LP-308: QuantumSwap

A Post-Quantum AMM Protocol with Mixed Fungible/Non-Fungible Liquidity Pools

Zach Kelling

Lux Industries

Original: March 2024 | Revised: March 2026

Abstract

QuantumSwap is an automated market maker protocol designed for the Lux Network with three distinguishing properties: post-quantum encryption of order flow via TFHE, mixed fungible/non-fungible token liquidity pools with configurable bonding curves, and a multi-chain teleport protocol using zero-knowledge bridges with Lamport and lattice-based signatures.

This paper formalizes the bonding curve algorithms (linear, exponential, XYK), the interest rate mechanism for RWA-backed price-stable currencies, and the capital efficiency model. We provide the concrete interest rate schedule and analyze its stability properties.

Section 8 maps the QuantumSwap design to the current Lux exchange architecture: `luxfi/dex` (CLOB engine), `luxfi/standard/contracts/amm/` (AMM V1–V4 contracts), and the USDL stablecoin.

Contents

1 Introduction

1.1 Motivation

Automated market makers revolutionized decentralized exchange by replacing order books with deterministic pricing functions. However, existing AMMs suffer from three limitations:

1. **No privacy**: All orders are visible on-chain before execution, enabling front-running and sandwich attacks.
2. **Fungible tokens only**: NFTs and real-world asset tokens cannot participate in standard AMM pools.
3. **Single-chain**: Cross-chain liquidity requires third-party bridges with variable security properties.

QuantumSwap addresses all three: homomorphic encryption prevents order visibility, mixed FT/NFT pools extend liquidity to non-fungible assets, and a native teleport protocol provides cross-chain token movement with post-quantum security.

1.2 Historical Context

Year	Protocol	Innovation
2013	BitShares	Decentralized order books
2016	0x Protocol	Gas-efficient meta-transactions
2018	Uniswap V1	First AMM, LP tokens, ETH/ERC-20 pairs
2020	Uniswap V2	ERC-20/ERC-20 pairs, flash swaps, oracle feeds
2021	Uniswap V3	Concentrated liquidity, range orders [1]
2024	QuantumSwap	Mixed FT/NFT pools, FHE-encrypted order flow

2 Bonding Curve Algorithms

QuantumSwap pools are parameterized by a bonding curve that determines price dynamics. Each `LUXQSAPair` contract is associated with exactly one curve. The curves are pure functions: they do not modify pool state. State updates occur in the `LUXRWAPair` contract after the curve is consulted.

2.1 Notation

Let *spot* denote the current spot price (instantaneous price to sell one item to the pool), δ the curve parameter, and x the trade size. The spot price to *buy* one item from the pool is always $spot + \delta$ (additive) or $spot \cdot (1 + \delta)$ (multiplicative), depending on the curve.

2.2 Linear Bonding Curve

The linear curve adjusts price by a constant additive amount δ per item traded:

$$spot_{\text{after sell}} = spot - \delta \tag{1}$$

$$spot_{\text{after buy}} = spot + \delta \tag{2}$$

For a multi-item sell of x items, the total payout is:

$$\text{Payout}(x) = \sum_{i=0}^{x-1} (spot - i\delta) = x \cdot spot - \delta \cdot \frac{x(x-1)}{2} \tag{3}$$

Remark 2.1. *The LP must set δ with the same decimal precision as the pair's underlying token. For an ETH-denominated pair with spot $= 1\,ETH$ and $\delta = 0.1\,ETH$, selling 5 NFTs yields $5 \cdot 1 - 0.1 \cdot 10 = 4\,ETH$, distributed as $\{1, 0.9, 0.8, 0.7, 0.6\}$.*

