

* 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.

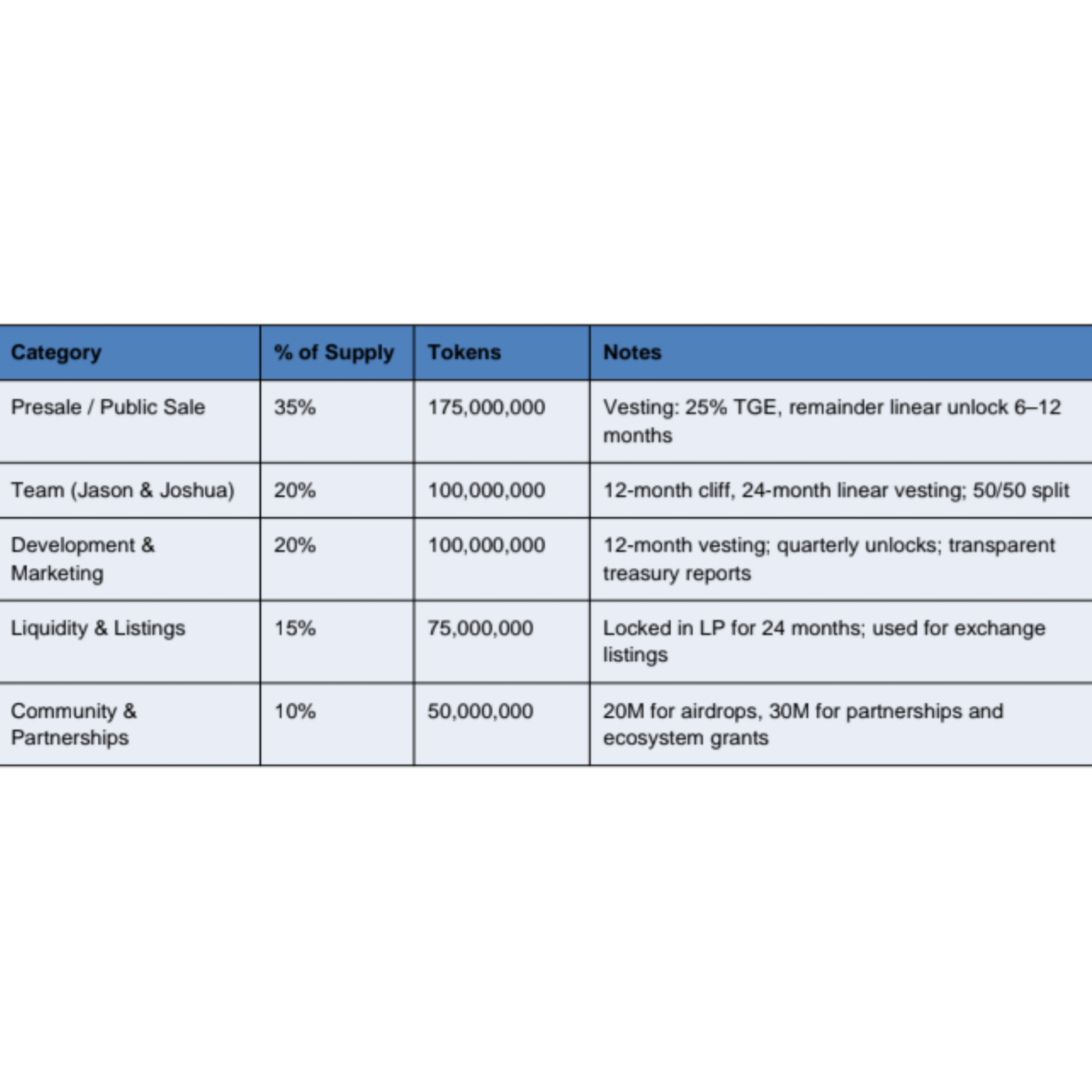
# The Verifyz Solution

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, rewards distributed automatically, 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  
  
1 Event Creation: Venue posts eventId, geofence, and time window to blockchain. Event  
parameters stored immutably.  
  
2 Challenge Issued: User scans a QR code or taps NFC at the venue. Challenge includes {eventId,  
nonce, expiresAt}.  
  
3 Proof Generation (on device): App collects GPS (rounded to geohash), device attestation, and  
venue challenge. Builds a zero-knowledge proof that validates location, time, challenge, and  
attestation. No raw GPS or identity ever leaves the device.  
  
4 Proof Submission: User app submits proof + nullifier (prevents double claims) to the Verifier  
contract. Contract validates proof and logs success.  
  
5 Reward Settlement: Rewards Escrow releases tokens to the user wallet. Optionally, a Presence  
Receipt (soulbound token) is minted for analytics and reputation.  
  
Anti-Cheat Protections  
  
• GPS Spoofing Prevention → requires device attestation and 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 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 ---|

* 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. Benefits:
* For individuals → ownership of their presence and fair rewards.
* For businesses → trustworthy data without legal/ethical risks.
* For communities → sustainable incentives tied to growth.

# Technology & Architecture

* Govern token distribution, presale rewards, and fee allocations. App Ecosystem
* Mobile/web interface integrates verification, token rewards, and industry dashboards.



# Transaction Fee Model

5% per transaction

* 1%→ Lifetime Rewards Pool (split equally among 5 presale winners).
* 4% → Project Treasury (1.5% Development, 1.5% Marketing/Operations, 1% Liquidity).

# Roadmap

Phase 1 – Presale (Weeks 1–3)

* 3-week presale window.
* Token distribution + allocation to 5 lifetime reward winners.
* Marketing push and community onboarding. Phase 2 – Immediate Blockchain Launch (Week 4)
* 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.
* Closed testing with selected users/partners.
* Community growth via airdrops, incentives, and network expansion. Phase 4 – Full App Rollout (Year 2)
* Public release of full-featured Verifyz Protocol app.
* User dashboards, advanced privacy tools, analytics for businesses.
* Expanded industry pilot programs.

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

* Global rollout of Verifyz app ecosystem.
* AI-driven analytics integrated for enterprise partners.
* International adoption initiatives.
* Long-term sustainability powered by the transaction fee treasury.

# Brand Identity

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) integrated into the presale contract.  
  
• At 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.  
  
• Rewards contract permanently routes 1% of transaction fees to these 5 wallets.  
  
Key Properties  
  
• Tamper-proof – team/participants cannot manipulate outcome.  
  
• Publicly verifiable – VRF proof published and queryable on PolygonScan.  
  
• Immutable – once selected, winners cannot be changed.  
  
Audit & Security Plan  
  
Audit Commitments  
  
• Targeted firms: OpenZeppelin, Certik, or Trail of Bits.  
  
• Timeline: smart contracts submitted post-presale, reports published before full launch.  
  
• Scope: Presale contract (allocation, lockups, VRF), Proof of Presence verifier, Rewards escrow,  
vesting mechanics.  
  
Bug Bounty  
  
Community/security researchers 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, multisig-controlled upgrades.  
  
• Liquidity Attacks – mitigated with LP lock (24 months).  
  
Governance & Compliance  
  
• Timelocked Governance – parameter changes delayed 48–72 hours after community vote.  
  
• GDPR/CCPA Compliance – raw data never leaves device; only hashes/proofs on-chain.  
  
• Biometric Data Policy – if biometrics added later, remain off-chain and privacy-protected.