, and the user chooses the destination (zakat-eligible or sadaqah) at the time of transaction, not the act of giving itself. The giving happens by architecture. The intent is what the user controls.

The Intent Toggle — Zakat vs Sadaqah

The Critical Distinction

Zakat and sadaqah are not interchangeable in Islamic jurisprudence. Zakat is *fard* (obligatory) for eligible Muslims, must be calculated against specific thresholds (nisab), distributed to specific categories (the eight *asnaf*), and requires conscious religious intent (*niyyah*). Sadaqah is voluntary charity, broader in scope, and does not carry the same jurisprudential strictness. The protocol's architecture preserves this distinction at the smart contract level: zakat-intent transactions route exclusively to the Zakat Charity Wallet (ZCW), funding only zakat-eligible causes per scholar-approved categories. Sadaqah-intent transactions route to the Sadaqah Charity Wallet (SCW), funding the broader range of voluntary charitable causes. **The protocol never blends them.**

The Zakat Toggle — How Intent Is Set

Charitable intent is set by the user through the **Zakat Toggle**. By default the toggle is off, and contributions are treated as voluntary sadaqah routed to the Sadaqah Charity Wallet (SCW). When a user enables the Zakat Toggle, they are presented with an intention (*niyyah*) acknowledgment; only upon that explicit acknowledgment is the contribution treated as zakat and routed to the Zakat Charity Wallet (ZCW).

The ZCW disburses only to charities that both accept zakat and maintain a segregated zakat account, drawn from the scholar-approved zakat-eligible categories. Eligibility is therefore enforced by the routing itself: funds designated as zakat can only reach recipients qualified to receive it. A contribution that is not accompanied by the toggle and the acknowledged intention is never represented as, or counted toward, zakat. This design places the deliberate act of intention — not a slider position or a default setting — at the center of any zakat determination, consistent with the requirements of the ecosystem's Shariah governance.

Section 6 — Charity Architecture

501(c)(3) conduit, ZakatRated NGOs, USDC-backed disbursement

The Dual-Wallet System

All Giving Contract distributions route to one of two destinations, custodied separately at an institutional brokerage and custody provider under the 501(c)(3) charitable entity:

Wallet	Purpose	Eligible Recipients
ZCW — Zakat Charity Wallet	Receives all zakat-intent distributions. Funds eligible only for the eight Quranic categories (*asnaf*) of zakat recipients per classical Islamic jurisprudence.	Verified NGOs serving the eight *asnaf*; specifically vetted for zakat-eligibility by the Board of Scholars
SCW — Sadaqah Charity Wallet	Receives all sadaqah-intent distributions. Funds the broader range of voluntary charitable causes consistent with Islamic charitable principles.	Verified NGOs covering humanitarian aid, education, healthcare, infrastructure, disaster relief, and other causes consistent with Islamic charitable principles

The 501(c)(3) Conduit Principle

Both the ZCW and SCW are wallets owned and operated by Zakat Coin Organization Inc., a registered 501(c)(3) non-profit (EIN 39-4624928). Zakat Coin Inc., the technology company, never custodies charitable funds. The smart contract routes ZUSD directly from buyers to the 501(c)(3)-controlled wallets. This is a structural conduit, not a discretionary one — the routing is enforced by smart contract logic, not by company policy.

Donors to the system receive tax-deductible acknowledgment from the 501(c)(3) for the portion of their participation that constitutes charitable contribution under U.S. tax law. The acknowledgment letter is generated automatically and matched to the on-chain charitable distribution record.

ZakatRated NGO Verification

Charities eligible to receive distributions are vetted through **ZakatRated**, a proprietary transparency-based approval system that verifies non-profits against strict compliance, accountability, financial transparency, and operational integrity standards. ZakatRated maintains a public registry of verified NGOs, their geographic scope, the categories they serve, and their historical disbursement records.

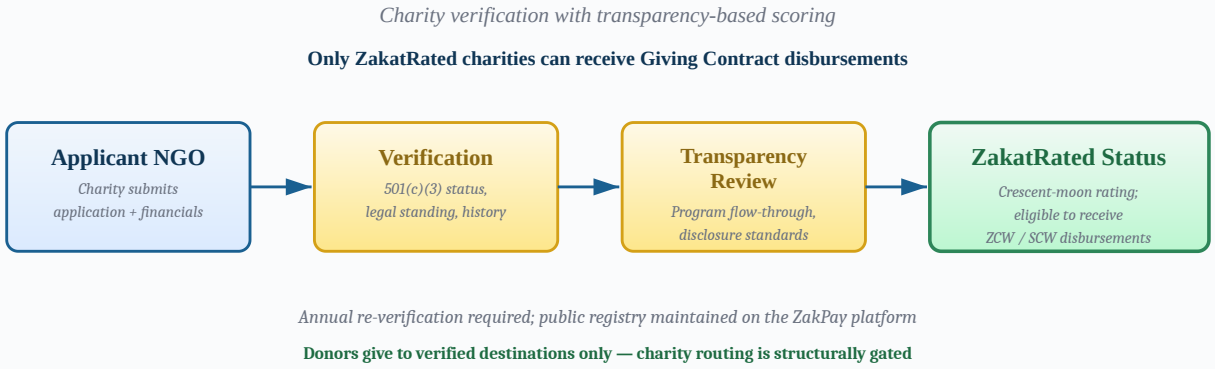

Figure E·ZakatRated Verification Framework — how charities qualify to receive protocol-routed disbursements

Why ZUSD Disbursement Matters

Most cryptocurrency charitable mechanisms fail the same way: they denominate charitable reserves in volatile tokens. When price falls, charitable capacity falls. Recipients can plan nothing. Impact becomes speculative. Zakat Coin solves this with a USDC-backed reserve model. All ZCW and SCW disbursements execute in ZUSD — the 1:1 USDC-backed stablecoin — ensuring that approved charities and NGOs receive predictable, real-world funds without exposure to crypto volatility.

Section 7 — The ZakPay Platform

Every action embeds charity. The destination varies. The giving does not.

ZakPay is a licensed halal payment platform serving the global Muslim community with Shariah-compliant domestic payments, international remittances, automated Zakat and Sadaqah flows, card spending, charitable giving, and native custodial token acquisition — all accessible through a single mobile and desktop application.

The user never interacts with ZKTC directly. They see ZakPay working. ZKTC is the operational layer beneath every transaction — the layer that makes ZakPay trustworthy by design rather than by promise.

Feature Availability Is Partner-Gated

ZakPay delivers domestic and international transfer corridors, card spending, and charitable disbursement to ZakatRated NGOs. Each capability depends on the alignment of the Banking and Financial Institution (BFI) partners required to deliver it in a given jurisdiction, and a capability becomes available in a market once the corresponding partner integration and regulatory approvals are in place. Because availability is tied to partner alignment rather than to a fixed schedule, the set of live features differs by market and expands as integrations complete. The Public Utility Dashboard is the authoritative source for which capabilities are live in which markets; it lets any reader verify the operational state directly rather than relying on this document.

The Launch Precondition

Zakat Coin will not launch the token publicly until ZKTC is operational as the SIR placeholder that settles transactions under the FUSE license. This is an architectural precondition, not a target: without ZKTC settling as the placeholder under FUSE-SIR, there is no On Demand Supply, and without On Demand Supply there is no functioning protocol. The requirement is therefore self-enforcing — a public launch is only possible once the settlement mechanism it depends on is live and verifiable on-chain.

The Core Product Insight

ZakPay is the first payment platform where **every primary user action triggers a charitable consequence by structural design**. Whether the user acquires ZKTC, donates directly to a 501(c)(3) charity, sends a P2P transfer domestically or internationally, or taps the ZakPay Card at a merchant — each action routes a defined portion to verified charitable destinations through the Giving Contracts layer. Charity is not a feature toggled on; it is the protocol's structural property.

The Four Primary Actions

Action	What the User Does	What ZKTC Does Beneath
ACQUIRE	Acquires ZKTC tokens through ZakPay's native custodial acquisition flow, exchanging USD, USDC, or other supported assets for ZKTC at the prevailing utility price — tokens custody at a federally chartered qualified custodian under the user's beneficial ownership	SIR records the acquisition; ACQUIRE-triggered Giving Contract routes a defined portion of the transaction to charitable reserves; ODS may activate proportional supply from operational reserves
DONATE	Sends a direct charitable contribution from their ZakPay balance to a ZakatRated-verified 501(c)(3) nonprofit — funds arrive in seconds rather than the weeks required by traditional charitable rails; user receives an on-chain ZKT-Badge representing a soulbound tax receipt from Zakat Coin Organization Inc., the protocol's 501(c)(3) fiscal sponsor	SIR records the donation instruction; FUSE orchestrates the ZUSD transfer instruction; the destination institution executes delivery to the nonprofit recipient in 1–3 seconds; ZKT-Badge mints to the donor's wallet as immutable proof of charitable contribution; tax-deduction substantiation is recorded on-chain

Action	What the User Does	What ZKTC Does Beneath
SEND (Zak-It)	Sends money to another person, domestically (via ACH/RTP) or internationally (across global corridors where the ZakPay application and licensed counterparty institutions are aligned) — the P2P transfer rail providing competitive, transparent transaction costs with no hidden fees	SIR records the transfer; FUSE orchestrates settlement; destination counterparties complete local-fiat delivery in 1–3 seconds; Giving Contracts route ZUSD to charitable reserves based on transaction context (charity amount can be set by sender or default routed automatically)
SPEND (Zap-It)	Taps the ZakPay Card at any merchant accepting Visa or Mastercard — everyday commerce becomes everyday charity	SIR records the card spend; merchant receives fiat instantly; Giving Contracts route a defined portion of interchange revenue to charity reserves

> CRYPTO TALK Four user-side functions, one underlying contract surface — each action hits a Giving Contract before settlement, so charity routing happens at the protocol layer, not at the app layer.
>
> PLAIN ENGLISH No matter what a user does on ZakPay — acquire tokens, donate, send money, or spend with the card — a portion automatically flows to verified charities. The user picks the destination; the giving is built into the system.
>
> BAD ACTOR No one can disable charity routing — the Giving Contracts execute at the smart-contract level on every primary action, with no admin override, no team multisig bypass, and no policy lever to turn it off.

The ZKT-Badge — On-Chain Nonprofit Receipt

When a user executes a DONATE action through ZakPay, the protocol mints a **ZKT-Badge**: a soulbound (non-transferable) NFT representing the user's charitable contribution. The ZKT-Badge serves three functions simultaneously:

Function	What It Provides
Tax Receipt	Immutable on-chain record of the donation amount, date, recipient 501(c)(3), and Zakat Coin Organization Inc. EIN (39-4624928). The donor can present this record to the IRS or equivalent tax authority as substantiation for a charitable deduction.
Soulbound Attestation	The badge cannot be transferred, sold, or traded. It permanently resides in the wallet of the donor who initiated the contribution. This matches the legal nature of a tax receipt — a charitable deduction cannot be assigned or resold — and prevents secondary markets from emerging around tax-substantiation artifacts.
Verifiable Provenance	Any third party (auditor, tax preparer, regulator) can verify the badge on-chain without contacting ZakPay or the recipient charity. The badge proves the donation occurred, the destination was a verified nonprofit, and the amount routed correctly — with cryptographic finality.

The 501(c)(3) Fiscal Architecture

Zakat Coin Organization Inc. (EIN 39-4624928) is a registered U.S. 501(c)(3) public charity that serves as the fiscal sponsor and tax-receipt issuer for all DONATE actions executed through ZakPay. When a user donates to a downstream charity through the platform, Zakat Coin Organization Inc. processes the contribution, issues the ZKT-Badge as the official tax receipt, and routes the funds to the user-selected ZakatRated-verified nonprofit recipient. This structure provides donors with a U.S. tax-deductible receipt regardless of the downstream recipient's individual tax status — substantially expanding the universe of charities a donor can support with confidence in deduction substantiation.

Why ZakPay and ZKTC Cannot Be Separated

ZakPay can technically process payments without ZKTC. But without ZKTC, there is no SIR mechanism — no tamper-proof settlement audit trail. There is no Giving Contracts layer — charity becomes a policy choice rather than a structural guarantee. There is no ODS mechanism — supply cannot respond to real commerce. There is no

ZKT-Badge — tax receipts become trust-based promises rather than cryptographic attestations. ZKTC is not an add-on to ZakPay. It is the architectural layer that makes ZakPay trustworthy: the difference between a payment app that *promises* to give to charity and a payment system that *gives to charity by design*.

Institutional Infrastructure

Despite the complexity of the multi-partner infrastructure behind it, every ZakPay user sees one wallet, one app, one experience. The MagicBox universal adapter layer translates between sponsor banks (ACH/RTP), institutional brokerage and prime liquidity counterparties, regulated stablecoin issuance, qualified custodian crypto custody, and the FUSE orchestration engine into a single unified API. The user sends money, receives money, holds ZKTC, and donates — all from one screen. The institutional machinery is invisible.

Crypto Custody	an OCC federally chartered national trust bank serving as qualified custodian
USDC Issuance	an institutional stablecoin issuer (institutional wholesale relationship)
Institutional Brokerage	an institutional brokerage and custody provider
Domestic Rails	FBO sponsor banks (ACH and Real-Time Payments, 50-state MTL coverage via a licensed Banking-as-a-Service provider)
Card Issuance	Visa/Mastercard via the card-issuing infrastructure partner
Identity Verification	an institutional identity verification provider (KYC/KYB), a bank verification provider
NGO Verification	ZakatRated (proprietary transparency-based approval system)

What ZKTC Consumption Costs

Every action on the platform consumes a small, defined amount of ZKTC as the fuel that records and settles the instruction on-chain. The cost of each action is fixed in United States dollars and converted to a ZKTC quantity at the token's current price at the moment of the transaction. This means the dollar cost of an action stays stable and predictable, while the number of tokens consumed falls as the token's value rises and rises as the token's value falls. Consumption is a cost of using the network, not a fee collected by ZakPay; the consumed tokens are burned.

The cost is calibrated by action type, reflecting the settlement complexity of each. Provisioning a new wallet is a one-time cost of approximately one cent (USD-equivalent) per user. A domestic transfer is calibrated at approximately two-tenths of a cent. An international transfer, which carries the greatest settlement complexity, is calibrated at approximately one-half of a cent. Card transactions and charitable donations are calibrated lower still, at approximately five-hundredths of a cent, reflecting their high frequency and, in the case of donations, their mission-aligned purpose.

For transfers, the cost includes a modest component that scales with the size of the transfer, so that a larger transfer costs somewhat more than a small one. This scaling is deliberately sub-linear: the cost as a proportion of the amount moved decreases as the transfer grows, so the mechanism never operates as a percentage levy on the value transmitted. The result is a consumption model whose real-world cost is stable and whose token effect is naturally deflationary, with the strongest effect early in the token's life and a diminishing per-transaction effect at higher token prices.

Section 8 — Business Model & Revenue Architecture

How Zakat Coin Inc. generates revenue independent of token price

Zakat Coin Inc. operates as a financial-infrastructure technology company. Its revenue is generated from commerce processed through the ZakPay platform — not from token-acquisition proceeds, and not from token-price appreciation. This separation is structural and is documented across the protocol's smart-contract architecture, its corporate governance, and its accounting treatment.

Where Revenue Comes From

Revenue Stream	Description	Status
Payment Transaction Fees	Fees on domestic and international transfers executed through ZakPay (Zak-It SEND action). Targeted pricing: 1.5–2.5% of transaction value depending on corridor.	Phase 1 launch revenue source
FX & Conversion Revenue	Margin on cross-border foreign-exchange conversion at the FUSE settlement layer, including USD-to-local-currency conversion in delivery jurisdictions.	Phase 1 launch revenue source

Revenue Stream	Description	Status
Card Interchange	Interchange revenue from ZakPay Card spending (Zap-It SPEND action). Card-issuer share of merchant processing fees per Visa and Mastercard standard interchange schedules.	Phase 1 launch revenue source
API & Platform Services	Targeted future revenue from licensing the ZakPay API to third-party Islamic-finance applications, NGOs requiring institutional-grade donation rails, and enterprise integrators.	Phase 3 onward
Enterprise Services	Targeted future revenue from white-label deployments of the Giving Contracts framework for institutional charitable platforms and corporate giving programs.	Phase 4 onward

How Token-Acquisition Proceeds Are Allocated

USDC received from token-acquisition activity (ACQUIRE actions and Donation Coin Offering participation) is allocated according to a structural five-way split — 80% liquidity, 10% team liquidity, 5% charitable backing, 2.5% custody and safeguarding, and 2.5% operations — applied at the smart-contract level and visible on the Public Utility Dashboard:

Allocation	Share	Purpose
Liquidity Pool (LP)	80%	Routed to the primary ZKTC/ZUSD AMM liquidity pool to support payment-grade pool depth, FLIP depth-provisioning capacity, and stable launch pricing.
Team Liquidity Pool (TLP)	10%	Builds the dedicated reserve that funds vested Team RTU cash-outs (Section 28 — cash-outs burn the ZKTC tokens rather than transferring them to the open market).
HTG Piggy Bank (HPB)	5%	Accumulates real USDC to back Hold-to-Give charitable matches. This is one of several inputs to the HPB (see below); charitable matches are paid only from USDC the HPB already holds.

