Privex Protocol

A Trust■Minimized Liquidity Bridge for a Multi■Chain World

Version 0.1 — October 10, 2025

Abstract

Privex Protocol is a trust■minimized cross■chain liquidity bridge that enables seamless value transfer and state messaging across heterogeneous blockchains, starting with EVM chains (Ethereum, BNB Chain, Base, Polygon) and Solana.

Privex combines multiple verification paths (native light clients / zk, optimistic security, and external MPC) with an intent/RFQ liquidity layer to provide fast, final, and capital■efficient bridging. The protocol is built around three pillars: Security■first modular verification, Unified liquidity via pooled AMMs and RFQ market makers, and Developer■first composability via a minimal messaging interface and SDKs.

Problem Statement

- Fragmented liquidity splits assets across many bridges and wrapped representations.
- Inconsistent security ranges from trusted multisigs to trust■minimized light client proofs.
- High latency and fees for canonical bridges; reorg risk and stuck funds during congestion.
- Complex UX—multiple confirmations, token mappings, and confusing flows.

Design Goals

- Security first: prefer verifiable proofs; minimize trust in any single committee.
- Speed without compromising safety: fast fills via LPs with on■chain final settlement.
- Neutral & extensible: pluggable verification backends and oracle sources.
- Composability: thin, permissionless messaging API for dApps; clean developer ergonomics.
- Capital efficiency: unified cross■chain pools and RFQ to reduce slippage and idle TVL.
- Transparent economics: predictable fees, revenue sharing, staking■based security with slashing and insurance.

System Overview

Privex comprises four layers: (1) Gateway Contracts per chain, (2) A modular Verification Layer, (3) A Liquidity Layer (unified pools + RFQ), and (4) Coordination & Monitoring (relayers and watchtowers).

Key Roles

- Users — initiate transfers and receive assets on the destination chain.
- LPs/Market Makers — provide instant liquidity via RFQ or unified pools.
- Relayers — submit proofs and target■chain transactions.
- Watchtowers — monitor anomalies; can trigger circuit breakers.
- Governance (PVX DAO) — manages risk, routes, and upgrades.

Bridging Modes

Canonical Lock■and■Mint / Burn■and■Release — Lock native assets on Chain A and mint wrapped pAssets on Chain B; burn to release the originals.

Liquidity Swap (Pool■to■Pool) — Swap Asset X on Chain A to Asset X (or equivalent) on Chain B using unified, inventory■aware pools.

Intent/RFQ Fast Bridge — Users sign intents; makers quote and pay out instantly on the destination chain; canonical settlement reconciles later.

Verification Layer (Modular Security)

Tier A — Verifiable (Preferred): Light clients / zk■proofs verifying headers and Merkle proofs on■chain.

Tier B — Optimistic with Watchdogs: Messages accepted after a challenge window; disputes trigger slashing and safe■mode.

Tier C — MPC Committee (Fallback): Threshold■signed attestations with strict caps and rate limits.

Each asset/route declares a Security Grade (A/B/C) shown to users at initiation with per■tx/daily caps and fees.

Smart Contract Architecture

Gateway (per chain): Deposit/Withdraw, Mint/Burn, ExecuteMessage, RateLimiter, Pausable/Guardian, and controlled upgradability.

Liquidity Pools: Inventory■aware AMM with oracle integration and imbalance/volatility fee bands.

RFQ Engine: Quote registry, PVX■backed slippage vault, and insurance fund.

Messaging Interfaces: sendMessage/receiveMessage and hooks for dApp composability.

Tokenomics (Proposed)

Ticker: PVX — **Supply:** 1,000,000,000 fixed.

Initial Distribution: Community & Liquidity 35%; Treasury (POL & Insurance) 25%; Core Contributors 15% (4■yr vest, 1■yr cliff); Strategic Partners/MMs 10% (3■yr vest); Public Sale 10%; Advisors/Audits/Grants 5%.

Utility: Staking for security with slashing; fee discounts; governance.

Fee Model

Base protocol fee: 4–20 bps depending on route/security tier.

Dynamic surcharge based on pool imbalance and volatility.