2.3 Exponential Bonding Curve

The exponential curve adjusts price by a multiplicative factor:

$$spot_{\text{after buy}} = spot \cdot (1 + \delta) \tag{4}$$

$$spot_{\text{after sell}} = \frac{spot}{1 + \delta} \tag{5}$$

After x consecutive buys from an initial spot price p_0:

$$spot(x) = p_0 \cdot (1 + \delta)^x \tag{6}$$

The total cost of buying x items is:

$$\text{Cost}(x) = p_0 \cdot (1 + \delta) \cdot \frac{(1 + \delta)^x - 1}{\delta} \tag{7}$$

Remark 2.2. *With $p_0 = 2\,ETH$ and $\delta = 0.5$ (50%), the price sequence for 3 buys is $\{3, 4.5, 6.75\}$ ETH. Selling into the pool divides by 1.5 at each step.*

2.4 XYK Bonding Curve

The XYK curve maintains a constant-product invariant over virtual reserves, adapted for NFT pools. At pool creation:

$$R_{\text{nft}} = (\text{number of items to buy or sell}) + 1 \tag{8}$$

$$R_{\text{token}} = R_{\text{nft}} \cdot spot \tag{9}$$

The price to buy x items from the pool (receiving NFTs, sending tokens) is:

$$\text{Cost}(x) = \frac{x \cdot R_{\text{token}}}{R_{\text{nft}} - x} \tag{10}$$

The price to sell x items to the pool is:

$$\text{Payout}(x) = \frac{x \cdot R_{\text{token}}}{R_{\text{nft}} + x} \tag{11}$$

After each trade, the virtual reserves update:

- Pool sells NFTs: $R_{\text{nft}} \leftarrow R_{\text{nft}} - x, \quad R_{\text{token}} \leftarrow R_{\text{token}} + \text{Cost}(x)$
- Pool buys NFTs: $R_{\text{nft}} \leftarrow R_{\text{nft}} + x, \quad R_{\text{token}} \leftarrow R_{\text{token}} - \text{Payout}(x)$

A concentration parameter allows LPs to tighten or loosen the curve around the current price, analogous to Uniswap V3's concentrated liquidity [1] but applied to discrete (NFT) assets.

3 Mixed FT/NFT Liquidity Pools

3.1 Pool Types

QuantumSwap supports three pool configurations:

Type	Assets	Use Case
FT/FT	Two ERC-20 tokens	Standard AMM
FT/NFT	ERC-20 + ERC-721	RWA token trading
NFT/NFT	Two ERC-721 collections	Cross-collection swaps

3.2 FT/NFT Mechanics

In an FT/NFT pool, the NFT side is treated as a discrete quantity while the FT side is continuous. The bonding curve operates on the NFT count, producing FT prices. This enables trade sequences like:

$$\text{FT} \xrightarrow{\text{Pool A}} \text{NFT}_1 \xrightarrow{\text{Pool B}} \text{NFT}_2 \xrightarrow{\text{Pool C}} \text{FT}'$$

Each hop uses the bonding curve of the respective pool. The router contract finds the optimal path across available pools.

3.3 Capital Efficiency

Concentrated liquidity in QuantumSwap achieves up to 4000× capital efficiency over Uniswap V2's uniform distribution, consistent with the analysis in Adams et al. [1]. The improvement comes from restricting liquidity to a narrow price range rather than distributing it uniformly from zero to infinity.

Remark 3.1. *The* 4000× *figure is a theoretical maximum for a single tick range. Practical improvement depends on the LP's price range selection relative to realized volatility. Empirical data from Uniswap V3 shows typical improvements of* 4× *to* 8× *for actively managed positions.*

4 RWA-Backed Price-Stable Currencies

4.1 Design

A Real World Asset (RWA) token represents a claim on a physical asset (gold, silver, uranium, real estate). When users stake RWA tokens into a governance pool, they mint a price-stable currency pegged to the underlying asset's market value. The bonding curve automatically adjusts an interest rate to maintain the peg.