Allocation	Share	Purpose
Custody & Safeguarding	2.5%	Funds regulated qualified-custody and insurance for deposited assets (institutional custody and brokerage providers). This allocation is spent to safeguard deposited assets, not retained as company revenue.
Operations	2.5%	Funds the operating costs of the on-chain protocol layer: independent smart-contract audits, oracle subscriptions, security monitoring, bug-bounty pools, and smart-contract maintenance.

How Token-Purchase Proceeds Are Used

ZakPay Inc. earns its revenue from transaction fees, not from token-sale proceeds. Of the USDC deposited to acquire ZKTC, a disclosed 2.5% funds general protocol operations; the remaining 97.5% is routed to purposes that serve the ecosystem and its participants — market liquidity, team liquidity settled separately from the public pool, charitable backing held in real USDC, and the regulated custody and insurance that safeguards deposited assets. The custody and safeguarding allocation is a protective cost spent on behalf of participants, not company profit.

What This Structure Implies

The acquisition-proceeds allocation is designed so that token sales fund **protocol infrastructure** rather than discretionary corporate expenditure:

- **The 80% LP allocation** directly supports user experience — deep liquidity means lower slippage, faster settlement, and protocol stability through volatility events.
- **The 10% TLP allocation** creates a structural alternative to open-market insider sales. Team RTU cash-outs draw from TLP and burn the associated tokens, removing the conventional insider-unlock-dump pattern from the protocol's market dynamics.
- **The 10% Operating Token Infrastructure allocation** ensures the on-chain layer is funded independently of commerce revenue. Audits, oracle costs, and security operations are recurring expenses; this allocation guarantees they are resourced over time.

- **Charitable funding flows separately** through the Giving Contracts on every protocol transaction (Section 5), not from acquisition proceeds. The two flows are structurally distinct.
- **Founders Reserve and Charity Reserve** are operationally-allocated token pools, not corporate working capital. They are not drawn down for general company operations.

Section 9 — The Problem Worth Solving

Trust-based finance was not built for instant, transparent, charitable giving

Universal Purpose

Zakat Coin introduces a global digital utility for charitable giving — designed for Muslims and non-Muslims alike. The platform makes donating seamless, transparent, and efficient, while preserving the sacred principles that guide Islamic charitable practice. At the same time, it extends usability to any individual or organization committed to philanthropy, creating a universal giving ecosystem powered by blockchain technology.

The Friction in Traditional Charity

Traditional Charity Challenges	The ZakPay Solution
Administrative costs of 5–35% absorbed before funds reach beneficiaries	Low transaction fees and direct on-chain settlement to verified recipients
Geographic limitations preventing cross-border giving	Global orchestration capability — FUSE can route to any country where the ZakPay application is accessible and licensed counterparty institutions are aligned
Lack of transparency and donor accountability	Immutable blockchain records — every donation traceable on-chain

Traditional Charity Challenges	The ZakPay Solution
Slow settlement — days to weeks for international transfers	1–3 second orchestrated settlement to local fiat via the FUSE engine and partner counterparties
Compliance uncertainty around Islamic finance principles	Shariah-reviewed by internationally recognized scholars, under continuing ZCBS oversight
Charitable mechanisms denominated in volatile tokens	All distributions in ZUSD (USDC-backed stablecoin) — charities receive stable value

What Zakat Coin Brings

Zakat Coin is the first system to embody an **Automated Donation and Distribution Protocol**. The act of acquiring, holding, or selling ZKTC is never neutral — every action can trigger a charitable consequence, encoded immutably into the rails of the network. Combined with the ZakPay payment platform, this creates the first financial infrastructure where charity is not an afterthought added to commerce, but a structural property of the protocol itself.

Section 10 — Global Market Opportunity

The intersection of remittance, Islamic finance, and charitable giving

ZakPay operates at the intersection of three large and growing markets: global remittance, Islamic finance, and charitable giving. Each market on its own is significant. The intersection — a Shariah-compliant payment platform that routes structural charity on every transaction — is currently underserved.

The Three Markets That Define ZakPay's Opportunity

Market	Scale	Why ZakPay Is Positioned For It
Global Remittance	Hundreds of billions of dollars sent across borders annually, with the largest corridors flowing into MENA, South Asia, and Sub-Saharan Africa.	ZakPay's FUSE settlement engine targets 1–3 second international delivery on regulated rails — addressing the speed and cost friction that defines conventional remittance.
Islamic Finance	A multi-trillion-dollar global industry covering banking, capital markets, and insurance, with continued double-digit growth in core markets.	ZakPay is Shariah-compliant by design with absolute ZCBS veto authority — structurally aligned with the principles that govern Islamic finance, not retrofitted to them.
Charitable Giving	Global charitable giving exceeds hundreds of billions annually, with significant Islamic charitable giving (zakat, sadaqah, waqf) flowing through informal and institutional channels.	ZakPay's Giving Contracts route charity structurally on every transaction class, with on-chain ZKT-Badge tax receipts from a U.S. 501(c)(3) fiscal sponsor.

The Demographic Tailwind

The global Muslim population is approximately 1.9 billion and is one of the fastest-growing demographic groups worldwide. Digital payments adoption in the largest Muslim-majority markets — including Indonesia, Pakistan, Bangladesh, Egypt, and Turkey — continues to outpace the global average. Mobile-first banking infrastructure is the default in these markets, not a transition state.

ZakPay is designed for this user base: Shariah-compliant by design, mobile-first by interface, instant-settlement by architecture. The product fit is engineered into every layer of the protocol.

Why the Intersection Is Underserved

Conventional remittance platforms are not Shariah-compliant and do not route charity. Conventional charitable platforms do not provide cross-border instant settlement and do not function as everyday payment infrastructure. Conventional crypto remittance rails do not provide Shariah governance, do not provide tax-deductible receipts, and do not provide consumer-grade UX. The intersection of these three capabilities — addressed in ZakPay — is structurally underserved.

The Targeted Opportunity

ZakPay's go-to-market focus is the intersection where these three markets overlap: **Muslim-community payments and remittance with embedded charitable consequence**. The Team is not trying to compete with general-purpose payment platforms in the U.S. domestic market or with general-purpose crypto wallets. The platform is designed for the user who values Shariah compliance, charitable impact, and cross-border instant settlement as a combined product — a user the existing financial infrastructure does not serve as a unified experience.

Section 11 — Network Effects & Ecosystem Growth

How the ecosystem becomes stronger with each participant added

The ZakPay ecosystem is designed to exhibit positive feedback dynamics across multiple participant categories. As each category grows, the value proposition for every other category strengthens. This is the conventional definition of a network effect, applied to the specific architecture of charitable payment infrastructure.

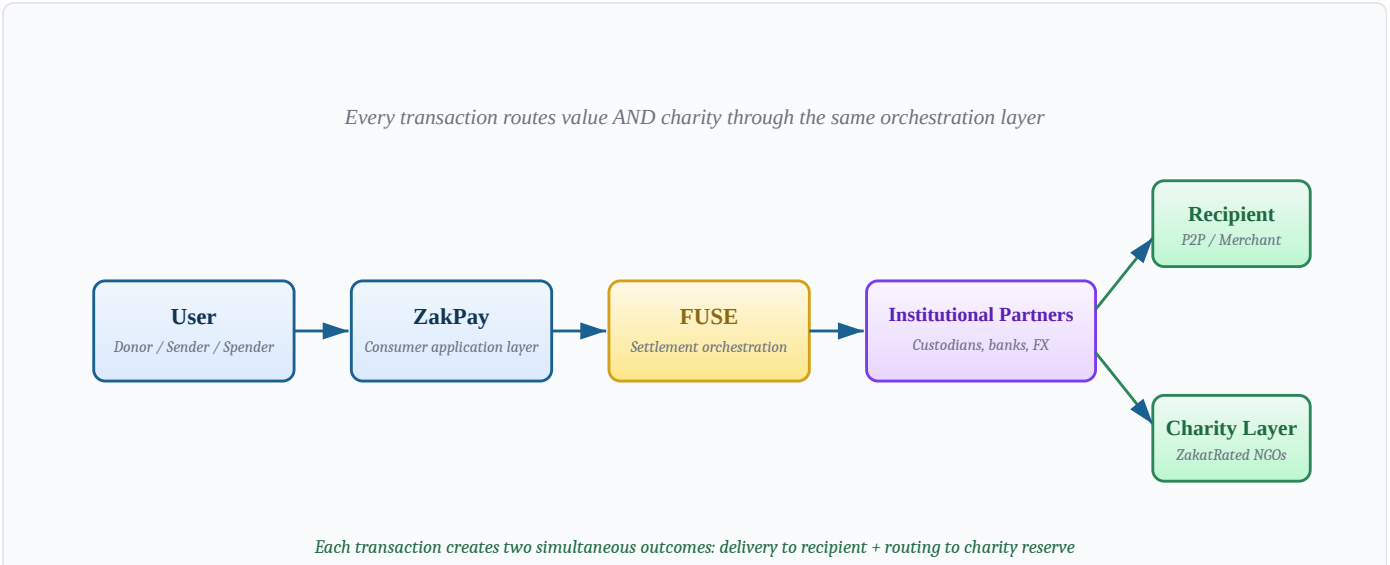

Figure A ·ZakPay Ecosystem Overview — user, application, orchestration, partners, and the dual-outcome charity layer

The Six Participant Categories

Participant	What They Bring	What They Receive
Users (Donors / Senders / Spenders)	Transaction volume, charity contributions, card spend	Instant settlement, Shariah compliance, tax-deductible receipts, structural charity
Merchants	Card acceptance, transaction volume, real-world utility for Zap-It	Access to a growing user base with consistent Shariah-aligned spending intent
Charities (ZakatRated NGOs)	Verified disbursement endpoints, real-world impact, donor confidence	Instant ZUSD funding, recurring giving flows, structural revenue from Giving Contracts
Settlement Partners (Banks, FX Providers)	Regulated rails, banking access, FX corridors, off-ramp capacity	Transaction volume from a growing payment platform, integration into a compliant ecosystem

Participant	What They Bring	What They Receive
Liquidity Providers	Pool depth on AMM, supports payment-grade UX	Yield from trading activity, exposure to a structurally deflationary token
Scholars & Compliance Reviewers	Shariah review, fatwa authority, jurisprudential rigor	Influence over a leading Shariah-compliant payment platform in the consumer market

The Positive Feedback Loops

Three distinct network effects compound across the ecosystem:

- **User ↔ Merchant.** More users on ZakPay create more demand for Zap-It card acceptance, attracting more merchants to integrate or accept the card. More merchant acceptance creates more daily utility for users, driving further user growth.
- **User ↔ Charity.** More users on ZakPay create more donation volume to ZakatRated charities through DONATE, embedded Giving Contracts, and card-spend routing. More charity-funding capacity attracts more NGOs to apply for ZakatRated verification, expanding the destination network donors can give to.
- **Volume ↔ Token Health.** More transactions through ZakPay generate more SIR burns (deflationary), more ODS activation (supply tied to real commerce), and more FLOP overflow (buying and burning ZKTC, topping up charity, and refilling the FLIP reserve without taxing user pools). Each transaction strengthens the protocol's structural integrity.

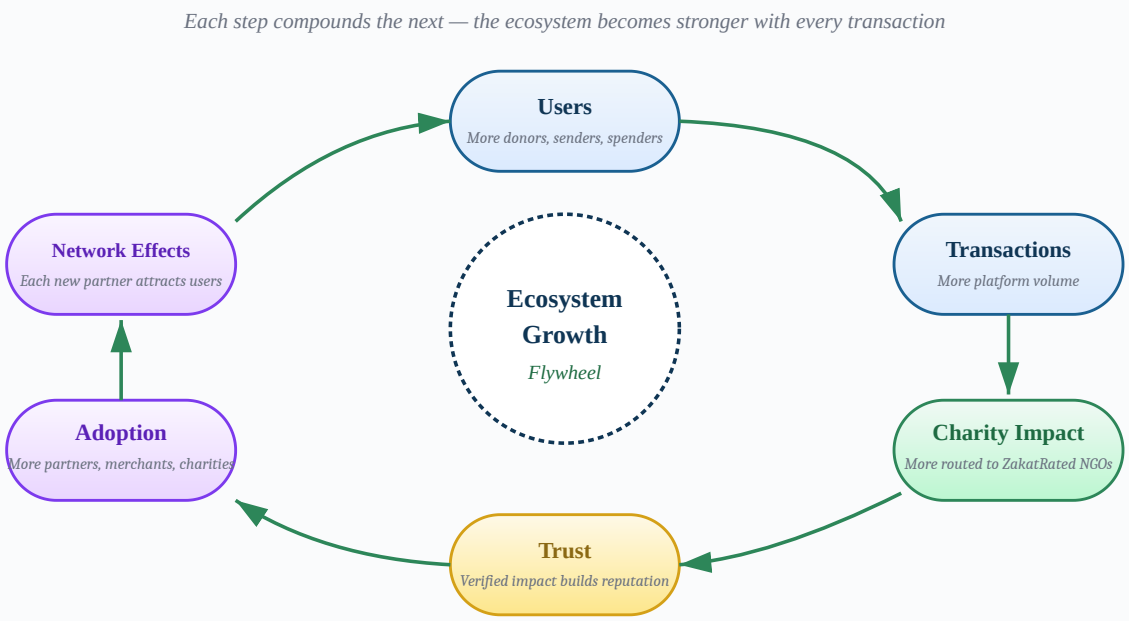

Figure G · Ecosystem Growth Flywheel — the compounding loop between users, transactions, impact, trust, and adoption

Why Network Effects Create Long-Term Defensibility

The ZakPay ecosystem is designed to become structurally harder to replicate as it grows. A competitor entering the market in Year 3 would face a charity network of hundreds of ZakatRated NGOs already onboarded, banking partnerships established across MENA and Muslim-majority corridors, ZCBS jurisprudential authority recognized by the community, on-chain proof of operational integrity across millions of completed transactions, and a tax-receipt artifact (ZKT-Badge) integrated into U.S. donor tax workflows. Each of these takes years to build from scratch. The protocol's value to each participant grows as the total participant base grows — the textbook definition of a defensible network business.

Section 12 — ZakPay Competitive Positioning

How ZakPay compares to existing categories of charitable payment and remittance solutions

This section positions ZakPay (the platform) against the broader market categories in which it competes. The comparison focuses on ZakPay's product capabilities relative to **category-level capabilities** typical of established players in each segment; no specific competitor is named, as the Team's intent is to characterize the structural gap ZakPay fills rather than to draw individual comparisons. ZakPay's principal product differentiation is the integration of charitable consequence into every transaction class through smart-contract enforced Giving Contracts, regardless of whether the user explicitly opts in to charity.

ZakPay vs. Traditional Charitable Giving Platforms

Capability	ZakPay	Typical Charitable Giving Platforms
Direct charity transfers	Yes — seconds finality through FUSE	Yes — typically days to weeks
On-chain tax receipt	Yes — ZKT-Badge soulbound NFT, blockchain-verified	No — email or PDF receipt only
501(c)(3) fiscal sponsor	Yes — Zakat Coin Organization Inc.	Varies; many require nonprofit registration with the platform
Verified nonprofit network	ZakatRated verification with on-chain audit trail	Platform-specific verification, no public audit trail
Shariah-compliance review	Yes — ZCBS oversight with absolute veto authority	Generally none
Cross-border charity delivery	Targeted MENA + Muslim-majority markets at launch; expanding globally	Generally restricted to platform-supported jurisdictions

Capability	ZakPay	Typical Charitable Giving Platforms
Donor anonymity option	Yes — privacy preserved while receipt remains verifiable	Limited; varies by platform
Transaction structure	Defined portion via Giving Contracts on every transaction class	Standard platform fees on opt-in donations only

ZakPay vs. Remittance & Payment Platforms

Capability	ZakPay	Typical Remittance / Payment Platforms
Domestic P2P transfer	Yes — ACH / RTP, seconds finality	Yes — minutes to hours typical
International remittance reach	Targeted MENA + Muslim-majority markets at launch; expanding	Varies widely — from few corridors to broad coverage
Settlement speed (international)	1–3 seconds (FUSE)	Minutes to days typical
Domestic transaction fee	**1.5–2.5%**	Varies widely by provider and corridor
International transaction fee	**1.5–2.5%**	Varies widely; high-fee corridors common
Embedded charity routing	Yes — structural on every transaction	No
Card spend at merchants	Yes — ZakPay Card (Visa / Mastercard)	Varies by provider

Capability	ZakPay	Typical Remittance / Payment Platforms
Shariah compliance	Yes — ZCBS certified	Generally none
On-chain audit trail	Yes — SIR records publicly verifiable	Internal records only
Consumer-facing app	Yes	Yes — varies in design and capability

ZakPay vs. Crypto Remittance & Charity Rails

Capability	ZakPay	Typical Crypto Remittance Rails
End-user experience	Consumer app + card; fiat-denominated UX	Generally developer-facing or self-custody required
Settlement speed	1–3 seconds (FUSE)	Network-dependent; typically seconds to minutes
Embedded charity protocol	Yes — structural via Giving Contracts	No — charity is application-layer, not protocol-layer
Compliant tax receipts	Yes — ZKT-Badge from U.S. 501(c)(3)	No — receipt is donor's responsibility
Shariah compliance	Yes	Generally none
Custodial & KYC compliant	Yes — federally-chartered qualified custodian + KYC	Mixed; many are non-custodial / self-custody
Fiat onramp / offramp	Native, integrated	Via third-party partners

ZakPay's Structural Differentiation

The combination ZakPay offers does not exist elsewhere in the market: **(1)** consumer-grade payment app with seconds-finality international remittance, **(2)** structural charity routing on every transaction class through smart-contract enforced Giving Contracts, **(3)** on-chain tax-deductible receipts via ZKT-Badge soulbound NFTs from a U.S. 501(c)(3) fiscal sponsor, and **(4)** Shariah-compliant by design with absolute ZCBS veto authority. Existing categories of providers offer subsets of this capability; none integrate all four.

