NightSwap Decentralized Exchange

Privacy-Preserving DEX Built for Midnight

NightSwap Labs

July 23, 2025

Abstract

NightSwap is an upcoming decentralized exchange (DEX) that will be deployed natively on Midnight, Cardano's privacy-focused sidechain. NightSwap allows pairing the confidentiality guarantees of zero-knowledge proofs with the open-access ethos of decentralized finance, delivering non-custodial trading where users retain full control over both their assets and the visibility of their data.

Disclaimer: This document is intended for general information purposes only. It is not intended as investment advice and should not be used to make any investment decision. The information and concepts provided in this whitepaper are subjected to change without prior notification.

1 Introduction

Midnight[1] is designed to serve applications that demand both programmability and data protection. Three features are especially relevant for a DEX:

1. **Zero-knowledge validity proofs**: every contract call is accompanied by a proof that enforces balance conservation and business logic without revealing wallet addresses or trade amounts.
2. **Selective disclosure**: developers can encode fine-grained rules that allow transaction details to remain shielded yet be decryptable for chosen counterparties or regulators, supporting compliance without blanket transparency.
3. ***Compact* smart-contract language**: a TypeScript-inspired, formally specified language that shortens audit cycles and lowers the barrier to entry for web-native teams.

Building on these primitives, NightSwap will introduce:

- *Confidential swap pools* that let traders exchange assets without exposing their order flow.
- *Opt-in transparency paths* so users can share verifiable trade data when they choose.

By combining Midnight's privacy infrastructure with familiar DeFi mechanics, NightSwap aims to demonstrate that meaningful confidentiality and open participation are mutually compatible goals in the next generation of blockchain markets.

2 Solution Overview and Privacy Design

NightSwap is designed to enable private on-chain trading while preserving the core principles of a decentralized exchange. Built on Midnight, it inherits a privacy-first execution model powered by zero-knowledge validity proofs and selective disclosure mechanisms.

At its core, NightSwap operates as a shielded automated market maker (AMM), where swap logic is enforced via ZK proofs rather than exposed public transaction data. This enables:

- Trades that do not reveal originator addresses or transferred amounts.
- Liquidity that cannot be trivially mapped, deterring extraction strategies like sandwich attacks.
- Optional transparency paths, empowering users to disclose transaction details to counterparties, auditors, or regulators when required.

Smart contracts are written in *Compact*, Midnight's high-assurance, TypeScript-like language, designed for privacy-aware application logic and formal verification.

[1] `https://midnight.network/whitepaper`

3 Key Features

NightSwap is designed to deliver practical privacy in decentralized trading without sacrificing usability, security, or developer access. Its architecture introduces several key capabilities:

- **Confidential Swaps:** Enables fully private asset exchanges without revealing liquidity paths, counterparty identities, and price impact, yet still recording every swap on-chain for verifiability. All transaction details remain authenticated by the protocol without ever exposing sensitive trade data to outside observers.

  Standard blockchains reveal every transaction detail publicly; confidential swaps conceal both participants and volumes, preventing external tracking.

- **Shielded LP Tokens:** Liquidity providers receive encrypted receipts representing their positions, allowing private ownership and redemption. Liquidity providers receive encrypted proof-of-position tokens that represent their share in a pool, allowing them to hold, transfer, or redeem stakes without revealing exact amounts.

  Traditional liquidity pools expose pro-rata shares openly, inviting adversaries to track "whale" reallocations. Shielded tokens keep this information private.

- **Opt-in Disclosure:** Gives users fine-grained control over which transaction metadata to share, and with whom. This supports auditors, counterparties, or third-party services only when explicitly authorized, balancing privacy with compliance by enabling verifiable audits without exposing unnecessary data.

  Unlike public blockchains where all metadata is broadcast universally, opt-in disclosure lets you choose exactly what to reveal and to whom.

- **Gas Abstraction:** Integration with DUST sponsorship allows protocols to subsidize user interactions, enabling Web2-style onboarding. Newcomers can interact with the chain without needing to acquire or manage native gas tokens, thereby reducing friction and improving accessibility.

