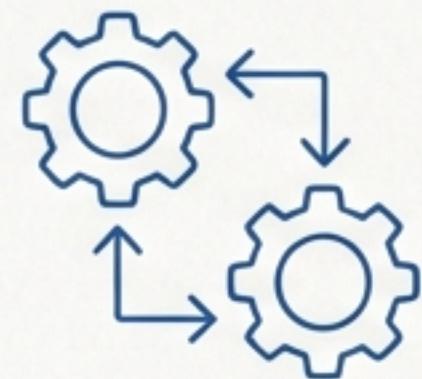


SUI AMM: A Production-Ready Decentralized Exchange



A sophisticated automated market maker protocol on the Sui blockchain featuring NFT-based LP positions, StableSwap pools, and advanced DeFi capabilities.

An Evolved AMM Architecture for Modern DeFi



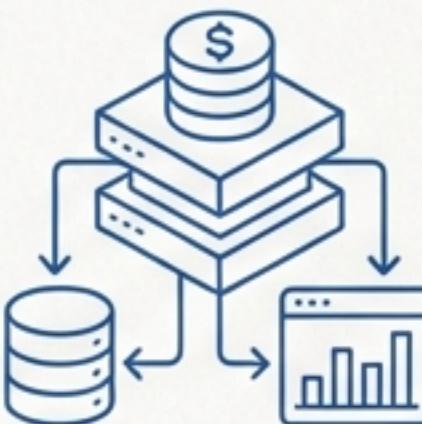
Dual Pool System

- **Constant Product AMM:** For standard volatile pairs ($x^*y=k$).
- **StableSwap Pools:** Curve-style, low-slippage pools for stable assets.
- **Multi-Tier Fees:** Flexible 0.05%, 0.3%, and 1% fee tiers to match pair volatility.



Next-Generation Liquidity

- **NFT LP Positions:** Liquidity positions are represented as tradable, transferable NFTs.
- **Dynamic On-Chain Metadata:** Real-time position value, accrued fees, and impermanent loss are displayed directly on the NFT.
- **On-Chain SVG Generation:** Visually rich, self-contained NFTs generated without external dependencies.



Advanced DeFi Capabilities

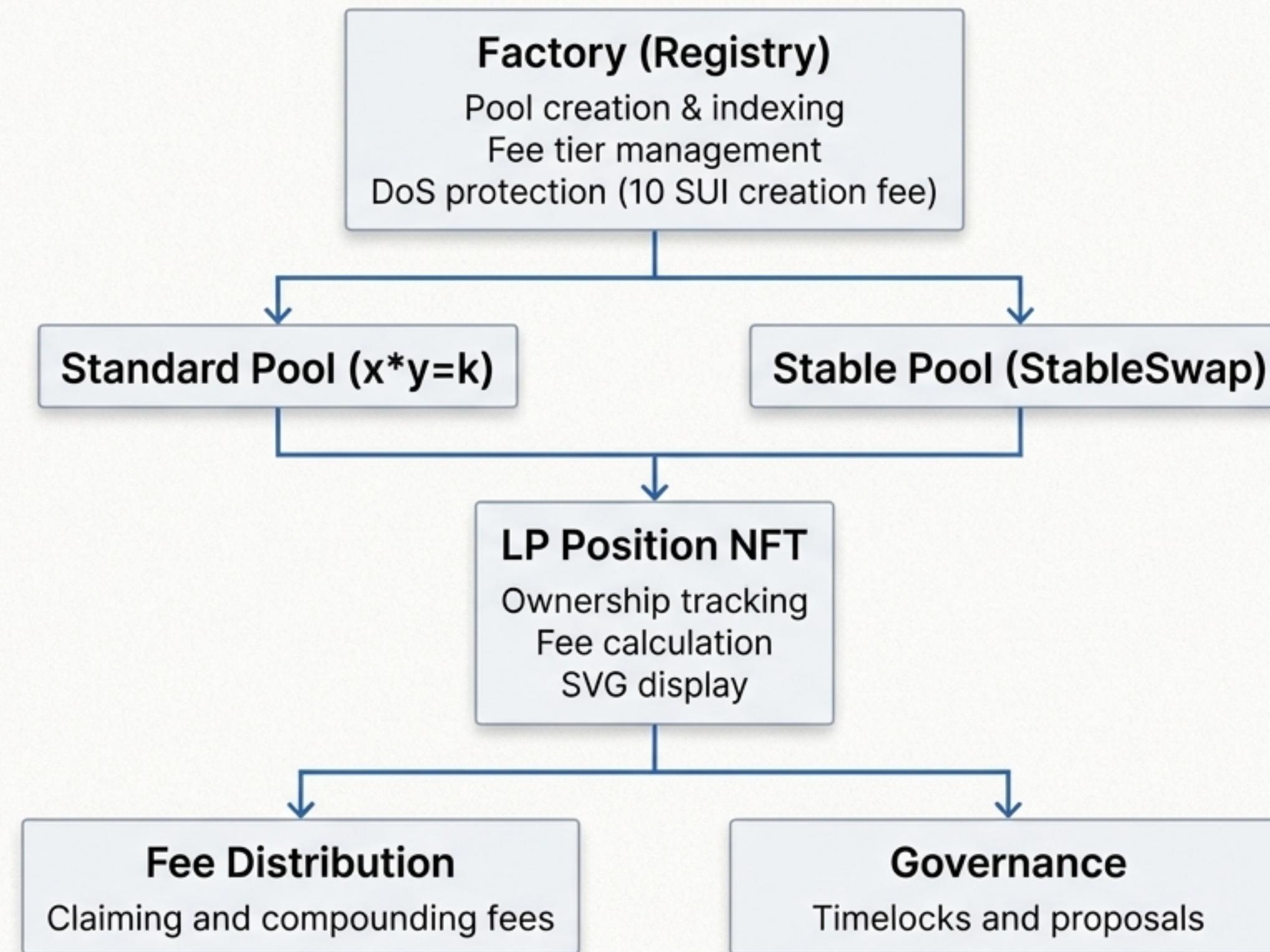
- **Fee Auto-Compounding:** One-click reinvestment of earned fees into the LP position.
- **Decentralized Limit Orders:** An on-chain order book with expiry, executable by anyone.
- **On-Chain Analytics:** Built-in swap history and statistics tracking.