PART IV — UNDERLYING TECHNOLOGY

FUSE, the patent, and the settlement architecture

Section 13 — FUSE: Settlement Orchestration Engine

The bridge between blockchain instruction and real-world delivery

FUSE (Fiat Universal Settlement Engine) is the patent-protected orchestration engine that coordinates blockchain payment instructions with regulated banking and payment counterparties to enable real-world fiat delivery in 1–3 seconds across any country where the ZakPay application is accessible and where licensed counterparty institutions are aligned. FUSE is the operational core of ZakPay — the orchestration layer that makes "send money internationally" actually work in seconds rather than days. **FUSE itself does not perform recipient settlement**; it routes, governs, and audits the instruction. Settlement is executed by destination institutions licensed in each jurisdiction.

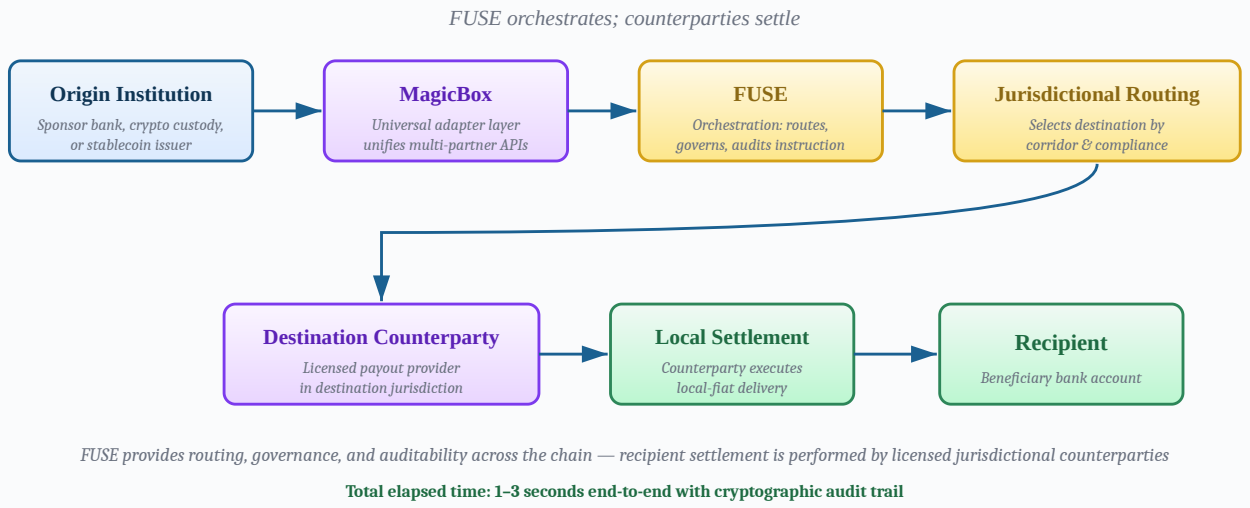

Figure C · FUSE Settlement Orchestration Flow — orchestration on the protocol side, settlement on the counterparty side

The SIR Lifecycle

The SIR (Settlement Instruction Record) is the on-chain artifact that proves a ZakPay transaction was initiated, executed correctly, and settled. SIRs are the unit of utility consumption in the protocol — every transaction creates one, every settlement burns one. This is the core mechanism subject to the patent application via independent IP counsel.

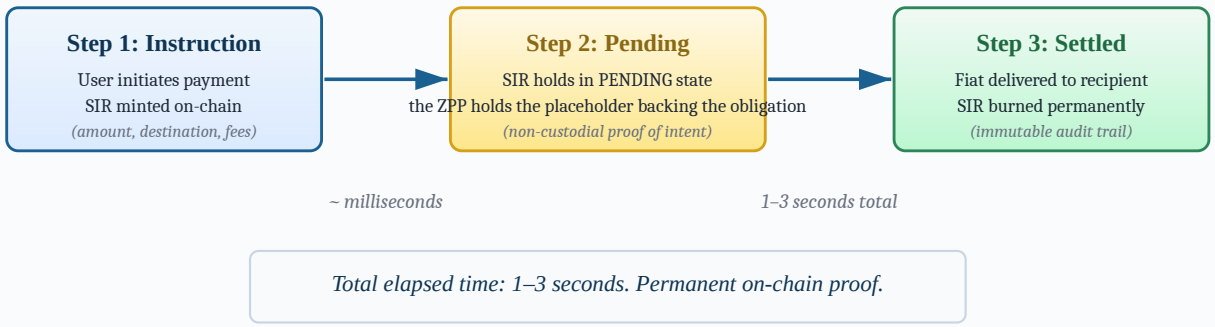

Figure 1 · The SIR Lifecycle — from instruction to settlement

The Non-Custodial Guarantee

Because ZakPay is the instruction layer — not the asset layer — users retain beneficial ownership of their funds at all times. a federally chartered qualified custodian custodies the crypto assets. a licensed Banking-as-a-Service provider (and partner FBO sponsor banks) hold fiat in FBO accounts. ZakPay orchestrates the settlement instruction. The SIR is the on-chain proof that ZakPay executed the instruction correctly. This architecture satisfies the patent's non-custodial design requirement and the Shariah requirement that operational uncertainty (*gharar*) be minimized at every layer.

ZPP — The Asset-Layer Mirror

The ZKTC Placeholder Pool (ZPP) is a multi-signature holding layer for matched-release ZKTC. It sits between two states of the token. When a user acquires ZKTC, a multi-signature match releases the corresponding amount from the Founders Reserve into the ZPP; at this stage the ZKTC waits in the pool, matched but not yet claimed by any settlement. It is only when a Settlement Instruction Record takes governance of a waiting token — representing a specific payment instruction now in flight — that the ZKTC becomes a placeholder, effectively already burned, awaiting only FUSE settlement. Outside the ZPP, ZKTC is a utility token; inside the ZPP under an active SIR, it is a placeholder holding its position until settlement resolves.

For every SIR in flight, the ZPP holds the corresponding ZKTC. When the SIR settles, that ZKTC burns. When the SIR reverses on a failed settlement, governance is released and the ZKTC returns to the waiting state in the ZPP, available to be claimed by a future SIR. The relationship between SIR state and ZPP balance is enforced by mathematical invariant — see Section 16.

Why Settlement in Three Seconds Matters

Conventional international payment rails take days to weeks. Reversals can occur up to 60 days after settlement. Recipients across the world must plan around this uncertainty. FUSE collapses this to seconds with cryptographic finality — meaning a charity in East Africa receiving a Zak-It transfer from a donor in North America can verify, accept, and deploy those funds the same day. This is operational impact at the architectural level.

Section 14 — Intellectual Property: The FUSE Patent & License

The Inventor holds the patent; Zakat Coin holds an executed, irrevocable license

The intellectual property behind ZKTC is described by two facts, both true in the present tense.

First: the FUSE settlement architecture — the SIR-based orchestration at the core of this protocol — is patented, and the patent is currently held by the Inventor. The FUSE invention originated directly from the work of building the Zakat Coin ecosystem; it was not acquired from an unrelated party, but emerged from solving this protocol's own settlement problem.

Second: the Inventor has granted Zakat Coin Inc. (DBA ZakPay) an executed, irrevocable, perpetual, royalty-free license to the FUSE patent. The license is structured to survive any change of control and any future assignment of the patent, so the ecosystem's access to FUSE does not depend on who holds the patent at any given time. Ecosystem continuity is secured by the license, independent of the patent's ownership.

Why This Structure

Holding the patent separately from the operating company, while granting the operating company an executed irrevocable license, insulates the core IP from any future corporate restructuring or financing event affecting Zakat Coin Inc. The protocol's access to its foundational technology is contractually secured and does not lapse if

the operating company's circumstances change.

Section 15 — SIR & ZPP Mathematical Invariants

The protocol's self-audit equations — documented in the Technical Protocol Appendix

The protocol enforces three mathematical invariants that mirror the SIR (Settlement Instruction Record) state against the ZPP (ZKTC Placeholder Pool) token balance at every block height. These invariants are continuously verifiable on-chain and form the protocol's structural self-audit layer.

- **Bounded-Reserve Conservation** — the ZPP is maintained as a bounded settlement reserve rather than a pool that mirrors cumulative sales. Its balance moves only through settlement burns, reversals, and protocol-funded replenishment, and is held within fixed bounds enforced on-chain. The reserve is seeded from the Founders allocation; no charitable allocation is ever a source.
- **ZPP State Equation** — ZPP balance equals cumulative matched releases minus in-flight obligations, accounting for reversals and settlements.
- **SIR-ZPP Mirror Symmetry** — every SIR's state maps to one of three token locations (contract, ZPP, burn address); no fourth state is permitted.

The smart contract reverts on any inconsistency between SIR state and token location — the protocol is self-policing. Continuous on-chain verification is displayed on the Public Utility Dashboard (Section 35). Full equations and audit trail mechanics are documented in **Appendix A.1**.

Section 16 — Modular Smart Contract Architecture

Many small contracts working together — documented in the Technical Protocol Appendix

The Zakat Coin protocol is implemented as a network of interconnected smart contracts, each with a specific responsibility — not as a single monolithic contract handling all functions. This is a deliberate architectural choice grounded in EVM technical constraints and industry best practice across mature DeFi protocols.

Modular architecture supports targeted audits, independent upgradeability during the pre-launch phase, clean composability between FUSE / MagicBox / ZakPay platform contracts, and reduced attack surface per contract. The pattern aligns with Aave V3, Uniswap V4, MakerDAO, Compound, and Gnosis Safe.

Full architectural rationale, EIP-2535 alignment, and industry precedent are documented in **Appendix A.2**.

Section 17 — The Mutability-to-Immutability Strategy

The protocol begins mutable. It ends immutable. The transition is sequenced — documented in the Technical Protocol Appendix

The protocol operates in two governance phases. During the pre-launch maturity period (prior to the immutability transition at mainnet launch), individual contracts (excluding the already-immutable ZKTC token) are upgradeable via multi-signature governance combining founders and Board of Scholars members. This window allows audit remediation, scholar refinement, regulatory feedback integration, and operational learning to be reflected in the protocol.

At Public Mainnet Launch, the protocol transitions to immutability. Upgrade authorities are renounced via standard mechanisms; multi-signature keys are ceremonially decommissioned. Once immutable, protocol behavior is fixed at the EVM level.

Certain protocol invariants — the 14.25 billion operational supply cap, the bounded ZPP settlement-reserve limits, the 500M Founders Reserve Release Cap, the three Mathematical Invariants, and the named reserve allocations — are immutable from the moment of deployment, independent of the renunciation ceremony.

Full transition mechanics, renunciation sequence, and the on-chain notarization ceremony are documented in **Appendix A.3**.

Section 18 — The Operational Supply Architecture

Every token has a job. Every job has a token.

The entire operational supply of ZKTC is hard-capped at **14,250,000,000 tokens**. This number is locked at the protocol level and cannot be expanded by management decision, board vote, or any administrative action. Supply growth occurs only through the ODS mechanism — tokens activated from operational reserves in proportion to real ZakPay platform commerce. There is no other path to supply expansion.

The 14.25 billion operational supply is apportioned across four named reserves — the Founders Reserve, the Charity Reserve, the Team RTU Reserve, and the Ecosystem & Partnerships reserve — each enforced as an on-chain allocation wall. The full allocation table, reserve functions, vesting terms, and the Founders Reserve Release Cap are set out canonically in **Section 19 (Tokenomics Distribution & Vesting)**.

What Stays Locked Forever

The 14.25 billion operational supply cap is enforced at the smart contract level. The ZPP is maintained as a bounded settlement reserve, seeded from the Founders allocation, with its floor and cap hard-coded. The ZPP bounded-reserve limits are `require()` statements that revert any transaction attempting to exceed them, and the Charity Reserve is firewalled from settlement use entirely. These are not policy commitments — they are architectural constants that cannot be changed even by the multi-signature upgrade authority during the protocol's pre-launch mutable phase. Changing them would require deploying entirely new contracts to entirely new addresses, which would constitute a separate protocol, not an upgrade.

How Supply Enters Circulation

ZKTC tokens enter active circulation through exactly two legitimate paths:

- **Acquisition through ZakPay:** Participants acquire ZKTC through the ZakPay platform during the Donation Coin Offering phase, subject to vesting schedules. Tokens transfer to participant custody at a federally chartered qualified custodian. The acquisition USDC routes proportionally to liquidity pools and charitable reserves — zero portion becomes company revenue.

- **ODS activation:** After Public Launch, the On Demand Supply engine activates tokens on the completed settlement *event* — the real ZakPay transaction itself, not the fee revenue it generates. The settlement releasing supply and the revenue funding pools are two decoupled consequences of one transaction. No commerce — no activation. Tokens are earned into existence by platform utility, not issued by management.

Management cannot expand supply. Insiders cannot expand supply. Supply grows only when the platform earns it through real, completed transactions.

Figure B ·ZKTC Utility Lifecycle — acquisition through permanent removal via SIR consumption

How Supply Leaves Circulation

Just as importantly, ZKTC has structural mechanisms for permanent supply destruction. Every SIR (Settlement Instruction Record) created during a ZakPay transaction is burned upon settlement confirmation — meaning every real-world payment processed by ZakPay literally consumes ZKTC supply. RTU cashouts trigger burn-on-cashout: when a vested team member sells, the corresponding ZKTC is permanently destroyed. FLOP overflow distributions include a permanent burn allocation. Over time, with sustained platform commerce, the protocol exhibits net deflationary behavior.

PART V — TOKENOMICS

Supply, allocation, vesting, and launch gating

Section 19 — Tokenomics Distribution & Vesting

Transparent allocation, on-chain reserve walls, and the Founders Reserve Release Cap

ZKTC's total operational supply cap is 14.25 billion tokens, enforced at the smart-contract level. The allocation below shows how this supply is structurally apportioned across the protocol's functional reserves. Note that **"Team" allocation** in ZKTC refers to RTU (Restricted Token Units) subject to burn-on-cashout: every team member sale permanently destroys the corresponding ZKTC, meaning insider liquidation is structurally deflationary rather than dilutive.

Operational Supply Allocation

Reserve	Allocation	Lockup & Release	Function
Founders Reserve	38.6% (5,500,000,000 ZKTC)	Locked. Releases only to fund protocol mechanics — ZPP matched releases, FLIP depth provisioning, ODS supplemental supply, and RTU vesting. Matched releases from this reserve are subject to the **Founders Reserve Release Cap** (see below). Not transferable to external parties.	Primary operational source pool for live protocol mechanics

Reserve	Allocation	Lockup & Release	Function
Charity Reserve	42.1% (6,000,000,000 ZKTC)	Permanent charitable reserve, dedicated solely to charity (HPB and direct charitable distribution). It is firewalled from settlement use and is never a source of settlement fuel. Releases under Zakat Coin Organization Inc. and ZCBS oversight.	Backs all charitable token releases (HPB/ODC); secondary matched-release source after the cap
Team RTU Reserve	14.0% (2,000,000,000 ZKTC)	Restricted Token Units issued under documented vesting agreements subject to ZCBS oversight. All RTU is subject to burn-on-cashout — liquidated tokens are permanently destroyed, never transferred to a buyer. Team liquidity is settled against the segregated Team Liquidity Pool (Section 28), not the public market.	Long-term team alignment with protocol success
Ecosystem & Partnerships	5.3% (750,000,000 ZKTC)	Released under documented agreements subject to ZCBS review. Allocated to ecosystem partnerships, marketing distributions, and strategic relationships with infrastructure partners and verified NGOs.	Ecosystem development, partnerships, and strategic growth

The Founders Reserve Release Cap

The ZKTC Placeholder Pool is a bounded settlement reserve, seeded from the Founders allocation and held for the sole purpose of provisioning settlement. It is not an uncapped pool that grows with every sale; it is a fixed-size reserve maintained within defined bounds that are enforced at the smart-contract level and verifiable on-chain. As settlement consumes and burns ZKTC from the reserve, the reserve is replenished through the protocol's own liquidity-overflow mechanism rather than by drawing on any charitable allocation. The Charity Reserve is never a source of settlement fuel; it funds charity alone.