  Usually, blockchain users pay a fee ("gas") for each action. Gas abstraction lets apps handle fees for you.

- **Developer Access:** Smart contracts are designed to be fully modular and extensible, built around standard Compact interfaces that encourage secure, privacy-aware integrations. This framework enables developers to easily adopt and extend privacy features while adhering to best practices in auditability and security.

Together, these features make NightSwap a high-assurance platform for private, programmable trading within the Midnight ecosystem.

4 Tokenomics

The NightSwap ecosystem will be supported by a native utility token known as NSWAP. This token will serve as a foundational component of the NightSwap infrastructure and community. NSWAP will have a permanently fixed total supply of 25,000,000 tokens, ensuring long-term value alignment within the ecosystem. It will represent a central element in how users interact with the platform and participate in its ongoing development and governance.

Token Utility

NSWAP will play an important role in the NightSwap ecosystem, acting as a multifunctional asset with key utilities that empower users and contribute to a more dynamic and engaged community. The token's utility includes:

- **Ecosystem Access:** NSWAP will be required to unlock access to premium or advanced features on the NightSwap platform. It may also be used to grant privileged early access to upcoming tools, products, or experimental services that are in development.
- **Community Token:** Holders of NSWAP will be able to take part in important community-driven processes. This includes participation in governance-related temperature checks, non-binding community polls, and discussions on proposed upgrades to the protocol or adjustments to protocol parameters.
- **Staking Rewards:** Stake your NSWAP tokens to earn passive rewards and support the long-term stability of the NightSwap ecosystem.

Token Allocation

The total supply of NSWAP tokens will be allocated across several core categories to ensure long-term sustainability, robust growth, and active engagement across the ecosystem. The breakdown is as follows:

- **60% – Token Sale (Public + Private):** A majority of the tokens will be distributed through both public and private token sales. Further details regarding the structure and timeline of these sales will be disclosed in separate communications.
- **10% – Team Tokens:** A dedicated portion of the supply is reserved for the core development team behind NightSwap. This may also be extended to future team members and key hires who contribute meaningfully to the project.
- **8% – Ecosystem Treasury:** These tokens will be held in reserve for the ongoing development and expansion of the NightSwap protocol. This allocation may also support the future creation of a community-led DAO to help guide the ecosystem's direction.
- **22% – Ecosystem and Liquidity Incentives:** This allocation will support initiatives such as liquidity mining programs (e.g., farms to incentivize LP provision), user incentives, rewards for partners, marketing campaigns, and other promotional or growth-focused activities.

5 Roadmap

NightSwap's development is structured around phased milestones, each focused on delivering core functionality, progressive decentralization, and ecosystem growth:

- **Milestone 1 - Basic Testnet Launch:** Deploy basic zk-swap functionality paired with a minimal front-end interface for testing and feedback.
- **Milestone 2 - V1 Mainnet Release:** Launch NightSwap v1 on Midnight and onboard the first users to NightSwap.
- **Milestone 3.a - AMM Testnet Phase:** Roll-out core AMM contracts with shielded swap functionality and LP token issuance to the Testnet.
- **Milestone 3.b – V2 Mainnet Release:** Launch NightSwap v2 on Midnight, featuring the first shielded token trading pairs.
- **Milestone 4 – Ecosystem Extension Phase:** Introduction of liquidity pools, yield programs, and advanced order types.
- **Milestone 4 - Governance & DAO:** Introduce a community-driven governance framework and evaluate activation of the `NSWAP` token for protocol upgrades, treasury control, and staking-based participation.

6 The Future of Private DeFi Starts Today

NightSwap is more than a decentralized exchange - it's a commitment to restoring privacy in on-chain finance without compromising usability, performance, or developer freedom. By leveraging Midnight's zero-knowledge architecture, shielded execution, and opt-in transparency, NightSwap sets a new standard for trustless, programmable privacy.

As the Midnight ecosystem evolves, NightSwap will serve as a foundational layer for private liquidity, composable financial tools, and next-generation DeFi applications.

NightSwap reinvents what a DEX can be - where privacy is default, not a feature, and the future of private DeFi is closer than ever.