SolSeal Protocol

Encrypted Balance Infrastructure for Solana

Litepaper - Simplified Technical Overview

SolSeal Protocol Team
solseal.xyz

February 9, 2026

Abstract

SolSeal is a privacy-focused protocol for Solana blockchain. It has two main parts: **Part I** provides basic privacy tools for hiding balances and transactions (already live on mainnet), while **Part II** introduces advanced features for earning yields in DeFi while maintaining privacy (in development). This setup helps users and institutions keep their finances private without losing Solana's speed and efficiency.

1 Part I: Core Privacy Tools

1.1 Why Privacy Matters on Solana

Solana's architecture exposes all balances and transactions publicly—essential for trustless verification but problematic for financial privacy. Users managing significant positions, executing trading strategies, or conducting business operations face a fundamental transparency problem.

Existing privacy tools fall short. Traditional mixers obscure transaction linkages but leave amounts visible. If you deposit 5 SOL, observers see 5 SOL entered. Even when connections between deposits and withdrawals are hidden, the values themselves remain public. Worse, mixers tie funds to specific wallet addresses, enabling probabilistic attribution through timing and behavioral analysis.

SolSeal takes a different approach: encrypted balance vaults. Your balance exists as scrambled ciphertext on-chain—computationally indistinguishable from random data to any observer lacking your secret key. This provides persistent privacy throughout deposits, internal operations, and withdrawals.

1.2 How It Works

Vault Creation

Users generate a secret key locally—never transmitted on-chain or to servers—and create an encrypted vault. Unlike traditional accounts tied to wallet addresses, vaults are controlled by cryptographic keys. Ownership remains private through this separation.

Deposits & Withdrawals

Depositing funds encrypts the amount immediately. Observers see a transaction occurred but cannot determine the size. A 0.25% fee supports protocol operations. Withdrawals require generating a zero-knowledge proof (5-15 seconds client-side) demonstrating sufficient balance without revealing the amount to validators.

Stealth Transfers

Send encrypted amounts between vaults in two transactions (Solana's size limit requires splitting). Transfer values remain hidden throughout both phases—neither sender nor recipient amounts are publicly visible.

The system employs **homomorphic encryption** enabling mathematical operations on encrypted balances without decryption. Quick balance recovery via encrypted "hints" achieves ∼50ms average discovery time.

1.3 Tech Basics (Simplified)

SolSeal employs **additively homomorphic encryption**, allowing mathematical operations on encrypted balances without decryption. The protocol can verify deposits, withdrawals, and transfers without ever seeing plaintext values—everything remains encrypted on-chain.

Zero-knowledge proofs complement this encryption layer. Users prove they have sufficient funds or proper authorization without exposing balances to validators or observers. Each proof demonstrates validity while revealing nothing about the underlying amounts.

The system implements **dual authentication**: transactions require both a Solana wallet signature (standard blockchain authorization) and a secret key (cryptographic proof generation). Compromising only one factor cannot move funds.

Status: Live on Solana mainnet. Performance: Fast transactions (<1 second finality), low costs.

1.4 System Parameters & Security

Scale & Capacity

The protocol supports balances up to approximately 281,000 SOL per vault—more than sufficient for institutional treasuries and trading operations. Users requiring larger holdings can employ multiple vaults with independent keys.

Attack Resistance

The system prevents common threats: replay attacks through nonce binding, inflation attacks through zero-knowledge proof verification, and front-running through encrypted amounts. An attacker gaining access to a user's Solana wallet cannot decrypt balances or generate valid proofs without the separate secret key.

2 Part II: Privacy for DeFi Yields

2.1 The Institutional Opportunity

Corporate treasuries, trading firms, and fund managers seek DeFi returns—protocols like Kamino and Marinade offer 8-15% APY compared to 2-3% in traditional finance. But public balances create a dealbreaker: institutions cannot expose position sizes, deployment strategies, or treasury reserves to competitors, vendors, and adversaries.

Part II extends SolSeal's encrypted vault infrastructure to institutional yield generation. Same proven technology, enhanced with compliance features and yield integration.

2.2 Privacy Pool Architecture

The solution aggregates encrypted deposits into **privacy pools**. Multiple users contribute encrypted amounts—the pool knows the aggregate total but cannot see individual balances. This pooled capital deploys to yield protocols (Kamino, Marinade) as a single institutional-sized position.

From the yield protocol's perspective, they receive one large deposit and return interest normally. They never see individual users or encrypted amounts—**no protocol modifications required**.

Users receive **encrypted delegation tokens** representing their pool share. As yields accrue, share values appreciate proportionally. Users withdraw their grown shares privately—amount remains encrypted end-to-end.

Integrates with top Solana protocols like Kamino and Marinade—no changes needed on their side.

2.3 Compliance Infrastructure

Institutional adoption requires regulatory auditability without market exposure. Part II introduces **viewing keys**: read-only access for authorized auditors or regulators, granted at the institution's discretion. This enables compliance verification while maintaining privacy from market participants.

Pre-deposit screening integrates with compliance oracles (Chainalysis, TRM Labs), verifying addresses against sanctions lists before accepting funds. Users prove they passed screening via zero-knowledge proofs—satisfying compliance without broadcasting identity publicly.