4.2 Interest Rate Algorithm

Let:

- b_{LUX} = value of one unit of the RWA token on QuantumSwap (in USD)
- b_{market} = value of the same underlying asset on major external exchanges (in USD)
- $\text{premium} = (b_{\text{LUX}} - b_{\text{market}})/b_{\text{market}}$

The annualized interest rate r is determined by:

$$r = \begin{cases} 0\% & \text{if premium} = 0\% \\ 2\% & \text{if } 0\% < \text{premium} \leq 2\% \\ \text{premium} & \text{if } 2\% < \text{premium} \leq 15\% \\ 15\% & \text{if premium} > 15\% \end{cases} \tag{12}$$

4.3 Stability Analysis

The rate schedule in (12) has three regimes:

1. **Dead zone** (premium = 0): No incentive to issue or redeem. The peg is exact.
2. **Threshold** ($0 <$ premium $\leq 2\%$): A fixed 2% rate provides a clear signal to issuers. The step function avoids oscillation around zero.
3. **Linear tracking** ($2\% <$ premium $\leq 15\%$): Rate tracks premium 1:1, providing proportional incentive.
4. **Cap** (premium $> 15\%$): Protects holders from unbounded interest obligations.

Remark 4.1. *The 2% threshold was chosen empirically: users respond more reliably to a discrete step than to continuous micro-incentives. The 15% cap prevents death spirals where rising rates cause holder panic and further depegging.*

4.4 Comparison to Prior Art

BitShares' pegged currencies (bitUSD, bitCNY) were collateralized solely by BTS, a volatile crypto-asset. This created reflexive collapse risk: BTS price drops $\rightarrow$ collateral falls $\rightarrow$ peg breaks $\rightarrow$ BTS price drops further. QuantumSwap's design requires 1:1 physical asset collateral (gold, uranium, etc.), breaking the reflexivity. The interest rate mechanism then handles *demand*-side deviations from peg, while the physical collateral handles *supply*-side solvency.

5 Privacy: Homomorphic Encryption of Order Flow

5.1 Threat Model

In a standard AMM, pending transactions are visible in the mempool. An adversary can:

- **Front-run**: Place a transaction before the victim's to profit from the price impact.
- **Sandwich**: Place transactions before and after the victim's, extracting value from the spread.

5.2 TFHE-Protected Pools

QuantumSwap encrypts order parameters (amount, direction, slippage tolerance) under TFHE before submission. The AMM contract evaluates the bonding curve on encrypted inputs:

- Comparison operations (is the price within slippage tolerance?) execute as TFHE boolean circuits.
- Reserve updates use TFHE integer arithmetic.
- The result (trade executed or rejected) is encrypted; only the trader can decrypt their outcome.

The performance cost is significant: a single TFHE-protected swap requires approximately 100 bootstrapping operations ($\sim$10 seconds at PN10QP27 parameters). This is acceptable for high-value RWA trades but not for high-frequency token swaps.

6 Multi-Chain Teleport Protocol

6.1 Architecture

The teleport protocol enables cross-chain token movement without relying on third-party bridges. It consists of:

1. **Source chain lock**: Tokens are locked in a vault contract on the source chain.
2. **ZK proof generation**: A zero-knowledge proof of the lock event is generated, attesting to the token identity, amount, and destination without revealing the sender.

3. **Relay**: A trustless relayer transmits the proof across chains. The relayer cannot modify the proof or redirect the tokens.
4. **Destination chain mint**: The proof is verified on-chain using a ZK verifier (Groth16 or PLONK). On verification, equivalent tokens are minted on the destination.

6.2 Post-Quantum Security

The ZK bridge uses Lamport signatures for proof authentication (quantum resistance from hash-only construction) and lattice-based encryption for the relay channel. The combination provides post-quantum security for the bridge even if the underlying chains use ECDSA.

7 Gas-Free Meta-Transactions

QuantumSwap implements ERC-2771 [2] compliant meta-transactions. Users sign transactions off-chain; a trusted forwarder contract verifies the signature and forwards the call to the AMM, paying gas on the user's behalf. This eliminates the gas barrier for new users.