What Makes This Tokenomics Different

Three structural properties distinguish the ZKTC allocation from conventional token-sale tokenomics. **First**, all USDC paid into ACQUIRE flows to liquidity pools and charitable reserves — *zero* percent constitutes company revenue. The Team is compensated from RTU vesting under ZCBS oversight, not from token-acquisition proceeds. **Second**, Team RTU is subject to burn-on-cashout: liquidation by insiders reduces total supply, removing the dilution mechanism that distinguishes typical insider behavior from holder interests. **Third**, all reserve allocations are visible on-chain through the Public Utility Dashboard (Section 35); allocation walls are smart-contract enforced rather than policy promises.

> CRYPTO TALK Team tokens burn on exit and all acquisition proceeds route to LP + charity — no team-equity dilution, no rug-pull surface, and insider liquidation is settled against a segregated pool rather than dumped on the public market.
>
> PLAIN ENGLISH When the Team sells their tokens, those tokens are destroyed rather than added to circulation. Money from new token acquisitions goes to charity and to keeping the system liquid — not into Team pockets.
>
> BAD ACTOR Team can't rug-pull because their tokens burn rather than transfer when sold; team liquidity settles against the segregated Team Liquidity Pool rather than the public market; allocation walls are on-chain constants, not policy choices.

Section 20 — The Tiered Float Architecture

Lockups are enforced by smart contract, and each phase's funds are committed to a defined operational purpose.

The central objective of the Donation Coin Offering (DCO) is to fund the operational buildout of the Zakat Coin ecosystem — the settlement engine, the platform, custody and compliance integrations, and the charitable infrastructure — through participants who acquire ZKTC to use it, phased by the protocol's operational maturity at the point of entry. Contributions are committed to defined operational purposes rather than held as speculative capital, and all lockups are enforced at the smart-contract level.

Participation Phases and Lockups

Participation falls into three phases, distinguished by how early each entered relative to the protocol's operational maturity and by the lockup each accepted. Earliest participants (the Private DCO phase) entered before a working platform, public market, or completed audit existed; their contribution funded foundational infrastructure and they accept the longest post-launch lockups. Pre-sale phase participants entered as the platform approached launch, with audits underway; their tokens remain locked through the post-launch stabilization window. Public-market participants enter a live, audited system with operational price discovery and hold immediately liquid tokens with no lockup. All lockups are enforced at the smart-contract level; the specific release terms for each phase are set out in the participants' respective agreements under ZCBS oversight.

The Release Schedule

Figure 2 · Release schedule — earlier phases unlock after later phases, by smart-contract lockup

Entry Phase and Operational Commitment

Each participation phase corresponds to a different stage of the protocol's operational maturity, with a correspondingly different lockup period:

- **Earliest participants (Private DCO):** Entered before a working platform, public market, or completed audit existed. Their funds built the foundational infrastructure, and their tokens carry the longest lockup.
- **Middle participants (Public Pre-Sale):** Entered as the platform approached launch, with audits in progress. Their funds support launch-period scaling, and their tokens are locked through the post-launch stabilization window.

- **Latest participants (Public Market):** Enter a live system with completed audits and operational price discovery. Their tokens are immediately liquid, with no lockup.

The lockup length corresponds to how early a participant entered relative to the protocol's operational maturity: earlier entry carries a longer lockup, and later entry — into a live, audited system — carries none. Lockups are enforced entirely at the smart-contract level.

Why This Is Shariah-Aligned

Each cohort's commitment carries operational consequence:

- Private DCO funded the foundational infrastructure buildout (FUSE engine, MagicBox, ZakPay platform engineering, the qualified custodian and an institutional brokerage and custody provider integrations).
- Public Pre-Sale funds the AMM bootstrap and operational scaling through the launch period.
- Public Market activity activates the live operational economy — commerce, settlement, charity routing.

The funds are not speculative capital awaiting appreciation — each cohort's contribution has a concrete operational destination. *Gharar* (operational uncertainty) is minimized at every cohort level. This is the operational substance underlying each cohort's participation in the ecosystem's utility.

Section 21 — Milestone Proof & Public Launch Gating

What must be true before ZKTC publicly launches

This section is written for two audiences: **(1) the reader evaluating Zakat Coin today**, who deserves to know what the Team has committed to before launching publicly; and **(2) the reader evaluating Zakat Coin in the future**, who can use this section as a checklist against the observable public record. If ZKTC has publicly launched, this section tells you which structural milestones have been met. If ZKTC has not yet publicly launched, this section tells you why and what is being completed.

The Principle: Milestones Are Proof, Not Promises

The Team has committed to the following principle as a matter of structural discipline rather than marketing convenience: **ZKTC will not be released into a public presale, and ZakPay will not be publicly launched, until each of the milestones below is independently verifiable in the public record.** This is not a roadmap goal — it is a release-gate. The mutable-phase governance authority (multi-signature) will not approve a public release until the gates are cleared.

Phase-by-Phase Milestone Gates

Phase	Milestone Gate	What it Proves to the Reader
Pre-Private-Sale	Joint Shariah fatwa for ZKTC and ZUSD issued and ratified by ZCBS	The economic design is Shariah-compliant by considered scholarly judgment, not by self-certification.
Pre-Private-Sale	Non-provisional patent filed with USPTO via outside IP counsel	The protocol's novel mechanisms are documented in a verifiable public record (USPTO filing), establishing prior art and protecting against derivative imitation.
Private Sale Conclusion	Matched-release activation capital generated (Founders Reserve into ZKTC Placeholder Pool)	The protocol has the operational reserves required to seed FLIP depth provisioning, FUSE bridging, and partner integration.
Pre-Public-Presale	FUSE (Fiat Universal Settlement Engine) built and tested with real transactions	The core payment-settlement primitive works. Settlement is not a whitepaper promise; it is an executed transaction with verifiable on-chain and bank-rail records.
Pre-Public-Presale	SIR (Settlement Instruction Records) lifecycle operational	The protocol's audit, charity-routing, and tax-receipt logic is executing on real transactions, not test data.

Phase	Milestone Gate	What it Proves to the Reader
Pre-Public-Presale	ZakPay app executes real domestic transfers (ACH / RTP)	Domestic payment-platform capability is verified through institutional banking rails.
Pre-Public-Presale	ZakPay app executes real international transfers	Cross-border remittance is operational through partner BFIs (Banking and Financial Institutions). At least one corridor live and audited.
Pre-Public-Launch	Smart-contract audit completed (Section 34) with public report	Independent third-party verification of all on-chain code.
Pre-Public-Launch	Off-ramp partners secured in **targeted MENA and Muslim-majority markets**	Global capability is real where it matters most for the user base. The Team does not claim 150-country coverage at launch; it claims coverage in markets that match the actual product-market fit.
Pre-Public-Launch	Minimum **100 ZakatRated charities** onboarded	The nonprofit wing has built genuine network capacity. The charity infrastructure described in this whitepaper is not a single-organization fiscal sponsor with theoretical reach; it is an active network of vetted recipients.

The Honest Read: BFI-to-BFI Requires Partners

The Team is being explicit about a structural truth that many crypto projects obscure: **the technology described in this whitepaper is designed for BFI-to-BFI integration, and BFI integration requires partner agreements that the Team cannot build alone.** The protocol's settlement layer (FUSE), card-issuing capability (the card-issuing infrastructure partner, a backup card-issuing partner, a global card-issuing scale provider), and off-ramp distribution all depend on institutional partnerships. The Team will not publicly launch ZKTC until these partnerships are in place in target markets. This is not a delay in ambition — it is a refusal to launch until the technology has somewhere real to land.

What the Reader Can Verify

If you are reading this whitepaper after the events have occurred, you can verify the following independently:

- **USPTO patent record** — Application No. 19/640,087 is publicly searchable.
- **BscScan contract record** — The ZKTC token contract on BNB Smart Chain is publicly visible and shows token holder distribution.
- **Audit reports** — Published at `audits.zakatcoin.com` upon completion of audit cycle (Section 34).
- **Public Utility Dashboard** — Real-time on-chain proof of reserves, SIR records, and charity disbursement (Section 35).
- **App Store / Google Play presence** — If ZakPay is downloadable, the app has passed platform review.
- **ZakatRated NGO directory** — Published list of onboarded charities, verifiable through partner due-diligence records.

The Team's commitment is that **each of these proofs corresponds to a structural milestone gate**. The reader does not have to take the whitepaper on faith — they can check the public record.

PART VI — MARKET & LIQUIDITY MECHANICS

Settlement-and-disbursement liquidity provisioning

Section 22 — FLIP: Liquidity Depth Provisioning

When the pool needs depth, FLIP delivers it — automatically

FLIP (Founders Liquidity Injection Protocol) is the automated mechanism that maintains settlement-grade depth in the ZKTC liquidity pool. It triggers on a settlement-depth and slippage threshold — never on token price. When pool depth falls below the level required for payment-grade and charitable-disbursement transactions to settle without prohibitive slippage, FLIP deploys USDC from a dedicated FLIP reserve into the AMM to restore depth, and burns founder ZKTC from the Founders Reserve. FLIP never injects ZKTC into the pool. The mechanism costs the founders tokens rather than paying them: USDC defends settlement depth, and the founder ZKTC burn is the deflationary sacrifice leg.

The Three FLIP Triggers

FLIP activates when any of three conditions are met:

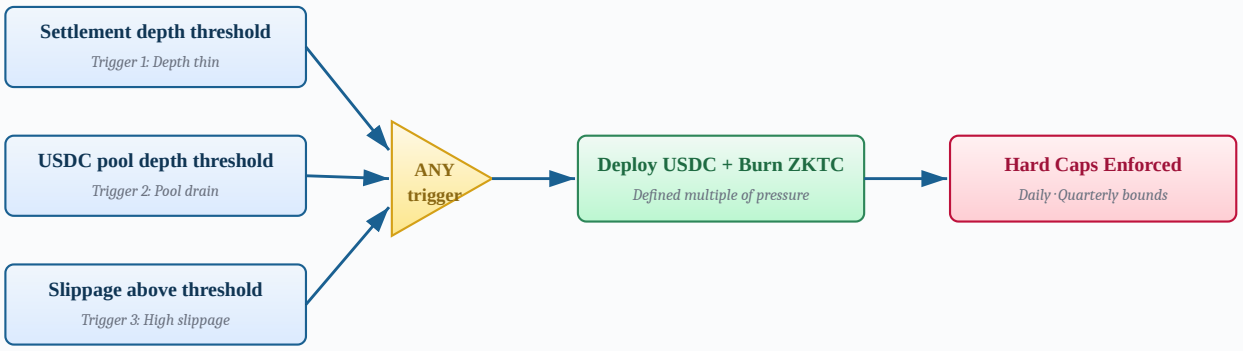

Figure 2 · FLIP Activation — any single trigger fires a depth injection, hard caps prevent runaway

FLIP Activation Conditions

The FLIP smart contract evaluates settlement-depth and slippage conditions continuously and on-chain — never token price:

- **Pool-depth trigger** — USDC reserve in the AMM falls below a defined fraction of launch depth, at which point slippage on payment-grade transaction sizes becomes prohibitive.
- **Sell-pressure trigger** — cumulative ZKTC sold over a multi-hour window exceeds a defined threshold, indicating coordinated pressure rather than ordinary trading.

Any single trigger is sufficient to activate a depth injection. Specific thresholds and window lengths are documented in internal technical appendices reviewed by the ZCBS and by independent auditors prior to deployment (see Section 36).

CRYPTO TALK Pool depth and slippage are watched on-chain — if the AMM gets thin, the contract deploys USDC from the FLIP reserve to restore depth (and burns founder ZKTC), so payment-grade and charitable-disbursement transactions keep settling without prohibitive slippage.

PLAIN ENGLISH If pool depth drops or a large sell thins the AMM, the protocol automatically restores depth from reserves so transactions keep settling cleanly — no human approval needed.

BAD ACTOR A coordinated sell-off can’t drain the pool because the time-weighted average smooths flash movements and the hard daily cap stops the injection mechanism itself from being weaponized.

The FLIP Injection Magnitude

When triggered, FLIP injects a defined multiple of the verified depth shortfall observed in the trigger window. The multiple is calibrated to restore settlement-grade depth to the pool. Specific multipliers and verification methodology are documented in internal technical appendices.

The Injection Caps

Per 24-hour cap	Defined percentage of Founders Reserve maximum
Per quarter cap	Defined percentage of Founders Reserve maximum
Auto-pause	When cap binds, FLIP automatically pauses (hard-coded `require()`)
Resume authority	Three-board approval required to continue beyond cap
Source	Founders Reserve (operational source pool)

This is automated, not discretionary. The FLIP contract evaluates conditions and executes depth injections without human intervention, within the documented caps. There is no administrator who decides whether to inject; the protocol maintains its own settlement-grade depth.

Section 23 — ESR: Effective Supply Resistance

Low-volatility pool behavior built from real assets and disclosed rules — never from misrepresented depth

FLIP and FLOP each manage one side of pool depth: FLIP restores depth when it thins, FLOP redistributes it when it overflows. Effective Supply Resistance (ESR) is the framework that ties them together with two further layers into a single property: a pool that is difficult to move sharply in either direction, so that payment-grade and charitable-disbursement transactions settle at predictable value. ESR matters because ZakPay is a payment and charity rail, not a trading venue — a rail must deliver stable execution for the payments and disbursements routed across it. The resistance ESR describes is resistance to settlement disruption, engineered entirely from assets that are actually present in the pool and from rules that are published and apply equally to everyone.

The Integrity Standard

ESR delivers low-volatility, hard-to-pump and hard-to-dump behavior using only real assets present in the pool and disclosed rules that apply equally to all participants. The stability is engineered, not represented — every unit of resistance is backed by real assets or disclosed rules. The pool is never presented as larger or deeper than it actually is; there is no phantom liquidity, no simulated depth, and no display of reserves that are not genuinely available to trade.

The Three Layers

Layer 1 — Concentrated Real Liquidity

The primary pool concentrates the protocol's real USDC and ZKTC into a defined price band rather than spreading it thinly across the full price curve. Price resists movement within that band because real, tradeable assets are positioned exactly where trading occurs — not because the pool misrepresents its size. This is a standard concentrated-liquidity approach applied for an operational reason: settlement-grade depth where transactions actually execute. The assets backing this resistance are on-chain and verifiable; the resistance is a consequence of where genuine liquidity sits, nothing more.

Layer 2 — FLIP Depth Provisioning

When pool depth falls below defined thresholds, FLIP injects real Founders Reserve capital into the AMM as a disclosed market participant, restoring the depth required for transactions to settle without prohibitive slippage (Section 22). FLIP operates within hard-coded per-epoch and per-quarter caps that automatically pause the mechanism when a cap binds, and it draws only on capital that genuinely exists in the Founders Reserve. Its role within ESR is the depth-provisioning layer: it replenishes real liquidity from a disclosed source under disclosed limits, and it does so to keep the rail functional, not to guarantee any price to any holder.

Layer 3 — Disclosed Trading Limits

The protocol applies transparent, on-chain trading limits that are published in advance and applied equally to every participant: a maximum transaction size, per-wallet cooldowns between large trades, and optional graduated caps during defined sensitive windows. These limits dampen the sudden, outsized movements that would disrupt settlement, and because they are on-chain and uniform, no participant is advantaged or disadvantaged relative to another. They are rules of the venue, disclosed and equal — not discretionary interventions.

What ESR Is and Is Not

ESR is a settlement-reliability property: it keeps the pool stable enough that payments and charitable disbursements execute predictably. It is built only from concentrated real liquidity, disclosed reserve provisioning under hard caps, and published trading rules that apply to all. It is not a mechanism for representing depth that does not exist, and it is not a promise about token price to holders. Every element of the resistance corresponds to a real asset in the pool or a disclosed rule in the contract — verifiable on-chain, applied equally, and engineered for the reliability of the rail.

Section 24 — FLOP: Liquidity Ceiling Operations

When the pool overflows, FLOP redistributes excess to where it serves the protocol

FLOP (Founders Liquidity Operations Protocol) is the counterpart to FLIP. When the primary liquidity pool overflows past a defined ceiling (made healthy by real ZakPay transactions), FLOP atomically buys ZKTC from the open market and burns it in a single contract call — the protocol never holds or accumulates the token. The recovered surplus is routed only to charity, FLIP-reserve refill, and public AMM depth. FLOP has no insider or team-liquidity leg: like FLIP, it costs the ecosystem tokens rather than paying insiders, managing the ceiling through deflation, not price support.

