Verifyz Protocol

Verifyz Protocol Whitepaper

"Real proof in presence."

Abstract

The token model sustains itself through transaction fees, community incentives, and a one-of-a-kind presale structure in which five early supporters receive lifetime rewards.

Introduction / Problem Statement

The modern data economy is broken. Individuals' data is routinely harvested without consent, resold without transparency, and monetized with little to no benefit for the people who create it. Industries struggle to access verified, reliable data without breaching privacy, creating inefficiency, mistrust, and lost opportunities.

Key issues in the current system:

* Users do not control their own data.

* Businesses rely on incomplete or unreliable third-party datasets.

* Incentive structures are misaligned, rewarding corporations but excluding individuals.

The Verifyz Solution

Proof of Presence (PoP) Flow

Objective

Enable users to prove “I was here, at this time, for this event” without revealing their identity or exact location. Proofs are validated on-chain, and all sensitive data remains private.

Actors

* User Device (Verifyz mobile/web app)

* Event/Venue (issues one-time challenge via QR/NFC)

* Verifier Contract (Polygon) (validates zero-knowledge proofs)

* Rewards Escrow (handles payouts)

Step-by-Step Flow

* Event Creation: Venue posts eventId, geofence, and time window to the blockchain. Event parameters are stored immutably.

* Challenge Issued: A user scans a QR code or taps NFC at the venue. The challenge includes {eventId, nonce, expiresAt}.

* Proof Generation (on device): The app collects GPS (rounded to geohash), device attestation, and venue challenge. It then builds a zero-knowledge proof that validates location, time, challenge, and attestation. No raw GPS or identity ever leaves the device.

* Proof Submission: The user app submits a proof + nullifier (which prevents double claims) to the Verifier contract. The contract validates the proof and logs success.

* Reward Settlement: When the VerificationRewards.sol contract is deployed in a later phase, the Rewards Escrow will release tokens to the user's wallet, pegged dynamically to a $2 USD equivalent in VFYZ per check-in.

Anti-Cheat Protections

* GPS Spoofing Prevention → requires device attestation and a QR/NFC challenge.

* Replay Attacks → QR/NFC tokens expire quickly.

* Double Claims → nullifiers ensure one claim per event per device.

* Remote Collusion → optional Wi-Fi/BLE signal hashes tied into the proof.

Public vs Private

* On-Chain (Public): eventId, proof, nullifier, minimal event parameters.

* Off-Chain (Private): raw GPS, Wi-Fi, device identity, personal info.

Sequence Diagram (simplified)

User Device Venue(QR/NFC) Verifier(Polygon) Rewards Escrow

|------------ scan challenge ------------->|

|---- build ZK proof (local signals) ------->|

|---- submit tx {proof, eventId, nullifier}->|

| |--- verify ------->|

| |<- PresenceVerified|

|<---------- reward ---|

Benefits

* Privacy-first verification – Individuals prove presence without exposing identities.

* Decentralized trust – Verification runs on immutable smart contracts.

* User rewards – Participants and presale winners benefit financially from the ecosystem.

* Industry-grade data – Businesses receive clean, verified, anonymous data streams.

For individuals → ownership of their presence and fair rewards, pegged to approximately a $2 USD equivalent in VFYZ per Proof of Presence check-in.

For businesses → trustworthy data without legal/ethical risks.

For communities → sustainable incentives tied to growth.

Technology & Architecture

VeriFyz Protocol will deploy all smart contracts on the Polygon blockchain. Polygon was chosen for its low transaction fees, scalability, and compatibility with Ethereum tooling, ensuring that VeriFyz Protocol can support both trading activity and Proof-of-Presence verification events efficiently.

* Smart Contracts: Govern token distribution, presale rewards, and fee allocations.

* App Ecosystem: Mobile/web interface integrates verification, token rewards, and industry dashboards.

TOKENOMICS

Category	% of Supply	Tokens	Notes
Presale / Public Sale	35%	175,000,000	Vesting: 25% TGE, remainder linear unlock 6–12 months
Team (Jason & Joshua)	20%	100,000,000	12-month cliff, 24-month linear vesting; 50/50 split
Development & Marketing	20%	100,000,000	12-month vesting; quarterly unlocks; transparent treasury reports
Liquidity & Listings	15%	75,000,000	Locked in LP for 24 months; used for exchange listings
Community & Partnerships	10%	50,000,000	20M for airdrops, 30M for partnerships and ecosystem grants

Total Supply: 500,000,000 VFYZ (fixed, no minting or burning).

Allocation Breakdown

| Category | Percentage | Tokens | Details |

| :--- | :--- | :--- | :--- |

| Presale / Public Sale | 35% | 175M | N/A |

| Team (Jason & Joshua Emerick) | 20% | 100M | Split equally, locked with 12-month cliff + 24-month vesting |

| Development / Marketing / Operations | 20% | 100M | Immediately liquid, funding salaries, campaigns, and development |

| Liquidity & Exchange Listings | 15% | 75M | Dedicated to LPs and exchange fees |

| Community Growth / Partnerships | 10% | 50M | 20M for airdrops, 30M for partnerships |

Presale Details

Investors will use MATIC (the native Polygon token) to purchase VFYZ tokens during the presale at a fixed price of $0.05 per token. Following the presale, VFYZ will be tradable on decentralized exchanges (DEXs) such as QuickSwap and Uniswap (Polygon).