Formally, a meta-transaction $M = (to, value, data, sig)$ is a standard transaction with the sender address derived from sig rather than from `msg.sender`. The forwarder verifies sig against a nonce to prevent replay.

8 Current Status

8.1 Architecture Evolution

The Lux exchange architecture has evolved from AMM-first (QuantumSwap, 2024) to a hybrid CLOB + AMM design:

Component	2024 (QuantumSwap)	2026 (Production)
Matching engine	AMM bonding curves	CLOB (`luxfi/dex`)
AMM contracts	Proposed	Deployed (V1–V4)
Order privacy	TFHE on all orders	TFHE on Z-Chain only
Stablecoin	Gold/uranium-backed	USD-backed (USDL)
Cross-chain	ZK teleport	Warp messaging + MPC bridge

8.2 What Shipped

- **AMM contracts** in `luxfi/standard/contracts/amm/` implement V1 (constant-product), V2 (multi-asset), V3 (concentrated liquidity), and V4 (hook-extensible) designs. The bonding curve algorithms from Sections 2–3 are implemented in the V1/V2 pair contracts.
- **CLOB engine** (`luxfi/dex`) provides 104–250M byte-exact `uint256` fills/s of GPU-accelerated matching (104–126M/s on an NVIDIA GB10, ∼250M/s on an Apple M4 Max), used as the primary exchange engine. AMM pools serve as passive liquidity that the CLOB can route through.
- **USDL**: The stablecoin shipped as a straightforward USD-backed ERC-20, not the RWA-collateralized multi-asset design. Physical commodity backing (gold, uranium) was deferred due to regulatory complexity around commodity-backed tokens.
- **Mixed FT/NFT pools**: The `LUXRWAPair` contract is deployed for RWA token trading, including SecurityToken (ERC-20) swaps.

8.3 What Changed

- **CLOB over AMM**: For securities trading, a CLOB provides price discovery, order types (limit, stop, market), and regulatory compliance (best execution obligations) that AMMs cannot. AMM pools remain available for DeFi use cases.
- **Warp + MPC over ZK teleport**: The production bridge uses Warp messaging with BLS aggregation and 2-of-3 MPC threshold signing, which is simpler to audit and maintain than a full ZK bridge circuit.
- **USD-backed over commodity-backed**: USDL is 1:1 USD-backed via ACH deposits. The interest rate mechanism from Section 4.2 was not needed for a fiat-backed stablecoin.

9 Conclusion

QuantumSwap introduced three ideas that influenced the production Lux exchange: mixed FT/NFT liquidity pools with formal bonding curves, FHE-encrypted order flow for front-running prevention, and an interest rate mechanism for maintaining asset-backed pegs. The CLOB engine superseded AMM as the primary matching mechanism for securities, while AMM contracts remain deployed for DeFi liquidity provision. The interest rate algorithm remains available for future commodity-backed stablecoin deployments.

References

[1] H. Adams, N. Zinsmeister, M. Salem, R. Keefer, and D. Robinson, "Uniswap v3 Core," Uniswap Labs, 2021.

[2] R. Sandford, L. Siri, D. Tirosh, Y. Weiss, and A. Forshtat, "ERC-2771: Secure Protocol for Native Meta Transactions," Ethereum Improvement Proposals, 2020.

[3] 0xmons, "sudoswap: An on-chain NFT AMM," https://docs.sudoswap.xyz/, 2022.

[4] C. Gentry, "A fully homomorphic encryption scheme," Ph.D. dissertation, Stanford University, 2009.

[5] L. Lamport, "Constructing digital signatures from a one-way function," Technical Report SRI-CSL-98, 1979.

[6] Z. Kelling, "LP-020: Quasar—Hybrid BLS + Lattice Consensus for Post-Quantum Finality," Lux Industries, 2026.