This aligns with emerging frameworks like the **GENIUS Act**, establishing federal standards for compliant privacy infrastructure in digital assets.

3 Development Roadmap & Milestones

3.1 Completed Milestones (✓)

Milestone	Achievement
✓	**Core Protocol Design** - Encrypted vault architecture finalized
✓	**Cryptographic Primitives** - ElGamal encryption & Groth16 ZK proofs implemented
✓	**O(1) Hint System** - ECDH-based hint mechanism deployed
✓	**Smart Contract Development** - On-chain programs completed and tested
✓	**Mainnet Deployment** - Part I live on Solana mainnet
✓	**User Interface** - Web application for vault management
✓	**Initial Security Audit** - Internal security review completed

Table 1: Completed development milestones for Part I

3.2 In-Progress & Upcoming Milestones

Phase	Key Milestones	Timeline
3***Phase 1**	Viewing key architecture design Multi-recipient encryption implementation Threshold decryption committee (5-of-9)	3*2-3 months
3***Phase 2**	Compliance oracle integration (Chainalysis/TRM) Pre-deposit screening smart contracts Regulatory reporting dashboard	3*1-2 months
3***Phase 3**	Delegation token smart contracts Kamino/Marinade integration wrappers Privacy pool deployment mechanisms	3*2-3 months
3***Phase 4**	External security audits (Trail of Bits, Zellic) Bug bounty program launch Institutional pilot deployment	3*2-3 months

Table 2: Development roadmap for Part II (Privacy Yield)

3.3 Success Targets

- **Total Value Locked (TVL):** $100M+ within 12 months of Part II launch
- **Institutional Users:** 10+ corporate treasuries, funds, or trading firms
- **Yield Competitiveness:** Within 50 basis points of transparent alternatives
- **Privacy Pool Adoption:** >95% of institutional volume through privacy pools
- **Regulatory Compliance:** Zero enforcement actions, proactive engagement

4 Technical Architecture Overview

4.1 Part I: Encrypted Balance System

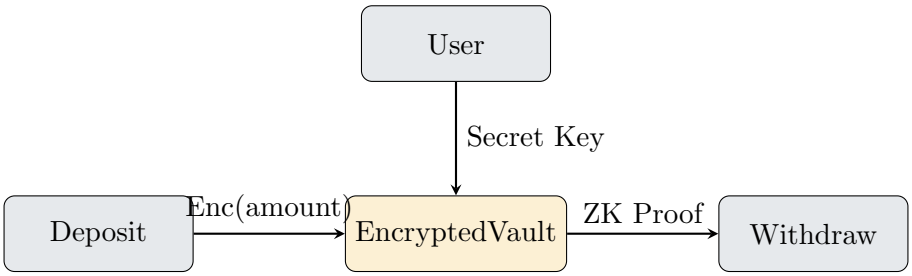

Figure 1: Simplified encrypted vault operation flow

4.2 Part II: Privacy Yield Architecture

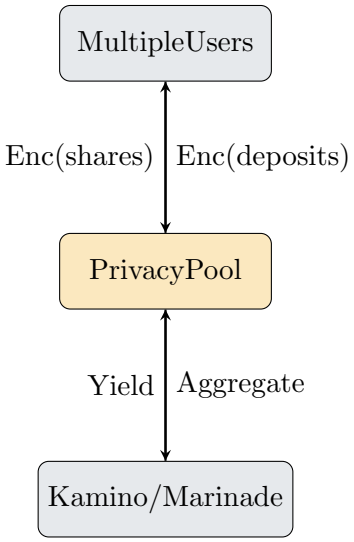

Figure 2: Privacy pool yield distribution mechanism

5 Key Differentiators

6 Target Integrations (Part II)

Liquid Staking:

- Jito ($1.87B TVL)
- Marinade ($1B+ TVL)

Lending & Yield:

- Kamino Finance ($2.36B TVL)
- Jupiter Lend ($1.65B TVL)

DEX Liquidity:

- Raydium ($1.47B TVL)
- Orca (concentrated liquidity)

Real-World Assets:

- Ondo Finance (tokenized Treasuries)

Feature	SolSeal Advantage
Hidden Balances	Permanently encrypted amounts (not just transaction mixing)
O(1) Discovery	Instant balance updates via hints (∼50ms vs. minutes of scanning)
Secret Key Ownership	Wallet-independent access; prevents ownership attribution
Partial Withdrawals	Withdraw any amount (vs. fixed denomination mixers)
Dual Authentication	Requires wallet signature *and* secret key for security
Production Ready	Part I live on mainnet; Part II extends proven infrastructure
Compliance-First	Viewing keys & screening designed from inception (not retrofitted)

Table 3: SolSeal competitive advantages

7 Conclusion

SolSeal offers ready-to-use privacy today (Part I) and scales to institutional DeFi tomorrow (Part II). It combines proven cryptographic technology with regulatory compliance for secure, private finance on Solana.

Part I demonstrates that encrypted balance infrastructure works in production, providing the foundation for broader adoption.

Part II extends this proven technology to institutional use cases, enabling privacy-preserving yield generation with full regulatory compliance.

For full technical documentation and detailed specifications, visit `solseal.xyz`

This litepaper simplifies technical details for accessibility while protecting proprietary implementations.