The Five-Way FLOP Distribution

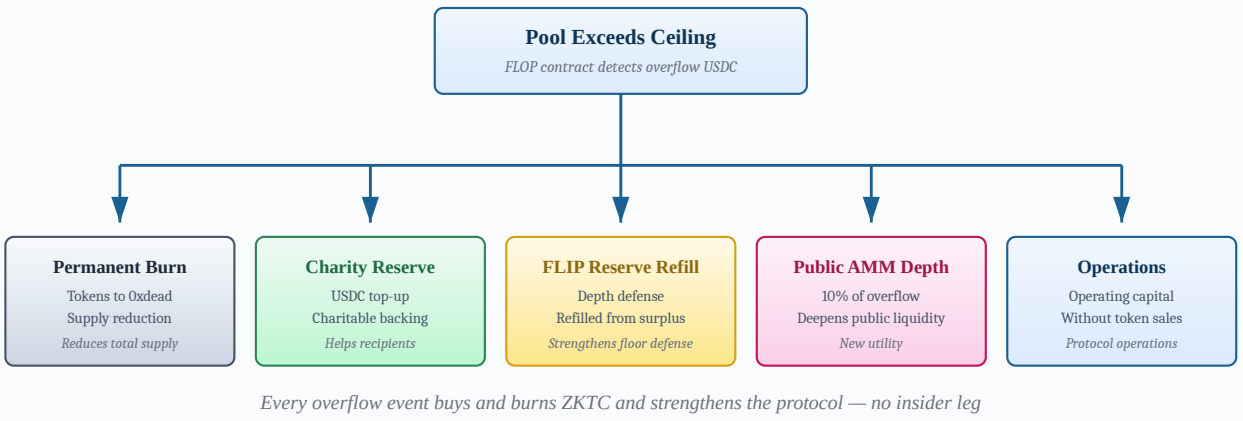

Figure 4 · FLOP Distribution — healthy markets get redirected to permanent structural value

Destination	Allocation	Purpose
Permanent Burn	Defined portion	Tokens sent to `0xdead` — permanent supply reduction, deflationary pressure
Charity Reserve Top-Up	Defined portion	USDC routed to Charity Reserve — healthy markets build charitable backing
Team Liquidity Pool	Defined portion	Builds the segregated insider liquidity pool from commerce, not from token issuance
ZUSD Backing Reserve	10% of overflow USDC	Routed to the 1:1 USDC reserve backing ZUSD — healthy markets deepen the stable-token reserve
Operational Treasury	Defined portion	Enables Zakat Coin Inc. to receive operating capital from healthy market conditions rather than from token sales

> CRYPTO TALK When the AMM gets fat with USDC, FLOP buys and burns ZKTC and routes surplus to charity and FLIP-reserve refill — deflationary by design, no insider leg, no dump pressure on the pool.
>
> PLAIN ENGLISH When the protocol is doing well, instead of letting that value sit idle or get extracted by speculators, it gets automatically split into burns, charity funding, team support, stablecoin reserves, and operating capital.
>
> BAD ACTOR No one can game FLOP to drain the treasury — the five allocations are smart-contract enforced ratios, not discretionary releases, so even insiders can’t redirect overflow to themselves.

The Structural Insight

In the ZKTC system, the value generated by healthy markets is *redirected* by protocol design rather than accruing to holders as price appreciation: into permanent burn (reduces supply), into charitable reserves (funds giving), into team liquidity (replaces insider selling that would otherwise drain the community pool), into stablecoin backing (creates new utility infrastructure), and into operating capital (lets the company fund operations without selling tokens). Every overflow event strengthens the protocol's structural integrity rather than accruing to holders.

Section 25 — ODS: On Demand Supply

Commerce activates supply. No commerce, no activation.

The Inventive Concept

New ZKTC supply activates exclusively from completed settlement events on ZakPay processing real-world transactions. Tokens cannot be minted, released, or added to circulating supply by any action other than the platform earning fee revenue from completed transactions. This mechanism is enforced by smart contract with no discretionary override.

How ODS Works

When ZakPay processes a transaction — a payment, a donation, a remittance, a card spend — the platform earns a fee. A defined portion of that net fee revenue accumulates in an on-chain supply activation budget. At each accounting interval, the ODS contract divides the accumulated budget by a stored anchor price to calculate how many tokens to activate from operational reserves into circulating supply.

The ODS Engine-Matched Formula

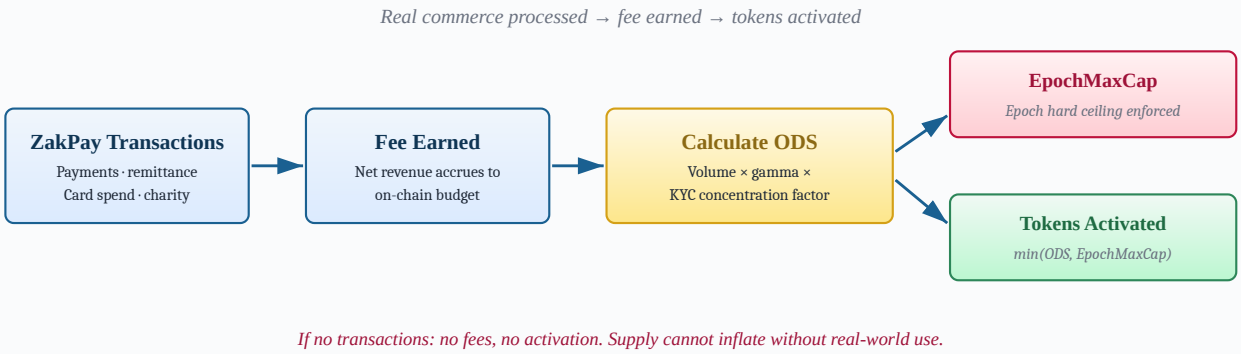

Figure 3 ·ODS Activation Chain — commerce is the only input that mints new circulating supply

How ODS Activation Is Calculated

ODS activation aggregates completed settlement events across all completed ZakPay transactions in an epoch, then scales the result by three structural factors before converting to a token-activation quantity:

- **Commerce volume** — the underlying fee revenue earned by ZakPay from completed transactions in the epoch.
- **KYC concentration adjustment** — a penalty that dampens activation when commerce volume concentrates in few wallets, structurally preventing wash-volume attacks from inflating supply.

The result is then bounded by the EpochMaxCap (described below). Specific coefficients, exponents, and calibration constants are documented in internal technical appendices reviewed by the ZCBS and by independent auditors prior to deployment (see Section 36).

> CRYPTO TALK No mint function, no governance vote, no team multisig — supply only unlocks when ZakPay rails actually process txs. Fees in, tokens out, fully on-chain.
>
> PLAIN ENGLISH New tokens only become available when real customers use the app. If nothing is happening on the platform, no new supply is created.

> BAD ACTOR A bad actor can't fake-pump supply by spinning up wash transactions: the KYC concentration penalty crushes activation when one wallet dominates, and the epoch hard cap closes the rest of the door.

The Hard Activation Ceiling

No matter how high the calculated activation is in any given epoch, ODS cannot exceed a hard ceiling defined as a defined percentage of the Founders Reserve. This `require()`-enforced safety bound prevents rapid supply expansion under any market condition — including hypothetical extreme commerce volume or oracle compromise. When the ceiling binds, activation pauses; resumption requires three-board approval (see Section 36).

Why ODS Is Novel

Every existing token supply mechanism responds to financial system signals: market price, reserve ratios, or administrator discretion. ODS responds to a fundamentally different signal: *real-world commerce activity*. A completed payment transaction is the cause. Token supply activation is the effect. This causal chain — **real commerce processed → fee earned → tokens activated** — is protected under the non-provisional patent application covering the FUSE settlement architecture.

Section 26 — QALB: The Heart of the Ecosystem

The organs that pump liquidity and stability through the protocol

The preceding sections introduced four mechanisms individually: FLIP restores pool depth when it thins, FLOP redistributes it at the ceiling, ODS activates supply from real commerce, and ESR ties them into a low-volatility settlement property. Taken together, these are not four unrelated engines. They are a single circulatory system. We refer to them collectively as **QALB** — from the Arabic word for *heart* — because their combined function is exactly that of a heart: to keep liquidity and stability circulating through the ecosystem so that the system as a whole remains alive and functioning.

The metaphor is precise, not decorative. A heart does not create value on its own; it moves what the body already has to where the body needs it. QALB does the same with real assets already present in the protocol. FLIP moves liquidity into the pool when depth runs low. FLOP moves surplus out when the pool runs rich — buying and burning ZKTC, and topping up charity and the FLIP reserve. ODS paces the entry of new supply to the rhythm of genuine commerce. ESR holds the whole system steady enough that payments and charitable disbursements settle predictably. None of these mechanisms manufactures value from nothing; each moves real, present assets according to disclosed rules that apply equally to all participants.

The Heart and the Brain

If QALB is the heart of the ecosystem — circulating liquidity and stability — then FUSE and the SIR settlement layer are its brain: the coordination logic that decides what settles, when, and how, and records each event immutably on-chain. The brain directs; the heart sustains. Neither claims to guarantee any outcome to any holder. Together they describe a system whose stability is engineered from real assets and disclosed rules, not represented or promised.

Section 27 — The Launch Price Discovery Formula

No one decides the launch price. The protocol calculates it from its own operational data.

At the moment of Public Launch, the ZKTC/ZUSD AMM is created with initial liquidity provided by the FLIP engine. The launch price — the price at which public market trading begins — emerges from a deterministic six-step formula that resolves against the actual on-chain data accumulated during the Donation Coin Offering phase. No party predetermines the launch price. No party can predict it in advance.

The Critical Property

The launch price is not predictable in advance by any party — including the founding team. The formula's inputs (cumulative liquidity pool USDC, cumulative tokens distributed during the DCO phase, and the last active tranche price) continue to evolve until the moment the launch block executes. The launch price is the deterministic output of operational reality, not a managerial forecast.

The Six-Step Formula

Step 1 — Total USDC Pool

$$\text{USDC}_{\text{pool}} = \text{Seed}_{\text{initial}} + 0.90 \times \sum_{i=1}^{N} \text{Revenue}_{\text{tranche}_i}$$

The total USDC accumulated in the Primary Liquidity Pool at the moment of Public Launch. Sourced from the initial seed plus 90% of all tranche revenue from the Public Pre-Sale (the remaining 10% routes to the Team Liquidity Pool).

Step 2 — Total AMM Pool Value (50/50 split)

$$\text{AMM}_{\text{value}} = \text{USDC}_{\text{pool}} \times 2$$

The AMM is created with a 50/50 value split between ZKTC and USDC. The total pool value is therefore twice the USDC contribution.

Step 3 — FLIP ZKTC Injection

$$Y_{\text{flip}} = \frac{\text{USDC}_{\text{pool}}}{P_{\text{last-tranche}}}$$

The quantity of ZKTC tokens injected into the AMM by FLIP, sourced from the Founders Reserve. The injection is sized against the most recent active tranche price, ensuring continuity between the pre-sale price signal and the public market.

Step 4 — Total Initial Token Count

$$T_{\text{launch}} = \text{Tokens}_{\text{DCO sold}} + Y_{\text{flip}}$$

The total count of tokens in circulation at launch, including all tokens distributed during the DCO phase (subject to vesting per Section 20) plus the FLIP AMM injection.

Step 5 — Implied Market Capitalization

$$ \text{MC}_{\text{implied}} = \frac{\text{USDC}_{\text{pool}}}{0.10} = \text{USDC}_{\text{pool}} \times 10 $$

The implied fully-diluted valuation, using the convention that initial USDC liquidity represents 10% of total market cap. This is conservative: 10% USDC corresponds to roughly 20% of total pool value under the 50/50 split, against the 20–30% total-pool ratios typical of DeFi launches; the lower ratio preserves AMM depth relative to circulating supply.

Step 6 — Public Launch Price

$$ P_{\text{launch}} = \frac{\text{MC}_{\text{implied}}}{T_{\text{launch}}} $$

The price per ZKTC at the moment the public AMM opens for trading. The formula self-balances around the most recent tranche price as the operational anchor, with the implied market cap providing the launch-day price discovery.

The Formula as Pseudocode

Launch Price Discovery (Pseudocode — executes at the Launch Block)

```
function executeLaunchCeremony(): # Read state at launch block usdc_pool =
primary_lp.get_usdc_balance() tokens_dco_sold = dco_reserve.get_cumulative_sold()
p_last_tranche = tranche_manager.get_last_active_price() # Step 1-2: Pool value
amm_value = usdc_pool * 2 # Step 3: FLIP injection from Founders Reserve y_flip =
usdc_pool / p_last_tranche founders_reserve.transfer(amm, y_flip) # Step 4: Total
circulating supply t_launch = tokens_dco_sold + y_flip # Step 5: Implied market cap
(USDC = 10% of MC) mc_implied = usdc_pool / 0.10 # Step 6: Public launch price
p_launch = mc_implied / t_launch # Burn the remaining DCO Reserve allocation
dco_reserve.burnRemainder() # sends remainder to 0xdead emit LaunchCeremony(
p_launch = p_launch, t_launch = t_launch, y_flip = y_flip, timestamp = now() )
```

Why This Design Works

Three architectural properties make this launch mechanism strong:

1. **Deterministic.** Given the on-chain inputs, anyone can compute the launch price after the launch block executes. No managerial discretion, no private information about the price.

2. **Proportional to demonstrated demand.** More USDC raised during pre-sale → larger AMM → larger FLIP injection → bigger launch capitalization. The protocol is structurally sized by participant interest.
3. **Continuity with the operational price signal.** The last tranche price anchors the FLIP injection size, ensuring the public market opens at a price consistent with the most recent demonstrated demand, not at an arbitrary number.

Section 28 — The Team Liquidity Pool (TLP)

A token protocol designed so that insider liquidation helps the public

In conventional token launches, the moment of insider unlock is the moment of greatest public anxiety. Holders watch the calendar, brace for the cliff, and price the imminent dump into the market well in advance. When the insiders actually sell, the the public typically bears the loss while insiders exit first. This pattern is so well-established that experienced crypto holders treat insider unlocks as predictable adverse events. The Zakat Coin protocol is structured to invert this dynamic completely.

How Team Tokens Enter Circulation

Before a Team Restricted Token Unit can ever be sold or burned, it must first enter circulating supply — and understanding how it gets there is what makes the deflationary effect described below real rather than cosmetic. Team RTU tokens do not begin in circulation. They are held outside circulating supply and enter it through a disciplined, commerce-driven lifecycle.

The lifecycle has three stages, each gated:

First, real commerce activates the tokens. Team RTU tokens enter circulating supply only through the On-Demand Supply mechanism (Section 25), which is driven exclusively by genuine ZakPay transaction activity. No commerce means no activation. Team tokens cannot appear in supply because of a decision, a date, or an administrative action — they appear only as the platform processes real settlement volume. When activated, these tokens are counted toward circulating supply and market capitalization, but they carry a structural restriction: they are Team-sellable only. The public cannot acquire or trade an RTU on the open market; only vested Team members may sell them, and only into the segregated Team Liquidity Pool.

Second, vesting gates the sale. Activation alone does not let a Team member sell. The tokens remain subject to the vesting schedule — a twelve-month cliff followed by a multi-year release — so a Team member can only sell activated RTU tokens once those tokens have vested. Commerce determines whether the tokens exist in supply; vesting determines whether the Team member has earned the right to sell them.

Third, the sale burns the tokens. When a vested Team member cashes out, the transaction settles against the segregated Team Liquidity Pool — never the public liquidity pool — and the sold tokens are permanently burned from circulating supply.

This is the mechanism that makes the deflationary claim genuine. Because Team RTU tokens genuinely enter circulating supply through real commerce before they are ever sold, their removal at cash-out is a true contraction of circulating supply — the public benefits from the removal of tokens that had actually entered circulation, not from the destruction of tokens that were never there. A burn of tokens that never circulated would be cosmetic; a burn of tokens that entered through real commerce and are then destroyed on exit is a real, net reduction in supply.

How TLP Inverts the Conventional Model

The **Team Liquidity Pool (TLP)** is a dedicated reserve that funds the cash-out of vested Team RTU (Restricted Token Unit) holdings. When a Team member liquidates their vested RTU, the following happens at the smart-contract level:

1. The Team member's vested ZKTC tokens are **permanently burned**. They are not transferred to a buyer; they are destroyed.
2. The Team member receives cash payment from the TLP reserve, denominated in USDC, at the prevailing market price at the moment of cash-out.
3. Total circulating supply **decreases** by the burned amount.
4. The TLP reserve decreases by the cash paid out.

