# VOID SYSTEM Whitepaper v1.0

**Private, Trust-Minimized Solana Rail**

**Date:** March 2026

**Website:** https://voidsystem.site

## 1. Executive Summary

VOID SYSTEM is a privacy-preserving rail for Solana and connected chains. It enables confi

**Core utility**

- Private transfers of SOL, USDC, and wrapped assets
- Cross-chain remittances without KYC exposure
- Privacy-first DeFi interactions (swaps, lending, OTC)
- Low fees, fast finality (~30–90 seconds depending on route)

## 2. Problem Statement

Public blockchains leak every detail: sender/receiver, amounts, and hop graphs. Bridges extend those

## 3. Solution Overview — VOID SYSTEM Protocol

1. **Shielded deposit / burn-mint** inspired by Sapling + RenVM.
2. **Zero-knowledge proofs** for cross-chain validity without revealing routes.
3. **Guardian relayer network** (permissionless, incentivized by VOID token fees).
4. **Multi-chain shielded pools** (per-chain note trees).
5. **Selective disclosure keys** for auditors.

**Flow**

1. Deposit asset on source chain into a shielded pool (note created).
2. Generate zk-proof of valid commitment burn.

3. Guardian submits proof to destination contract.

4. Destination mints wrapped/private equivalent.

5. Recipient claims privately; sender and amount remain hidden.

## 4. Technical Architecture

### 4.1 Cryptographic Primitives

- Pedersen/Bulletproof commitments for value hiding.
- Groth16 + PLONK/Halo2 hybrid proving.
- Dual-key stealth addresses (view + spend).
- Nullifiers prevent double-spend across chains.
- Merkle trees for Sapling-style note commitments.

### 4.2 Bridge Components

- Source chain vault contracts locking deposits.
- zk-prover marketplace producing succinct proofs.
- Relayer incentives (VOID token + fee share 0.05–0.3%).
- Destination mint contracts verifying proofs and minting private credits.
- Challenge period (1–4 hours) combining optimistic checks + zk fallback.

**Initial chains:** Solana native, Polygon, Arbitrum, BNB, Ethereum, Bitcoin (BitVM adapters).

## 5. Tokenomics — VOID Token

- **Total supply:** 1,000,000,000 VOID (fixed, deflationary via fee burns)
- **Allocation:**
  - Liquidity & Farming — 25%
  - Team & Advisors — 15% (3-year vest)
  - Ecosystem / Grants — 20%
  - Relayer & Prover Rewards — 20%
  - Treasury / DAO — 15%
  - Private Sale / Seed — 5% (locked)

**Utility**

- Pay bridge fees (discount tiers for holders)
- Stake for guardian/relayer priority

- Governance voting on upgrades
- Fee sharing for stakers

**Deflation:** 30% of protocol fees burned permanently.

## 6. Security & Risk Mitigation

- Independent audits (Trail of Bits, PeckShield, zksecurity)
- Bug bounty up to $500K
- Relayers stake VOID; malicious proofs are slashed
- Progressive decentralization: multisig guardians → DAO
- Known risks mitigated through mandatory zk verification, formal proof audits, optimistic+zk hybri

## 7. Roadmap

- **Q2 2026** — Testnet (Solana ↔ Polygon)
- **Q3 2026** — Mainnet v1 + private stablecoin support
- **Q4 2026** — Cosmos IBC + Bitcoin adapters
- **Q1 2027** — Mobile SDK + institutional Fog Pools
- **H2 2027** — Full DAO governance + programmable privacy DeFi

## 8. Team & Advisors

- Founder/Lead Dev: anonymous zk/bridge veteran
- Contributors: ex-Zcash, Aztec, Polygon zkEVM engineers
- Advisors: privacy researchers, bridge security experts

## 9. Conclusion

VOID SYSTEM lets operators move value silently while staying audit-ready. As surveillance incre

**Disclaimer:** Informational only. Token distributions remain subject to local regulations. No guara