RFQ spread set by LPs; protocol takes 10–30% rev■share.

Revenue allocation: 50% Treasury, 30% Staker Rewards, 20% Ops & Grants (governance■tunable).

Security Model

Defense■in■depth with verifiable proofs preferred; optimistic fallback; MPC as last resort with tight caps.

Risk controls: daily/per■tx caps, circuit breakers on oracle deviation and mempool stress.

Monitoring: on■chain detectors, independent watchtowers, audits, and bug bounties.

Threat Model (non■exhaustive)

- Consensus reorgs/finality issues — chain■specific thresholds; probabilistic confirmation for RFQ payouts.
- Oracle manipulation — medianized feeds + TWAP + circuit breakers.
- Relayer collusion — proof diversity, slashing, disputes.
- Liquidity drains — imbalance caps, dynamic fees, treasury rebalancing.
- Wrapped asset risk — prioritize native representation; clearly label pAssets.

User Experience

Single■screen flow with explicit Security Grade, ETA, Fee, and Min Received; deterministic transfer IDs and a public explorer; future gas abstraction.

Developer Experience

TypeScript & Rust SDKs; minimal contract interfaces; multi■chain testnets; local sandbox scripts; EIP■712 intent templates.

Economics & Sustainability

Inventory■aware fees encourage rebalancing; protocol■owned liquidity and insurance backstop tail risks; governance can quickly tune caps and fees.

Governance

PVX DAO with delegated voting manages routes, parameters, treasury spend, and verifier selection with timelocks and staged rollouts.

Compliance & Legal (Guidance■Level)

Open■source, permissionless core; optional KYT hooks at front■end; clear risk disclosures and regional access policies at the interface layer.

Roadmap (Indicative)

Q4 2025 — Testnet v1 (ETH/BNB/Base/Polygon/Solana), 1 audit, explorers + SDK alpha.

Q1 2026 — Gradual mainnet with Grade A/B routes and strict caps, RFQ expansion, insurance launch, 2nd audit.

Q2 2026 — zk light■client integrations, gas abstraction, NFT bridging, intent router.

Q3 2026 — Mobile SDK, more chains (Arbitrum, Optimism, Avalanche, TON), buyback & burn vote.

Risk Disclosures

Bridging carries risks including chain reorgs, contract bugs, price volatility, oracle failures, and wrapped■asset depegs. Privex mitigates but cannot eliminate these risks. Users should evaluate Security Grade and caps per route and use at their own risk.

Glossary

Light Client: On■chain verifier of another chain's headers.

zk■Proof: Zero■knowledge proof attesting to state validity.

RFQ: Request■for■Quote; market maker offers a binding price.

POL: Protocol■Owned Liquidity used for stability and insurance.

pAsset: Privex■minted wrapped asset on a non■native chain.

Example Flows

Fast ETH → SOL (RFQ): User signs intent; maker pays out instantly on Solana; canonical message settles later and reimburses the maker.

Canonical USDC → USDC (Lock■Mint): Deposit on Chain A; proof verified on Chain B; mint pUSDC; burn to release native USDC.

Appendix A — Parameters (Initial Suggestions)

Finality thresholds: ETH 15 blocks; BNB 20; Base 10; Polygon 256; Solana 32 confirmations.

Dispute window (optimistic): 10 minutes (testnet), 30 minutes (mainnet Grade B).

Caps: Per■tx $100k, daily $5m per route at launch (subject to governance).

Fees: Base 8 bps Grade A, 12 bps Grade B, 18 bps Grade C; RFQ rev■share 20%.

Appendix B — Contract Registry (Placeholders)

Gateway: PrivexGateway; Verifier Modules: VerifierLC, VerifierZK, VerifierOpt, VerifierMPC; Liquidity Pool: PrivexPool; RFQ: PrivexRFQ; RateLimiter: PrivexGuard; Explorer: explorer.privex.xyz (placeholder).

Appendix C — Branding

Tagline: “Private. Fast. Final. Across Chains.” Abbreviation: Privex (PVX). Colors: Deep black with neon cyan/magenta accents. Tone: Premium, futuristic, developer■first.