The net effect on the protocol: **supply contracts, no sell pressure hits the public market, the Team is compensated.** The public does not have to absorb insider sales because no tokens enter the open market — they are destroyed before they could.

How TLP Is Funded

TLP grows over time from three structural sources, ensuring it has the capacity to fund Team cash-outs as they vest:

Funding Source	Mechanism	Function
Defined portion of token sales	A pre-defined share of USDC proceeds from the private and public Donation Coin Offering phases	Seeds the TLP at launch and grows it through each presale phase

Funding Source	Mechanism	Function
Defined portion of ZakPay platform revenue	A defined share of ZakPay transaction-fee revenue routed to TLP over time	Ties TLP maturation to the company's operational success — the more ZakPay transacts, the more TLP grows

The specific percentages for each funding source are defined and ratified during the mutable phase through three-board governance (Zakat Coin Inc., Zakat Coin Organization Inc., and ZCBS oversight), subject to the structural constraint that TLP must have sufficient liquidity at any vesting milestone to fund all eligible Team cash-outs without disruption. These percentages will be published in the Public Utility Dashboard (Section 35) and reaffirmed annually.

Why This Matters — The Public's Inverted Position

For the First Time, the Public Welcomes Insider Cash-Outs

In every conventional token launch, the calendar of insider unlocks is a calendar of public dread. Holders short the unlock dates. Long-term investors exit before the cliff. The token's price chart is shaped by what insiders are about to do, not what the protocol is achieving. The Zakat Coin protocol breaks this pattern at the structural level.

When a Zakat Coin insider liquidates their vested RTU, **the public benefits**: total supply contracts, the protocol becomes structurally more deflationary, and the public market is undisturbed. There is no sell pressure to absorb. There are no orphaned tokens that previously belonged to insiders now flooding into thin order books. There is simply a smaller total supply and an insider who has been compensated through the dedicated pool. The insider's incentive is to remain aligned with protocol success because their cash-out value is tied to the prevailing market price; the public's incentive to hold ZKTC is reinforced because supply contraction supports value over time.

The Structural Properties of TLP

- **Supply-contracting at every cash-out.** Every Team RTU liquidation reduces total supply. The aggregate effect over the full Team RTU vesting period is materially deflationary.

- **No open-market sell pressure from Team.** The Team's interaction with the open market is non-existent at the moment of cash-out. The public never absorbs Team supply, because Team supply is destroyed before it could enter the market.
- **Anti-rug-pull at the structural level.** Because cash-out is mediated through TLP and not through open-market sale, there is no mechanism by which the Team can dump unrestricted volumes to the public. The protocol's pace of cash-out is bounded by TLP liquidity, the vesting schedule, and the three-board governance.
- **Aligned incentives.** The Team's cash-out value is determined by market price at the moment of cash-out. Team members are therefore structurally aligned with protocol long-term success: a higher market price means higher cash-out value, a lower market price means lower cash-out value. There is no mechanism by which Team members can profit from harming the protocol.
- **Transparency.** TLP reserves, inflows, outflows, and cash-out events are all visible on-chain through the Public Utility Dashboard. There are no off-chain arrangements, side deals, or undisclosed transfers.

TLP and the Founders Reserve Are Different Pools

TLP funds **Team RTU cash-outs only**. It does not fund FLIP depth provisioning (which draws from the Founders Reserve, Section 22), ODS supply activation (also Founders Reserve, Section 25), ZPP matched releases (also Founders Reserve, Section 15), or any other protocol function. The structural separation between TLP and the Founders Reserve ensures that Team cash-out demand never competes with protocol depth-provisioning capacity. The protocol's stability mechanisms are not impaired by Team liquidation events.

> CRYPTO TALK TLP-mediated burn-on-cashout converts insider unlocks from a public-bag distribution event into a structurally deflationary one. No open-market sell pressure on RTU vest events. Anti-rug enforced at the contract layer, not at the policy layer.
>
> PLAIN ENGLISH When the Team cashes out their earned tokens, the protocol pays them from a dedicated pool and then destroys the tokens. The public never sees insider tokens flood the market — because they don't. Supply gets smaller, not bigger, when insiders sell.
>
> BAD ACTOR A Team member cannot dump tokens on the open market because cash-out happens only through TLP and only at the rate TLP can fund. Sudden mass insider exit is structurally bounded by the pool's funded capacity.

Section 29 — ZUSD

A stable token backed 1:1 by USDC

ZUSD is a stable token backed 1:1 by USDC. It is used within the ZakPay ecosystem for stable-value settlement and for charitable disbursement, so that charities and recipients receive predictable value rather than exposure to token volatility. ZakPay is not the issuer of the underlying stablecoin; ZUSD is backed 1:1 by USDC, a regulated stablecoin, and is presented as ZUSD within the ZakPay user experience. Every ZUSD is backed by USDC held 1:1 — not by directly held US dollars, and not by any asset the protocol represents as larger than it is.

What ZUSD Is

ZUSD is a 1:1 USDC-backed stable token used for disbursement and stable-value settlement inside ZakPay. It is non-interest-bearing. It carries no promise of yield or return; it exists to move stable value predictably through the ecosystem.

How ZUSD Is Created and Why It Is Backed by USDC

ZUSD is not issued by Zakat Coin Inc. or by ZakPay. The underlying stable asset is USD Coin (USDC), whose issuer is Circle, a regulated stablecoin issuer that publishes reserve attestations for USDC. ZUSD is the in-ecosystem representation of that USDC: it is created when USDC enters a ZakPay flow, held at a strict 1:1 ratio against USDC, and it resolves back to USDC when value leaves the ecosystem. A user does not hold ZUSD as a free-standing, externally transferable currency; outside the ZakPay ecosystem, the asset is simply USDC. ZUSD therefore does not circulate as, and is not intended to compete with, an independent stablecoin — it is a settlement and disbursement representation of USDC used inside the platform.

The choice of USDC as the backing asset is deliberate. USDC is issued by a regulated entity and is supported by published reserve attestations, which fits the transparency and compliance posture of the ecosystem. ZakPay maintains a direct minting-and-redemption relationship with Circle Mint that allows USDC to be minted and redeemed at a 1:1 ratio, and the 1:1 backing of ZUSD is maintained against that USDC at all times. Because the backing asset is a regulated, attested stablecoin rather than an asset the protocol self-issues or self-values, the value that moves through settlement and reaches charitable recipients is backed by a transparent, externally-verifiable reserve.

PART VII — RISKS

Substantive risk disclosures

Section 30 — Risks & Limitations

What could go wrong, and what mitigates it

This section enumerates material risks that could affect the Zakat Coin ecosystem. The Team believes transparent risk disclosure is essential both for regulatory standing and for the trust of participants. No mitigation eliminates risk; the items below should be read as ongoing engineering, legal, and governance constraints.

Technical Risks

- **Smart contract risk:** Contracts are subject to independent audit before mainnet deployment (see Section 34). No production-scale contracts will be deployed on public market without audit sign-off. Bug bounty via an established public bug bounty platform planned post-launch. Despite audit, residual smart-contract risk is non-zero for any decentralized system.
- **Oracle dependency:** ODS, FLIP depth provisioning, and burn-and-mint mechanics depend on reliable price feeds. Multi-source oracle consensus with divergence circuit breakers mitigates economic attacks. TWAP-based pricing on all consumption calculations.
- **BSC chain risk:** ZKTC is initially deployed on BNB Smart Chain (BEP-20). BSC is a centrally-influenced validator set and carries different decentralization characteristics than fully-permissionless chains. Bridge to Ethereum L2 (a leading Ethereum Layer 2 chain) is targeted for Phase 2 (see Section 36) to mitigate single-chain dependency.
- **Bridge risk:** Cross-chain bridges remain among the highest-attack-surface components in the crypto stack. Phase 2 bridge implementation will use only audited, institutional-grade bridge infrastructure (institutional-grade bridge infrastructure with full security review).

Economic & Liquidity Risks

- **Market liquidity:** Launch pool depth depends on Donation Coin Offering outcomes. Thin pools at launch create higher price volatility. FLIP depth provisioning activates automatically when pool depth falls below threshold.
- **Card adoption execution:** Some Giving Contract activation rates depend on ZakPay Card usage scaling. This is an unproven adoption trajectory.
- **Founders Reserve depletion under sustained stress:** Repeated FLIP activations during a sustained bear market could deplete the operational source pool. Daily and quarterly hard caps prevent runaway, but a multi-quarter coordinated assault remains a theoretical risk. Three-board approval is required to authorize resumption beyond cap.
- **USDC and stablecoin counterparty risk:** The protocol's reserves are denominated in USDC. A a primary stablecoin issuer insolvency, USDC depeg, or regulatory action against the institutional stablecoin issuer would materially affect ZKTC mechanics. The Team monitors the primary stablecoin issuer's reserve composition and is evaluating a multi-stablecoin reserve diversification strategy.

Partner Concentration Risks

- **an institutional brokerage and custody provider:** Institutional brokerage for liquidity operations. Loss of an institutional brokerage and custody provider relationship would require migration to alternative prime broker (alternative institutional prime brokerages) with potential operational disruption.
- **a federally chartered qualified custodian:** Federally-chartered qualified custodian for all user crypto assets. Single-custodian concentration is mitigated by the qualified custodian's OCC charter and institutional insurance, but custody-provider failure remains a tail risk.
- **an institutional stablecoin issuer:** Institutional USDC issuance. Backup providers (an alternative regulated USD stablecoin) are being evaluated.
- **a primary operational banking partner:** Primary operational banking. FBO account structure with limited single-point-of-failure exposure.
- **the domestic real-time payment provider:** Domestic real-time payment rail. Alternative RTP providers being evaluated for redundancy.

Regulatory & Legal Risks

- **Regulatory environment:** Cryptocurrency regulation continues to evolve in all jurisdictions. Material regulatory changes could affect operations. FinCEN MSB registration and independent legal counsel are active mitigations.

- **State money transmitter licensing:** ZakPay's routing role may require state-level MTL acquisition, authorized delegate agreements, or qualifications under agent-of-payee exemptions. State-by-state licensing is a multi-year process.
- **Token classification risk:** Despite the protocol's deliberate utility-driven structure, an adverse regulatory reinterpretation could reclassify ZKTC. The structural separation of token-acquisition proceeds from company revenue is a core mitigation; ongoing engagement with securities counsel is a second.
- **USDC dependency:** ZUSD is backed 1:1 by USDC. A depeg of USDC, insolvency of its issuer, or regulatory action against USDC would directly affect ZUSD and any ZUSD-denominated balances or disbursements within the ecosystem. The protocol does not control USDC and depends on its continued stability.
- **Tax-receipt registration:** Zakat Coin Organization Inc. issuing tax receipts at scale through the ZKT-Badge mechanism may require state-level charitable solicitation registration in multiple jurisdictions (NY EPTL, CA AG, etc.). This is being evaluated with fiscal-sponsor counsel.

Shariah-Interpretation Risk

- **Diversity of Islamic jurisprudence:** Islamic finance contains multiple schools of jurisprudence (madhahib) with sometimes divergent rulings on novel financial instruments. The ZCBS fatwa reflects the considered judgment of recognized scholars within mainstream Sunni jurisprudence; alternative interpretations from other traditions may differ. The Team commits to ongoing scholarly engagement and annual fatwa reaffirmation.
- **Future scholarly reconsideration:** The ZCBS retains absolute veto authority (Section 31) and may, upon further deliberation, require modifications to protocol mechanics if previously-approved features are found to conflict with evolved Shariah understanding.

Operational & Execution Risks

- **Phase 1 build-out:** a non-custodial smart-contract wallet provider smart-contract wallets, card infrastructure, and card-issuing integration require successful Phase 1 implementation. Delays in any one component affect launch timeline.
- **Team scaling:** The Team is small. Hiring qualified engineering, compliance, and Shariah-advisory staff in the volumes required for global scale is an execution risk.
- **Adversarial environment:** The crypto industry contains sophisticated bad actors. Despite structural anti-fraud mechanisms (see Bad Actor callouts throughout), zero-day exploits and social-engineering attacks remain possible.

PART VIII — GOVERNANCE & VERIFICATION

Oversight, Shariah governance, audit, and on-chain verification

Section 31 — Three-Body Governance Structure

Technology, charity, and Shariah — each with defined authority and structural safeguards

The Zakat Coin ecosystem is anchored by three governing entities, each with defined responsibilities and safeguards, ensuring both technological innovation and charitable integrity.

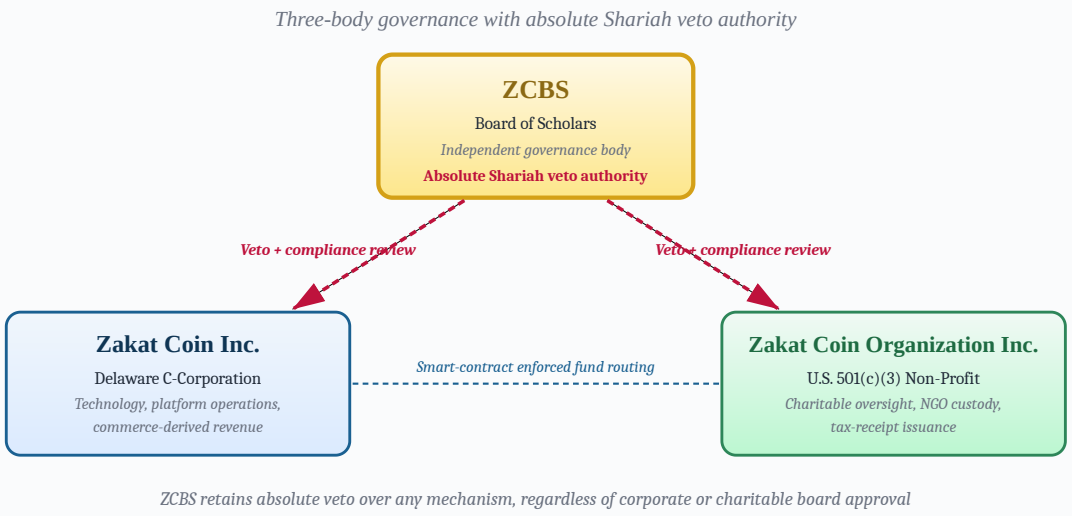

Figure D · Three-Body Governance Framework — technology, charity, and Shariah oversight as independent bodies

Entity	Form	Responsibility
Zakat Coin Inc.	Delaware C-Corporation	Oversees technology development, intellectual property, regulatory compliance, ZakPay platform operations, FinCEN MSB obligations, and the relationship with institutional partners. Revenue source: ZakPay platform transaction fees only.
Zakat Coin Organization Inc.	U.S. 501(c)(3) Non-Profit (EIN 39-4624928)	Provides charitable oversight, nonprofit governance, and permanent stewardship of donation disbursement policies. Owns the ZCW and SCW wallets at an institutional brokerage and custody provider. Issues tax-deductible acknowledgments to donors.
Board of Scholars (ZCBS)	Independent Shariah advisory body	Reviews, guides, and oversees the religious compliance of the Zakat Coin ecosystem. Retains **absolute veto authority** over any decision that conflicts with Islamic principles, regardless of corporate board majority or community vote. Conducts quarterly compliance reviews. Annual fatwa reaffirmation required.

Absolute Veto Authority

The Zakat Coin Board of Scholars (ZCBS) retains absolute veto authority over any decision, proposal, or governance action — regardless of corporate board majority approval or community sentiment — if it violates Islamic principles. No ecosystem function, smart contract, governance proposal, or operational process may override the framework certified by the ZCBS and its external advisors. This veto is not symbolic; it is operationally enforceable through the protocol's multi-signature governance architecture during the mutable phase.

Token Proceeds and Revenue Separation

A Critical Distinction

All USDC generated from ZKTC acquisitions is designated entirely to liquidity pools and charitable reserves. Zero token acquisition proceeds constitute company revenue for Zakat Coin Inc. The company earns revenue exclusively from ZakPay platform transaction fees. These are structurally separate income streams with separate accounting, separate wallets, and separate legal characterization.

This separation matters operationally as well as structurally. A company funded primarily by token sale proceeds has a financial interest tied to token price. ZakPay's revenue is generated from payment commerce. The more transactions ZakPay processes, the more revenue the company earns — a business model directly tied to platform usage rather than token market dynamics.

Section 32 — The Board of Scholars

The conscience of the ecosystem — independent Shariah governance with absolute jurisprudential authority

The Zakat Coin Board of Scholars (ZCBS) is the independent governance body responsible for Shariah oversight of every mechanism in the Zakat Coin ecosystem. The Board operates independently of Zakat Coin Inc. and Zakat Coin Organization Inc., reporting through documented governance processes rather than corporate hierarchy. Its authority is structural — encoded into the protocol's multi-signature governance architecture — rather than advisory.

