SUKICHAN Whitepaper v1.0

Private, Trust-Minimized Cross-Chain Transfers

Date: March 2026
Website: stealthflow.xyz

Executive Summary

SUKICHAN is a next-generation, privacy-preserving cross-chain bridge protocol that enables confidential asset transfers between otherwise incompatible blockchains.

Unlike traditional bridges that publicly expose sender/receiver addresses, transfer amounts, and transaction graphs, SUKICHAN combines zero-knowledge cryptography (hybrid zk-SNARK/zk-STARK approach), shiel ools, and a decentralized relayer network to achieve strong confidentiality and unlinkability across chains.

Core Utility

- Private transfer of native assets and wrapped tokens (ETH, BTC, stablecoins, and more)
- Cross-chain remittances without unnecessary identity exposure
- Privacy-first DeFi interoperability (e.g., private swap/lending access via bridge layer)
- Low-fee, fast finality targets (~30–120 seconds, chain-dependent)

SUKICHAN is designed for a world where chain surveillance is increasing and users require practical, high-performance privacy infrastructure.

---

1. Problem Statement

Public blockchains expose transaction metadata by default. This enables analytics systems to track users across addresses, clusters, and even chains through bridge activity.

Current bridge categories often force one of the following trade-offs:

- Fully transparent bridges -> severe privacy leakage
- Centralized/custodial bridges -> trust assumptions and single points of failure
- Partially private designs -> limited scope or chain-specific constraints

Users increasingly need robust cross-chain privacy for:

- Personal financial sovereignty
- Business remittances in sensitive/restricted jurisdictions
- Compliance-compatible privacy via selective disclosure mechanisms

Existing alternatives are often chain-specific, operationally complex, or too expensive for broad use. SUKICHAN addresses these gaps with a universal privacy-bridge architecture.

---

2. Solution Overview - SUKICHAN Protocol

SUKICHAN combines the following components:

1. Shielded Deposit + Burn/Mint mechanism (inspired by Sapling-like note systems)
2. Zero-Knowledge cross-chain validity proofs (without revealing sender/receiver/amount)
3. Decentralized relayer network (permissionless, incentivized in STF)
4. Per-chain shielded pools (note commitments in Merkle trees)
5. Optional selective disclosure (viewing keys for audit/compliance workflows)

High-Level Flow

1. User deposits assets on source chain into a shielded pool (private note created)
2. User generates zk-proof for valid shielded burn/commitment
3. Relayer submits proof to destination bridge contract
4. Destination verifies proof and mints private/wrapped representation
5. Receiver claims privately on destination chain (without origin linkage)

Result: no direct on-chain linkage between sender and receiver identities, with amount privacy protected by commitments and range proofs.

---

3. Technical Architecture

3.1 Cryptographic Primitives

- Commitments: Pedersen-style commitments for value privacy
- Proof systems: Groth16 (efficiency) + PLONK/Halo2 class systems (universality) as hybrid strategy
- Stealth addresses: dual-key model (view key + spending key)
- Nullifiers: cross-chain double-spend prevention without revealing source note
- Merkle trees: shielded note commitment trees (Sapling-inspired)

3.2 Bridge Components

- Source Chain Vault Contract - lock/deposit assets and emit shielded events
- zk-Prover Layer - generate succinct cross-chain validity proofs
- Relayer Network - permissionless proof submission with STF-based incentives
- Destination Mint Contract - verify proofs and mint destination representation
- Challenge/Safety Window - 1–4 hour fraud/challenge window with zk-backed safety assumptions

3.3 Target Chain Support

Initial target set:

- Ethereum
- BNB Chain
- Polygon
- Arbitrum
- Solana (adapter-based integration)
- Bitcoin (BitVM-inspired path in later phase)

---

4. Tokenomics - STF Token

Total Supply: 1,000,000,000 STF (fixed)

SUKICHAN uses a fixed-supply model with deflationary pressure via protocol fee burn.

4.1 Allocation

- 25% - Liquidity & Farming (initial DEX pools + LP incentives)
- 15% - Team & Advisors (3-year vesting)
- 20% - Ecosystem & Grants (privacy tooling, integrations, audits)
- 20% - Relayer & Prover Rewards (long-term network incentives)
- 15% - Treasury / DAO
- 5% - Private Sale / Seed (locked)

4.2 STF Utility

- Bridge fee payment (holder discounts)
- Staking for relayer/prover priority
- Governance voting for protocol upgrades
- Fee-sharing model for eligible stakers

4.3 Deflationary Mechanism

- 30% of protocol fees are permanently burned

---

5. Security & Risk Mitigation

5.1 Security Strategy

- Multiple independent audits (targets include Trail of Bits, PeckShield, zk-security specialists)
- Public bug bounty program (up to $500K+ target cap)
- Economic security via STF staking + slashing for malicious actors
- No permanent central custodian model
- Progressive decentralization:
  - Phase 1: multisig guardians (bootstrap)
  - Phase 2: full DAO governance

5.2 Known Risks and Mitigations

- Oracle/Relayer collusion -> mandatory on-chain zk-proof verification
- Proof-system soundness risk -> battle-tested circuits, formal verification, and staged rollouts
- Bridge exploit risk (historical category-wide) -> hybrid safety model, timelocks, and defense-in-depth architecture

---

6. Roadmap

- Q1 2026 - Testnet launch (Ethereum <-> Polygon)

- Q2 2026 - Mainnet v1 (EVM chains + private stablecoin support)
- Q3 2026 - Solana + Cosmos IBC integration
- Q4 2026 - Bitcoin/L2 support + mobile SDK
- 2027 - Full DAO governance + private DeFi primitives (lending, swaps)

---

7. Team & Advisors

- Founder / Lead Dev: pseudonymous (privacy-aligned), experienced in zk and bridge systems
- Core Contributors: backgrounds across ZK/privacy and scaling ecosystems
- Advisors: privacy researchers and bridge-security specialists

---

8. Conclusion

Stealth Flow (SUKICHAN) reframes cross-chain interoperability with privacy as a first-class property.

As financial surveillance intensifies, users require tools that preserve sovereignty without sacrificing speed, usability, or composability.

Stealth Flow is not just a bridge - it is an invisible value-transfer layer for the multichain future.

Disclaimer

This whitepaper is provided for informational purposes only. Any token sale, distribution, or network participation mechanics are subject to applicable laws and jurisdictional requirements. Nothing in this document constitutes financial, legal, tax, or investment advice. No guarantees are made regarding protocol performance, token value, or market outcomes.