SolanaBlender: Technical Whitepaper

1. Introduction

SolanaBlender is a privacy-focused obfuscation tool designed for the Solana blockchain. It enables users to anonymize SOL by routing funds through a complex, randomized path of stealth wallets, decoys, and timed delays-ensuring unlinkable outputs.

This whitepaper outlines the architecture, security model, and future roadmap of the platform.

2. Architecture Overview

SolanaBlender operates without smart contracts or tokens. It is a wallet-layer, off-chain tool running on a FastAPI backend, supported by system-level protections and deterministic wallet logic.

Main Components:
- API endpoints (FastAPI) for session handling
- Temporary filesystem-based wallets (solders.Keypair)
- Secure routing logic in `transfer_engine.py` and `decoy_engine.py`
- Telegram-integrated security monitoring

3. Wallet Obfuscation Flow

The obfuscation process begins with `generate-deposit`, creating a unique Keypair for each session. When the user deposits SOL, the backend initiates a session that:

- Creates 16 randomized hop wallets
- Inserts stealth forks (decoy branches)
- Introduces randomized delays (jitter) between transfers
- Ends with a final wallet, presented to the user in base58 form

Each hop wallet is burned (drained to the system burn address) after use.

SolanaBlender: Technical Whitepaper

4. Session Lifecycle

Each session is sandboxed under `sessions/<session_id>/` and follows a strict sequence:

1. `POST /generate-deposit` -> generates deposit wallet
2. `GET /check-balance/{session_id}` -> polls for deposit arrival
3. `POST /start-cleaning` -> initiates cleaning
4. `GET /check-cleaning-status` -> returns private key, balance, and progress

Logs, wallets, and status files are auto-cleaned after expiry.

5. Decoys and Timing Security

Decoys are forked branches triggered in parallel during main cleaning. They:

- Mimic wallet movement patterns
- Randomize amounts and delays
- Burn all outputs to void addresses

Jitter is introduced in sleep cycles between hops to prevent timing-based chain analysis.

6. Security Infrastructure

- IP banning via Fail2Ban (including 404 and `/wp-login.php` probes)
- Telegram alerts on session creation, wallet seeding, and suspicious pings
- No analytics, tracking cookies, or on-chain identifiers
- Dedicated .onion mirror for censorship-resistant access
- Referral system uses localStorage, not cookies or backend auth

Each endpoint is rate-limited and monitored.

SolanaBlender: Technical Whitepaper

7. Referral System

Users may share referral links using `?ref=yourcode`, stored client-side. On session completion, referrals are logged to `sessions/<id>/referral.json` and aggregated via a daily cron script.

Referrers can earn a configurable percentage of the cleaning volume.

8. Roadmap

Phase 1: Completed

- FastAPI backend
- Obfuscation logic
- Telegram + IP security
- Public launch (.onion + clearnet)

Phase 2: In Progress

- Cross-chain support: BTC and ETH via oBTC/oETH wrappers
- Referral analytics dashboard

Phase 3: Aspirational

- Token governance (if justified)
- DAO-like model for config votes
- CEX-facing stealth wrapper integration

Phase 4: Long-Term Vision

- Zero-trust relay nodes
- On-chain triggers via zk-proof commit states
- Mobile UX enhancements

9. Contact and Transparency

SolanaBlender: Technical Whitepaper

SolanaBlender.com is operated pseudonymously and publishes security signals via @solanablender_bot.

Public key: PGP fingerprint available on the site

Latest whitepaper version: 2025-05-22

Access via Tor: http://[your-onion].onion

Email: support@solanablender.com (PGP encrypted preferred)

8.1 Zcash Integration Plans

As part of our privacy-first expansion, we are integrating Zcash (ZEC) into our noncustodial swap engine,

- Support for both shielded and transparent ZEC addresses.
- Compatibility with lightwalletd, zcashd, and future Orchard upgrades.
- Use of script-based swaps triggered by shielded memos.
- Preservation of ZEC's anonymity properties throughout the swap process.
- Optional shielding/de-shielding at entry and exit points.
- Swap integration on both SolanaBlender.com and StealthXMR.io.

ZEC support will expand our reach to privacy-conscious users who want to move value between ecosyste

StealthXMR.io will serve as the public-facing access point for ZEC swaps. The backend architecture will