NovaChan Whitepaper v1.0

Private, Trust-Minimized Cross-Chain Transfers

Date: March 2026

Website: https://novachan.site

1. Executive Summary

NovaChan is a next-generation privacy-preserving cross-chain bridge protocol that enables

seam

Core utility

- Private transfers of native assets or wrapped tokens (ETH, BTC, stablecoins, etc.)
- Cross-chain remittances without KYC exposure
- Privacy-first DeFi interactions (private swaps, lending via bridge)
- Low fees, fast finality (~30–120 seconds depending on chains)

NovaChan addresses the growing demand for privacy in an era of increasing chain surveillance,

regul

2. Problem Statement

Public blockchains expose transaction metadata, enabling chain analysis firms to track users

acros

- Fully transparent → privacy leak
- Centralized/custodial → single point of failure & trust issues
- Privacy-limited (e.g., only optional shielded on one chain)

Users need true cross-chain privacy for:

- Personal financial sovereignty
- Business remittances in restricted jurisdictions
- Compliance-friendly private transfers (selective disclosure possible)

Current solutions like Monero bridges or Secret Network are chain-specific or slow/expensive.

Nova

3. Solution Overview — NovaChan Protocol

NovaChan combines:

1. Shielded deposit & burn/mint mechanism (inspired by Zcash Sapling + RenVM style)
2. Zero-knowledge cross-chain proofs (zk-proof of valid burn/deposit without revealing details)
3. Decentralized relayer network (permissionless, incentivized by protocol fees)
4. Multi-chain shielded pools (per-chain shielded note commitment trees)
5. Optional selective disclosure (viewing keys for audits/regulatory needs)

High-level flow

1. User deposits asset on source chain into shielded pool (private note created)
2. User generates zk-proof attesting valid shielded burn/commitment
3. Relayer submits proof to destination chain bridge contract
4. Destination mints wrapped/private equivalent (stealth address or shielded note)
5. Receiver claims privately on destination (no link to origin)

No on-chain link exists between sender & receiver addresses. Amounts remain hidden via range

proof

4. Technical Architecture

4.1 Cryptographic Primitives

- **Commitment scheme:** Pedersen / Bulletproofs-style for value hiding
- **Zero-knowledge proofs:** Groth16 (fast) + PLONK/Halo2 (universal, no trusted setup) hybrid
- **Stealth addresses:** Dual-key (viewing key + spending key) per transfer
- **Nullifiers:** Prevent double-spend across chains without revealing origin
- **Merkle trees:** Shielded note commitments (Sapling-like)

4.2 Bridge Components

- **Source chain vault contract:** Locks/deposits → emits shielded event
- **zk-prover network:** Generates succinct proofs (can be decentralized via prover

mark

- **Relayer incentives:** Nova token rewards + fee share (0.05–0.3%)
- **Destination mint contract:** Verifies zk-proof → mints private token

- **Challenge period:** 1–4 hour fraud-proof window (optimistic + zk fallback)

Initial support: Ethereum, BNB Chain, Polygon, Arbitrum, Solana (via adapters), Bitcoin (BitV

5. Tokenomics — STF Token

- **Total supply:** 1,000,000,000 STF (fixed supply, deflationary via burns)
- **Allocation:**
  - Liquidity & Farming — 25% (initial DEX pools + LP incentives)
  - Team & Advisors — 15% (3-year vesting)
  - Ecosystem / Grants — 20% (privacy tooling, integrations, audits)
  - Relayer & Prover Rewards — 20% (long-term incentives)
  - Treasury / DAO — 15% (community governance)
  - Private Sale / Seed — 5% (early backers, locked)

Utility
- Pay bridge fees (discounts for holders)
- Stake for relayer/prover priority
- Governance voting (protocol upgrades)
- Fee sharing for stakers

Deflationary lever: 30% of fees burned permanently.

6. Security & Risk Mitigation

- Multiple independent audits (target: Trail of Bits, PeckShield, zksecurity)
- Bug bounty program ($500K+ max tier)
- Economic security: relayers stake STF (slashing for malicious proofs)
- No central custodian — fully decentralized after launch
- Progressive decentralization: Phase 1 multisig guardians → Phase 2 full DAO

Known risks (mitigated)
- Oracle/relayer collusion → zk-proof verification mandatory
- zk-proof soundness → battle-tested systems + formal verification
- Bridge exploits → optimistic + zk hybrid design, timelocks

7. 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)

8. Team & Advisors

- Founder/Lead Dev: anonymous for privacy alignment (zk & bridge veteran)
- Core Contributors: ex-Zcash, Aztec, Polygon zkEVM developers
- Advisors: privacy researchers + bridge security experts

9. Conclusion

NovaChan redefines cross-chain interoperability by putting privacy first. In a world where

finan

Disclaimer: This document is for informational purposes. Token sale/distribution remains

subje