Composition Requirements

The ZCBS is composed of internationally recognized scholars in Islamic finance, classical jurisprudence, and contemporary digital-asset Shariah analysis. Composition is governed by minimum standards rather than fixed membership, allowing the Board to evolve over time while preserving its structural authority:

- **Minimum three scholars** with recognized standing in Islamic finance jurisprudence at the international level.

- **Diversity of madhhab** — the Board's collective expertise is intended to span the major Sunni schools of jurisprudence to ensure broad-based scholarly reasoning rather than narrow interpretation.
- **Demonstrated expertise** in contemporary Islamic financial transactions, digital assets, blockchain mechanics, and the practical application of Shariah principles in modern financial systems.
- **Independent appointment** — scholars are not employees of Zakat Coin Inc. and serve under written governance agreements documenting independence, oversight responsibilities, and conditions of service.

Current ZCBS membership and individual scholar biographies are maintained externally on the ZakPay platform website, in published fatwa documentation, and in formal governance disclosures. The whitepaper describes the governance framework; the public-facing portal documents the individuals serving under it.

ZCBS Oversight Responsibilities

- **Quarterly compliance reviews** conducted by all serving scholars on platform mechanics, charitable flows, and governance decisions.
- **Annual fatwa reaffirmation** required for all certified mechanisms.
- **Material change review** required before any change to token mechanics, charitable routing, or platform design is implemented.
- **Absolute veto** over any mechanism, governance proposal, or operational decision that conflicts with Islamic principles, regardless of corporate or community approval.
- **Public transparency** — all fatwa opinions and compliance certifications are published on the ZakPay platform website for public review.

Initial Fatwa & Ongoing Certification

The joint fatwa certifying the Zakat Coin ecosystem — covering the ZKTC token design, the charitable contribution structure (independent *Tabarru'* commitment), the payment methods, and the technical transaction flow — was issued by the inaugural ZCBS. The full fatwa documentation, the names and credentials of the issuing scholars, and supplemental jurisprudential reasoning across the four Sunni schools and contemporary AAOIFI standards are published in the public fatwa archive.

Ongoing certification is provided through the quarterly review and annual reaffirmation processes described above. The fatwa is renewed against the live, then-current state of the protocol — not against an earlier-frozen specification — ensuring continued Shariah alignment as the ecosystem evolves.

Shariah Classification of ZKTC and the DCO Structure

ZKTC Classification	*Mal mutaqawwam* — valid Shariah-recognized asset with lawful usufruct (*manfa'ah*)
DCO Structure	Consumptive utility acquisition — ZKTC is acquired to be consumed as settlement fuel within ZakPay; participation is for access and use, not deferred delivery of an investment asset.
Charitable Component	Independent *Tabarru'* (donation) commitment. Not a countervalue in the sale contract.
Hold-Based Giving	Conditional unilateral undertaking — not staking, not yield, not APR. Charitable trigger only.
ZUSD	A stable token backed 1:1 by USDC. Non-interest bearing. Shariah-neutral deployment.

Section 33 — Regulatory Standing

Licensed, registered, certified, and represented by tier-1 counsel

FinCEN MSB Registration	No. 31000302240755 — active
USPTO Patent (Non-Provisional)	Application 19/640,087, filed via independent IP counsel, Track One prioritized examination
PCT International Filing	Filed — international protection across PCT member countries
Patent Filings (Additional)	USPTO 63/805,645 and 63/838,299 covering related utility mechanisms
Legal Counsel	independent IP counsel — patent prosecution and securities compliance
501(c)(3) Determination	Zakat Coin Organization Inc., EIN 39-4624928 — active
Money Transmitter Coverage	50-state MTL coverage via a licensed Banking-as-a-Service provider with multi-state money transmitter coverage
Custodian (Crypto)	an OCC federally chartered national trust bank serving as qualified custodian
Custodian (Charitable)	an institutional brokerage and custody provider — institutional brokerage and 501(c)(3) wallet custody
USDC Issuance	an institutional stablecoin issuer — institutional wholesale relationship
Shariah Review	Reviewed by the inaugural Zakat Coin Board of Scholars; the current version is under continuing scholarly review. Scholar names and credentials published in the public archive.

Section 34 — Audit & Security

Independent verification before any production deployment

The Team treats audit as a structural precondition, not a marketing event. No production-scale smart contract will be deployed to mainnet without independent third-party audit sign-off. This commitment is binding under the protocol's pre-launch mutable governance and will be enforced at the multi-signature deployment authority level.

Planned Audit Engagement

Item	Status
Primary auditor (target)	a leading independent smart-contract audit firm — engagement in active negotiation. Final selection ahead of the audit engagement.
Audit scope	All ZKTC smart contracts including: FUSE settlement engine, SIR lifecycle, FLIP depth-provisioning mechanism, FLOP distribution logic, ODS activation calculator, Giving Contracts, ZKT-Badge soulbound NFT contract, ZUSD stablecoin mechanics (when activated).
Audit timeline	Full audit prior to mainnet deployment, followed by remediation and re-audit as required. Sequenced ahead of the immutability transition rather than to a fixed calendar; mainnet deployment occurs only after audit sign-off.
Secondary review	A secondary review by a different audit firm (a secondary independent audit firm with EVM specialization under evaluation) is targeted for the FUSE settlement engine specifically, given its role as the protocol's core settlement primitive.
Bug bounty	an established public bug bounty program to launch within 30 days of mainnet deployment. Bounty pool to be funded from operational treasury, with tier-based payouts for critical / high / medium severity findings.

Item	Status
Audit report publication	Full audit reports published at `audits.zakatcoin.com` upon completion. No production traffic routed through unaudited contracts.

Defense-in-Depth Security Posture

Beyond smart-contract audit, the protocol implements defense-in-depth across multiple security layers:

- **Custody layer:** User crypto assets held at a federally chartered qualified custodian under federally-chartered qualified custodian status, with institutional insurance coverage.
- **Key management:** Multi-signature governance with hardware-secured keys distributed across geographically separated signers during the mutable phase.
- **Oracle security:** Multi-source price feed aggregation (multiple institutional oracle providers) with divergence circuit breakers. No single oracle controls protocol parameters.
- **Hard caps as backstop:** Even in the event of an oracle manipulation or smart-contract exploit, hard-coded mint/burn caps prevent runaway value extraction. Caps execute at the EVM `require()` level and do not depend on multi-signature or oracle integrity to enforce.
- **Operational monitoring:** 24/7 on-chain monitoring with automated anomaly alerting. Coordinated incident response procedures.
- **Mutable-to-immutable migration:** Once stable, the protocol transitions to immutable contracts removing the upgrade authority as an attack vector (see Section 17).

> CRYPTO TALK Audit before deployment is the table-stakes baseline; defense-in-depth means even an oracle exploit can't drain the reserves because the hard caps are coded into the contract, not enforced by the multi-sig.
>
> PLAIN ENGLISH Independent security firms will check every smart contract before it goes live. Even if something gets through, multiple safety limits prevent any single failure from causing catastrophic damage.
>
> BAD ACTOR Even a compromised oracle or a hypothetical contract exploit can't break the protocol — the hard caps execute at the EVM level and don't depend on any external authority to enforce them.

Section 35 — The Public Utility Dashboard

Trust by visibility. Every minute the protocol operates is another minute of evidence.

The Public Utility Dashboard is a real-time web application directly accessible from the ZakPay website (target subdomain: **dashboard.zakpay.com**) that displays live operational data from the ZKTC protocol on BSC mainnet. It is read-only, requires no login, requires no wallet connection, and updates continuously as the protocol operates.

Five Strategic Purposes

Purpose	Why It Matters
1. Verifiable Utility Through Public Transparency	Real utility is publicly verifiable. Anyone can observe tokens flowing through actual transactions, charity being routed, and SIRs being minted and settled. Utility is happening, visibly, every minute — observable directly rather than asserted in a document.
2. Shariah Transparency	The Board of Scholars, the global Muslim community, and individual donors can verify in real time that zakat-intent flows to ZCW, that sadaqah flows to SCW, and that funds reach verified NGO destinations. Trust is built by visibility, not by promise.
3. Regulator-Facing Transparency	FinCEN, IRS, state money transmitter regulators, and 501(c)(3) governance bodies can verify operational reality without requesting reports. The dashboard IS the report — live, continuous, immutable in its on-chain data sources.
4. Marketing and Community Trust	"$X donated to charity this month, across Y transactions, settling in Z seconds globally" is compelling, public, and immediately verifiable. The strongest marketing the protocol could have is the visible reality of the architecture working.
5. Live Audit Trail	The Three Mathematical Invariants (Section 15) are verified continuously in real time. Anyone can confirm the system is operating as documented. Auditability becomes a public service.

The Core Display Modules (Launch Phase)

- **Live Charity Counter:** Total USDC routed to ZCW + SCW, broken into today, this month, and all-time cumulative. Animated counters tick up in real time.
- **ZPP Status Panel:** Current ZPP token balance, today's matched releases from Founders Reserve, count of PENDING SIRs, recent SETTLED events with burn counts, recent REVERSED events.
- **SIR Activity Feed:** Live scrolling feed of new SIRs being minted, recent settlements, recent reversals. Each entry shows SIR ID, value, state, timestamp — fully anonymized (no user identifiers).
- **Transaction Volume:** Zak-It and Zap-It transaction counts (today / this month / all-time), aggregate USD value moved.
- **Cumulative ZKTC Burned:** Total ZKTC permanently destroyed across all sources — SETTLED SIR burns, RTU cashout burns, FLOP burns. Shows supply contraction in real time.
- **Three Invariants Live Check:** Real-time computation and display of Invariants 1, 2, and 3. Green check if all hold; red alert if any inconsistency detected (which should never occur given self-policing contract logic).
- **DCO Status (pre-launch only):** Current Donation Coin Offering phase, current price per ZKTC, tokens remaining in the active phase, progress visualization.
- **Contract Status Map:** All deployed contracts with addresses (linked to BSCScan), audit status, immutability status.

Privacy Architecture

The dashboard displays aggregated and anonymized data only. No individual user wallets, names, KYC identifiers, transaction recipients, or transaction details are publicly displayed. Donor identities are protected: only aggregate amounts and counts are shown publicly. Internal acknowledgment letters and 501(c)(3) receipts contain donor identity for the donor's tax purposes only; that data NEVER appears on the public dashboard.

The Dashboard As Trust Architecture

The Public Utility Dashboard is more than a marketing tool. It is a structural element of the protocol's trust architecture. By making operational reality publicly and continuously visible, the dashboard accomplishes what reports, audits, and white papers can only partially achieve: it converts *trust-by-claim* into *trust-by-evidence*.

Every minute the dashboard runs and the invariants check green is another minute of evidence that the architecture documented in this whitepaper is the architecture operating in reality. Over months and years, that evidence compounds. By Public Launch, the protocol will have accumulated 9 months of continuous, public, on-chain operational evidence — visible to every regulator, every scholar, and every prospective participant.

This is the strongest possible answer to the question, "How do we know it works?" You watch it work.

Section 36 — Parameter Design Principles

How protocol constants are calibrated and governed — documented in the Technical Protocol Appendix

The protocol's operational parameters — FLIP activation thresholds, FLIP hard caps, ODS activation parameters, FLOP distribution allocations, and related constants — are calibrated against five design principles rather than chosen arbitrarily.

1. **Bounded by Reserve Size** — injection and activation caps are sized as percentages of operational reserves, scaling proportionally.
2. **Time-Window Smoothing** — triggers reference time-weighted averages rather than instantaneous values.
3. **Concentration Penalty** — volume-based mechanisms are dampened when activity concentrates in few wallets.
4. **Hard-Coded Backstops** — each economic mechanism includes a `require()` statement enforcing a maximum effect per epoch.
5. **Three-Board Reauthorization** — when a hard cap binds, resumption requires approval from all three governance bodies.

Parameters are reviewed at three layers: internal calibration with documented stress testing, independent smart-contract audit, and ZCBS Shariah ratification. Once the protocol transitions to immutability, parameters become fixed at the EVM level. Full design rationale and governance mechanics are documented in **Appendix A.4**.

PART IX — OPERATIONAL DISCLOSURES & CLOSING

Mandated operational items and closing

Section 37 — Operational Disclosures

Environmental, complaint, and offering-completion disclosures

This section sets out operational disclosures concerning the environmental profile of the underlying network, the handling of user complaints, and the treatment of contributions where an offering phase does not complete.

Environmental & Energy Disclosure

ZKTC is a BEP-20 token deployed on the BNB Smart Chain. BNB Smart Chain secures its network through a proof-of-stake-based consensus mechanism operated by a bounded set of elected validators, rather than through proof-of-work mining. Proof-of-stake-based consensus does not rely on energy-intensive computational competition to add blocks, and consequently consumes substantially less energy per transaction than proof-of-work systems. Because ZKTC settlement occurs as standard token transactions on this chain, its per-transaction energy footprint is that of an ordinary BNB Smart Chain transaction.

Zakat Coin Inc. does not operate, validate, or control the BNB Smart Chain and does not independently determine its consensus mechanism or energy consumption; it relies on the network as a third-party public infrastructure provider. Zakat Coin Inc. sources any quantitative energy or carbon indicators it publishes from the network's own published data and recognized third-party measurement methodologies, and updates those indicators as such data is revised. Beyond its reliance on an inherently low-energy consensus mechanism, Zakat Coin Inc. does not make independent claims of carbon neutrality for its own operations.

Complaint & Redress Procedures

Zakat Coin Inc. maintains a process for receiving, acknowledging, and responding to user complaints and support requests. Users may submit a complaint or support request through the contact channels published on the project's official website. Each complaint is acknowledged upon receipt and reviewed, and the user is provided with a substantive response or resolution within a reasonable period. Where a complaint cannot be resolved to the user's satisfaction, Zakat Coin Inc. will explain the basis for its determination and identify any further options available to the user. Records of complaints and their resolution are retained to support review and continuous improvement of the service.

Treatment If an Offering Does Not Complete

Where a defined offering phase does not complete — for example, because a stated condition or threshold for that phase is not met — contributions attributable to that phase are handled in accordance with the terms of the applicable participation agreement. The governing principle is that contributions received for an offering phase that does not complete are returned to the contributing participants, net only of any irreversible third-party transaction costs where applicable, rather than being retained by Zakat Coin Inc. The specific mechanics, timing, and any applicable conditions of such returns are set out in the participation agreement applicable to each phase, which participants agree to at the point of contribution.

Section 38 — Closing

Zakat Coin is not a token that promises to support charity someday. It is a system in which charity is structurally inseparable from every transaction that flows through it. Every acquisition gives. Every hold rewards giving. Every ZakPay payment routes through Giving Contracts. Every settled SIR burns ZKTC permanently. Every token in the 14.25 billion supply has an operational job; none exists for managerial discretion or speculation.

ZakPay is the commercial engine that gives ZKTC its utility. ZKTC is the architectural layer that makes ZakPay trustworthy. The two were designed as one system, in which payments and charity are the same operational primitive expressed in different routing destinations — and the regulatory foundation is already in place: FinCEN MSB registered, patent filed and pending, fatwa issued and active, and institutional custodians engaged.

This is what it looks like to build halal financial infrastructure that can stand in front of any regulator, any scholar, and any institution in the world — not by asserting compliance, but by structuring it into every mechanism from the foundation up.

نِيَّةُ الْمُؤْمِنِ خَيْرٌ مِنْ عَمَلِهِ

The intention of the believer is better than his deed.

The intention has been right from day one. The infrastructure now matches it.

TECHNICAL PROTOCOL APPENDIX

Detailed mechanics for auditors, integrators, and sophisticated reviewers

About This Appendix

This appendix documents the architectural mechanics referenced in the main whitepaper at a level of detail intended for smart-contract auditors, partner integrators, and reviewers who require visibility into the protocol's internal logic. Readers seeking a higher-level overview can stop at Section 38 (Closing) without missing the document's structural arguments. The four sub-sections below correspond to four pointers from the main body: Section 15 (SIR/ZPP Invariants), Section 16 (Modular Architecture), Section 17 (Mutability Transition), and Section 36 (Parameter Design).

A.1 — SIR & ZPP Mathematical Invariants

For every payment instruction, there is a backing token. For every settled payment, there is a permanent burn.

The relationship between SIRs (Settlement Instruction Records, the on-chain proofs of payment instructions) and ZPP (the ZKTC Placeholder Pool, the holding layer for matched-release tokens governed by pending SIRs) is governed by three mathematical invariants. These are not narrative claims — they are equations enforced by smart contract logic, continuously verified on-chain, and publicly auditable by any participant with a block explorer.