Dynamic Reward Model

Each Proof of Presence check-in pays participants the equivalent of $2 USD in VFYZ tokens, based on real-time Chainlink oracle price feeds. Rewards automatically scale with market value, ensuring sustainability.

Examples:

* If VFYZ = $0.05 → reward ≈ 40 VFYZ

* If VFYZ = $1.00 → reward ≈ 2 VFYZ

* If VFYZ = $10.00 → reward ≈ 0.2 VFYZ

This guarantees users predictable, fair incentives while protecting the long-term token supply.

Transaction Fee Model

The VeriFyz Protocol enforces a 5% transaction fee structure at the contract level. The allocation is automated and directed as follows:

* 1% is routed to the Rewards Wallet (0xDde2aD00BCdc1566c671a31b50a433796d50Eedf), which funds the lifetime reward system.

* 4% is routed to the Treasury Wallet (0xfaef76c67366b3948d11b4d846775a6cc7389c4d), which supports development, marketing, and future protocol growth.

These addresses are permanently visible on-chain, ensuring transparency and accountability.

Roadmap

Phase 1 – Presale (September 8th – September 22nd)

* 3-week presale window.

* Token distribution + allocation to 5 lifetime reward winners.

* Marketing push and community onboarding.

Phase 2 – Immediate Blockchain Launch (Wednesday, October 1st)

* Smart contract deployment.

* Token live for trading.

* Liquidity pool seeded + first exchange listings.

Phase 3 – Functional App (Existing Build) – (Months 1–12)

* Transaction fee integrations active with the dynamic $2 USD reward model in place.

* Closed testing with selected users/partners.

* Community growth via airdrops, incentives, and network expansion.

Phase 4 – Full App Rollout (Year 2)

* Public release of the full-featured Verifyz Protocol app.

* User dashboards, advanced privacy tools, and analytics for businesses.

* Expanded industry pilot programs.

Phase 5 – Expansion & Enterprise Adoption (Year 3+)

* Global rollout of the Verifyz app ecosystem.

* AI-driven analytics integrated for enterprise partners.

* International adoption initiatives.

* Long-term sustainability powered by the transaction fee treasury.

Verification Contract Roadmap

The VeriFyz Protocol will roll out automated verification rewards in alignment with the launch of the Proof of Presence (PoP) application. This ensures sustainable and scalable incentives without overcomplicating the initial deployment.

Timeline:

* Presale + Launch: Lifetime reward wallets are active immediately, funded by the 1% fee on all transactions.

* Year 1: Focus on adoption, trading, and growth; verification rewards are funded manually from

pre-allocated supply or treasury funds.

* App Release (~1 Year): Deploy the VerificationRewards.sol contract to automate payouts for users completing verified presence events.

Funding Sources:

* Pre-allocated reward pool in tokenomics.

* Treasury funds (4% fee allocation).

* Future revenue streams (enterprise adoption, buybacks, partnerships).

Brand Identity

The blue-purple gradient fingerprint design symbolizes identity and trust, while the circuit-like nodes to the right evoke a decentralized, tech-forward network. Together, they reflect the protocol's core mission: enabling secure, private, and verified presence in a digital world.

Note

This whitepaper is a living document and will be updated as the Verifyz Protocol evolves. For the latest version or inquiries, please visit the official Verifyz Protocol website or contact the development team.

VRF Randomness & Audit / Security Plan

VRF Randomness & Lifetime Rewards

* Purpose: Ensure the selection of the 5 "lifetime rewards" wallets is fair, transparent, and provably random.

* Mechanism: Chainlink VRF (Verifiable Random Function) is integrated into the presale contract. At the presale close, VRF generates a random seed. From that seed, 5 distinct wallet addresses are selected from presale participants. The VRF proof is stored on-chain and verifiable by anyone. The rewards contract permanently routes 1% of transaction fees to these 5 wallets.

* Key Properties: Tamper-proof, publicly verifiable, and immutable.

Audit & Security Plan

* Audit Commitments: Targeted firms include OpenZeppelin, Certik, or Trail of Bits.

* Timeline: Smart contracts will be submitted post-presale, with reports published before the full launch.

* Scope: Presale contract (allocation, lockups, VRF), Proof of Presence verifier, Rewards escrow, and vesting mechanics.

Bug Bounty

Community/security researchers will be rewarded for responsible disclosures of vulnerabilities after audits.

Threat Model

* Location Spoofing – mitigated via device attestation + QR/NFC.

* Replay Attacks – prevented with short-lived QR/NFC challenges.

* Sybil/Duplicate Claims – blocked with nullifiers per event/device.

* Contract Exploits – minimized via audit, timelocks, and multisig-controlled upgrades.

* Liquidity Attacks – mitigated with LP lock (24 months).

Governance & Compliance

* Timelocked Governance – parameter changes are delayed 48–72 hours after a community vote.

* GDPR/CCPA Compliance – raw data never leaves the device; only hashes/proofs are on-chain.

* Biometric Data Policy – if biometrics are added later, they will remain off-chain and privacy-protected.