The Three Invariants

> *Invariant 1 — ZPP Bounded-Reserve*
>
> $$ B_{\text{floor}} \le B_{\text{ZPP}} \le B_{\text{cap}} $$
>
> *The ZPP is maintained as a bounded settlement reserve rather than a pool that mirrors cumulative sales. Its balance stays within fixed floor and cap bounds enforced at the smart-contract level. The reserve is seeded from the Founders allocation and replenished, as settlement consumes it, through the protocol's own liquidity-overflow mechanism — never by drawing on any charitable allocation.*

> *Invariant 2 — ZPP State Equation*
>
> $$ B_{\text{ZPP}} = R_{\text{matched}} - I_{\text{in-flight}} + R_{\text{reversed}} - B_{\text{settled}} $$
>
> *where B_{ZPP} is the current ZPP balance, R_{matched} is cumulative matched releases, $I_{\text{in-flight}}$ is tokens currently locked in PENDING SIRs, R_{reversed} is cumulative REVERSED returns to ZPP, and B_{settled} is cumulative SETTLED burns. The four flows fully account for every token movement involving the ZPP.*

> *Invariant 3 — SIR-ZPP Mirror Symmetry*
>
> $$ \forall S \in \text{SIRs}, \forall T:\quad \text{Location}(S_T) = \begin{cases} S_{\text{contract}} & \text{if } S.\text{state} = \text{PENDING} \\ \texttt{0xdead} & \text{if } S.\text{state} = \text{SETTLED} \\ \text{ZPP} & \text{if } S.\text{state} = \text{REVERSED} \end{cases} $$
>
> *For every SIR at every block height, the location of its backing tokens must mirror its state. No fourth state is possible. The smart contract reverts on any inconsistency between SIR state and token location — the protocol is self-policing.*

The Triple Audit Trail

The Three Invariants are continuously verifiable on-chain through three independent layers of evidence:

1. **Event log:** Every release, settlement, reversal, and burn emits a standardized event with full parameters. Block explorers index these events by topic, enabling time-range queries against any ZPP or SIR state.
2. **State reads:** The current ZPP balance, current SIR state mapping, and cumulative release/burn counters are all readable from the smart contracts at any time, by any party.

3. **Public Dashboard:** The Public Utility Dashboard (see Section 35) displays a continuous real-time computation of all three invariants. Green check = invariant holds; red alert = inconsistency detected (which should never occur given the contract's self-policing logic).

A.2 — Modular Smart Contract Architecture

Many small contracts working together, not one mega-contract trying to do everything

The Zakat Coin protocol is implemented as a network of interconnected smart contracts, each with a specific responsibility — not as a single monolithic contract handling all functions. This is a deliberate architectural choice grounded in EVM technical constraints, industry best practice across the most mature DeFi protocols, and the operational requirements of audit, security, and maintainability.

The 24KB Constraint

The Ethereum Virtual Machine, inherited by BNB Smart Chain, imposes a maximum deployed contract bytecode size of approximately 24 kilobytes per contract. This ceiling, introduced in the Spurious Dragon hard fork in 2016 to mitigate denial-of-service attack vectors, makes monolithic contract implementations physically impossible at the protocol's scope. The contract *must* be split. This is not a design preference — it is a binding technical constraint.

Industry Precedent

Modular architecture is the dominant pattern across mature DeFi protocols — formalized in EIP-2535 (the Diamond Standard) and used in production by Aave, Uniswap, MakerDAO, Compound, and Safe. Zakat Coin applies a proven, audited pattern to a new domain rather than inventing one.

Five Concrete Benefits

1. **Within size limits.** Every individual contract stays well under the 24KB EVM ceiling. No deployment failures from oversized bytecode.
2. **Targeted, faster audits.** Auditors review one contract at a time. Per-contract findings rather than entangled bug interactions. Lower total audit cost.

3. **Reduced attack surface per contract.** A bug in one contract cannot drain a different contract. Each contract is its own security perimeter.
4. **Independent upgradeability during the pre-launch phase.** Individual contracts can be redeployed and rewired without redeploying the entire protocol (see Section 17).
5. **Clean composability.** FUSE, MagicBox, and ZakPay platform contracts communicate via well-defined interfaces — modular architecture enables integration without each system absorbing the others' logic.

A.3 — The Mutability-to-Immutability Strategy

The protocol begins life mutable. It ends life immutable. The transition is deliberate, sequenced, and ceremonial.

Why Mutability During the Pre-Launch Maturity Period

The period from Public Pre-Sale and ZakPay platform launch through Public ZKTC market launch is the protocol's maturity period. During this period, the protocol is operating live with real users and real transactions but is not yet subject to public market trading. Multiple sources of legitimate revision pressure exist during this window:

- **Audit findings.** a leading independent smart-contract audit firm audits may identify bugs during live operation that require correction.
- **Scholar refinement.** The Board of Scholars may identify edge cases requiring jurisprudential adjustment.
- **Regulatory feedback.** FinCEN, IRS, or state regulators may request parameter alignment with evolving guidance.
- **Operational learning.** Real transaction volume reveals optimization opportunities not visible in testnet conditions.

Individual contracts (excluding the live ZKTC token contract, which is already permanently immutable) are deployed during this period with upgrade authority held by a multi-signature wallet combining founders and Board of Scholars members. Upgrade patterns follow a secondary independent audit firm with EVM specialization's UUPS or Transparent Proxy standards — well-audited, industry-standard patterns.

Why Immutability at Mainnet Launch

Once ZKTC opens to public market trading at launch, the protocol becomes immutable. Three independent reasons each sufficient on its own justify this transition:

1. **Market trust.** Public market participants require certainty that the rules cannot change after they have purchased. An upgradeable contract under market trading is a centralization risk.
2. **Centralization risk reduction.** A central party retaining the ability to alter economic mechanics — even if never exercised — represents a centralization vector. Immutability removes this vector entirely.
3. **Shariah compliance.** *Gharar* (operational uncertainty) is impermissible. The ability for a central party to alter contract behavior IS *gharar*. Locking the contracts eliminates *gharar* at the architectural level.

The Immutability Transition Ceremony

At Public Mainnet Launch, the following sequenced events occur on-chain, publicly verifiable:

1. **Final audit completes.** a leading independent smart-contract audit firm signs off on the final state of all contracts.
2. **Final fixes deployed.** The last possible round of upgrades happens.
3. **Upgrade authority renunciation.** All contract upgrade authorities are renounced via standard mechanisms (UUPS upgrade functions removed, ProxyAdmin owners transferred to burn address, role-based admin roles renounced).
4. **Multi-signature key destruction.** The upgrade-authority multi-sig wallet is ceremonially decommissioned. Private keys are physically destroyed in a recorded ceremony witnessed by counsel, the Board of Scholars, and (where regulator presence is invited) FinCEN representatives.
5. **On-chain notarization.** The immutability transition is recorded in a final notarization transaction emitted on BSC mainnet, with all final contract addresses enumerated.
6. **Public Dashboard reflects locked state.** The Utility Dashboard displays the immutability transition prominently with cryptographic proof links.

What Remains Immutable at All Times

Certain protocol invariants are intrinsically unchangeable from the moment of deployment, independent of the renunciation ceremony:

- Operational supply hard cap: 14,250,000,000 ZKTC
- ZPP settlement reserve: bounded (floor and cap enforced in `ZKTCEngineAdapter`), replenished by protocol liquidity overflow, never from charity
- ZPP maintained as a bounded settlement reserve, seeded from the Founders allocation and replenished by protocol liquidity overflow; the Charity Reserve is never a settlement source
- The Three Mathematical Invariants — enforced as `require()` statements

- Founders Reserve allocation: 5,500,000,000 ZKTC
- Charity Reserve allocation: 6,000,000,000 ZKTC
- ZPP bounded-reserve limits (hard ceilings enforced in `require()` checks); Charity Reserve firewalled from settlement use

These cannot be changed even by the multi-sig upgrade authority during the mutable phase. Changing them would require deploying entirely new contracts to entirely new addresses, which would constitute a separate protocol, not an upgrade.

A.4 — Parameter Design Principles & Governance

How protocol constants are calibrated and governed

The protocol's operational parameters — FLIP activation thresholds, FLIP hard caps, ODS activation parameters, FLOP distribution allocations, and related constants — are calibrated against five design principles rather than chosen arbitrarily. Specific numerical values, derivation methodology, and calibration constants are documented in internal technical appendices reviewed by the ZCBS and by independent auditors during the audit cycle described in Section 34. This public document describes the principles; the technical appendices document the numbers.

The Five Design Principles

Principle	What It Means
1. Bounded by Reserve Size	Injection and activation caps are sized as defined percentages of operational reserves rather than absolute numbers. As reserves change, caps scale proportionally — ensuring the protocol cannot deplete itself through any single cap-bound event.
2. Time-Window Smoothing	Triggers reference time-weighted averages and multi-hour windows rather than instantaneous values. Smooths out flash events and short-term noise while remaining responsive to sustained pressure.

Principle	What It Means
3. Concentration Penalty	Mechanisms that activate based on commerce volume are dampened when activity concentrates in few wallets. Single-wallet dominance suppresses activation rather than amplifying it — preventing wash-volume attacks from inflating supply.
4. Hard-Coded Backstops	Each economic mechanism includes a `require()` statement enforcing a maximum effect per epoch. Even under oracle compromise or unexpected market conditions, no single event can exceed the hard backstop. The backstop exists at the EVM level, not at the multi-signature level.
5. Three-Board Reauthorization	When a hard cap binds, automatic operation pauses. Resumption beyond the cap requires approval from all three governance bodies (Zakat Coin Inc., Zakat Coin Organization Inc., and ZCBS) during the mutable phase. No single party can override caps unilaterally.

Parameter Governance & Review

Protocol parameters are subject to review at three independent layers before being deployed to production:

- **Internal calibration** — The Team performs stress testing and analytical derivation against documented market data and operational economics. Internal technical appendices document each parameter's basis.
- **Independent audit review** — Smart-contract auditors (Section 34) review parameters as part of the security audit, with particular attention to economic-attack vectors that depend on parameter choice.
- **ZCBS ratification** — The Zakat Coin Board of Scholars reviews parameters for Shariah-compliance implications before activation. ZCBS retains absolute veto authority.

Once the protocol transitions from mutable to immutable governance (Section 17), parameters become fixed at the EVM level and can no longer be modified by any party. The transition is itself subject to three-board approval, audit sign-off, and public ceremony.

ZUSD Launch Pricing & ZPP Matching

The Launch Price Discovery formula (Section 27) and the ZPP settlement-reserve model (Section 15) are derived from the principle that **token price is anchored to the operational economics of ZakPay commerce**. Because circulating supply expands only when real settlement occurs and contracts as SIRs burn, supply tracks genuine commercial activity rather than

speculative inflows — providing utility-anchored price discovery without treating acquisition as an automatic, unbounded supply-expansion vector.

GLOSSARY

Terminology for the ZKTC ecosystem

ZKTC

Zakat Coin — the utility engine token of the ZakPay ecosystem. BEP-20 token on BNB Smart Chain. Functions as the SIR placeholder for all ZakPay settlements and the trigger asset for Giving Contracts.

ZUSD

A stable token backed 1:1 by USDC, used for charitable disbursement and stable-value settlement within the Zakat Coin ecosystem. ZakPay is not the issuer; ZUSD is backed 1:1 by USDC, a regulated stablecoin, and presented as ZUSD within the ZakPay user experience. Non-interest-bearing.

ZakPay

The halal payment platform serving the global Muslim community. The commercial engine that generates the transactions, fee revenue, and utility consumption that activate ZKTC supply.

FUSE

Fiat Universal Settlement Engine — the patent-protected orchestration mechanism that coordinates blockchain payment instructions with regulated banking and payment counterparties to enable 1–3 second delivery of ZUSD-denominated value to local fiat in any jurisdiction where the ZakPay application is accessible to users and where licensed counterparty institutions are aligned. FUSE routes, governs, and audits the instruction; destination counterparties execute jurisdiction-specific settlement.

FLIP

Founders Liquidity Injection Protocol — the automated mechanism that maintains settlement-grade depth in the ZKTC liquidity pool by injecting tokens when pool depth falls below defined thresholds.

FLOP

Founders Liquidity Operations Protocol — the counterpart to FLIP. Redistributes pool overflow when depth exceeds ceiling, routing excess to permanent burn, charity, team liquidity, the ZUSD backing reserve, and operational treasury.

ODS

On Demand Supply — the patent-protected mechanism activating ZKTC supply exclusively from completed ZakPay settlement events. Supply cannot expand without real platform activity.

SIR

Settlement Instruction Record — the on-chain record minted at the moment of payment instruction creation, burned at settlement confirmation. The unit of utility consumption in the protocol.

ZPP

ZKTC Placeholder Pool — the multi-signature wallet that holds ZKTC backing all PENDING SIRs in the system. The asset-layer mirror of the SIR mechanism.

Giving Contracts

The unified family of smart contracts that route ZUSD to charity based on user actions. Triggered by acquire, hold, or sell events. Routes to ZCW (zakat) or SCW (sadaqah) based on user intent.

ZCW

Zakat Charity Wallet — the 501(c)(3)-owned wallet receiving all zakat-intent charitable distributions. Funds eligible only for the eight Quranic categories (*asnaf*) of zakat recipients.

SCW

Sadaqah Charity Wallet — the 501(c)(3)-owned wallet receiving voluntary sadaqah distributions. Funds the broader range of charitable causes consistent with Islamic charitable principles.

DCO

Donation Coin Offering — the umbrella term for all pre-public-market token distribution phases (Private DCO + Public Pre-Sale + Strategic Reserve allocations).

Zak-It

The ZakPay SEND action — peer-to-peer and international payment transfers via FUSE.

Zap-It

The ZakPay SPEND action — card payments via the ZakPay Visa/Mastercard card.

ZakatRated

The proprietary transparency-based approval system that verifies non-profit organizations for eligibility to receive distributions from the ZCW and SCW.

ZakPay Card

The Visa/Mastercard card issued by ZakPay (through a regulated card-issuing partner) enabling Zap-It card spending. Every tap generates a SIR.

MagicBox

The universal adapter layer that translates between sponsor banks, institutional brokerage and prime liquidity counterparties, regulated stablecoin issuance, qualified custody, and the FUSE orchestration engine into a single unified API — the integration layer that makes the multi-partner infrastructure invisible to users.

FinCEN MSB

Financial Crimes Enforcement Network — Money Services Business registration. Zakat Coin Inc. holds active MSB registration No. 31000302240755.

Mal mutaqawwam

A valid Shariah-recognized asset with lawful usufruct (*manfa'ah*). The Shariah classification of ZKTC.

Tabarru'

Voluntary charitable donation in Islamic jurisprudence. The classification of the charitable component within the ZKTC ecosystem — independent of the sale contract.

Nisab

The minimum wealth threshold above which zakat becomes obligatory in Islamic jurisprudence. Calculated annually based on gold and silver prices.

Hawl

The one lunar year holding period after which zakat obligation accrues on qualifying wealth.

Asnaf

The eight Quranic categories of zakat recipients (Qur'an 9:60). The exclusive eligible destinations for zakat-intent distributions.

Gharar

Operational uncertainty in Islamic jurisprudence. The protocol's architecture is designed to minimize *gharar* at every layer.

LEGAL NOTICES & DISCLAIMERS

Not a Securities Offering

ZKTC is a utility token. This whitepaper does not constitute an offer to sell or a solicitation to buy any security. ZKTC tokens are acquired solely for access to the ZakPay platform and its charitable giving mechanisms. No expectation of profit from token appreciation exists, and ZKTC serves purely functional purposes within the halal financial ecosystem.

Not Investment Advice

Nothing in this whitepaper constitutes investment advice, financial advice, legal advice, tax advice, or any other form of professional advice. Participants should conduct their own due diligence and consult qualified legal, financial, and tax counsel before acquiring ZKTC.

Forward-Looking Statements

This document contains forward-looking statements regarding the protocol's design, planned features, and operational trajectory. Actual results may differ materially. Adoption rates, volume projections, charitable impact figures, and timing milestones are estimates based on stated assumptions and are not forecasts or guarantees. The Public Launch Price emerges from a deterministic formula resolved at the launch block; no specific price is forecast, predicted, or guaranteed by this document or by any party.

Regulatory Risk

Cryptocurrency regulation continues to evolve in all jurisdictions. Zakat Coin Inc. holds active FinCEN MSB Registration No. 31000302240755 and is represented by independent IP counsel. Material regulatory changes may affect operations. Participants should monitor regulatory developments in their jurisdiction.

Patent Protection

The FUSE engine, SIR mechanism, ODS supply system, and related architectural mechanisms are protected under non-provisional patent application 19/640,087 via independent IP counsel, and a corresponding PCT international application. Additional patents 63/805,645 and 63/838,299 cover related utility mechanisms.

Shariah Compliance

Shariah compliance certification issued by joint fatwa from the inaugural Zakat Coin Board of Scholars. The Zakat Coin Board of Scholars (ZCBS) conducts ongoing quarterly reviews. Scholar names, credentials, and the full fatwa text are published in the public fatwa archive maintained on the ZakPay platform website. **Acquiring ZKTC does not constitute zakat fulfillment.** The obligation of zakat remains a personal religious duty upon each eligible Muslim.

---

legal@zktcoin.com · zktcoin.com · zakpay.com