Institutional-Grade Security

- **Governance Timelock:** A 24-hour delay on all critical parameter changes.
- **Comprehensive Protection:** Built-in guards against reentrancy, pool manipulation, and DoS attacks.
- **Meticulous Testing:** Over 80% code coverage across a suite of 24 test modules.

The Protocol Blueprint: A Modular and Robust Design



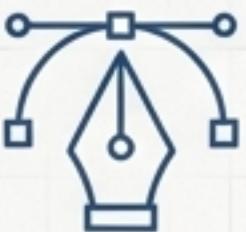
A Paradigm Shift: Liquidity as Dynamic, Composable NFTs

Instead of fungible LP tokens, each liquidity position is a unique, self-contained NFT. This transforms liquidity into a tradable, visually rich asset.



Dynamic Metadata

The NFT's on-chain data is a live dashboard, not a static image. Caches current position value, pending fees, and impermanent loss percentage.



On-Chain SVG Rendering

Generates a complete, data-rich visual representation of the LP position directly on-chain. No IPFS or external hosting needed. Includes gradient backgrounds, real-time value display, and color-coded impermanent loss indicators (green/yellow/red).



High-Precision Tracking

Fee and IL calculations use 1e12 precision for accuracy.



Enhanced Composability

As standard NFTs, positions can be easily transferred, used as collateral in other protocols, or traded on marketplaces.

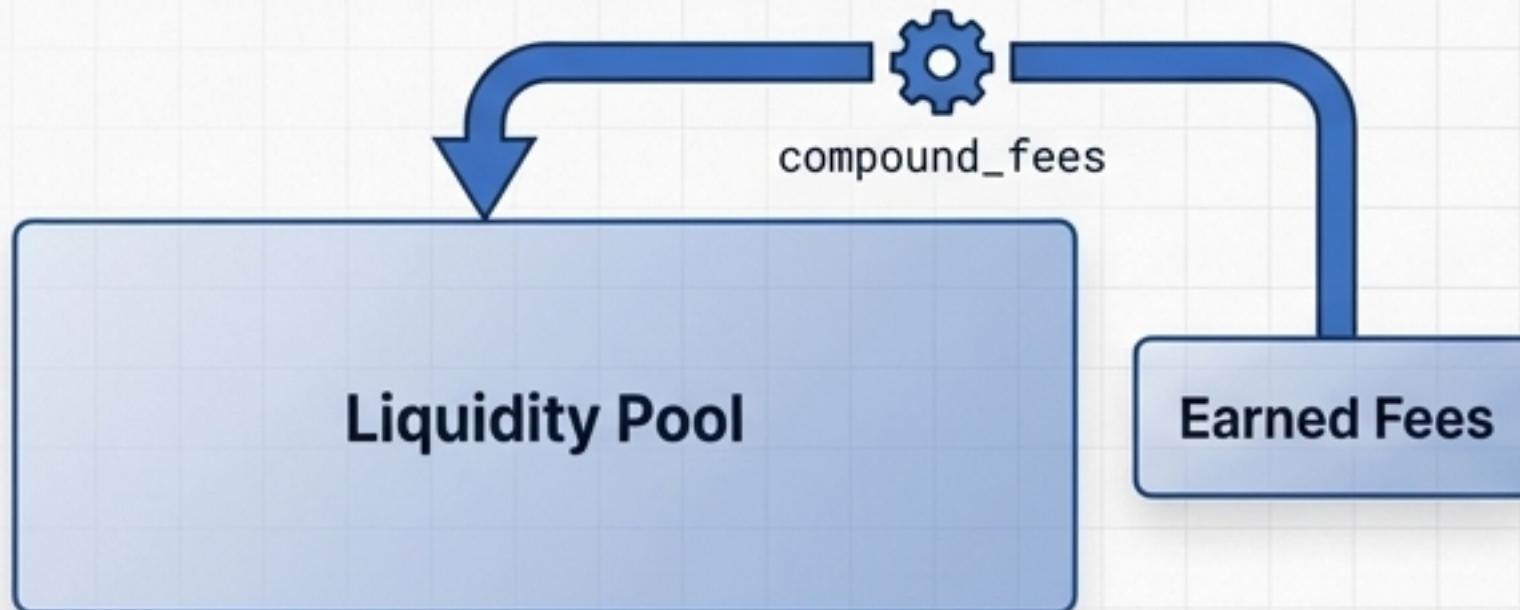


Advanced Tooling for Sophisticated Users

Fee Auto-Compounding

A one-click function ('compound_fees') to reinvest earned fees directly back into the LP position, maximizing capital efficiency.

- Gas-efficient implementation.
- Works for both standard and stable pools.
- Includes a dust prevention check ('is_worth_compounding') to avoid wasteful transactions (1,000 unit minimum).
- Guarded against double-claiming exploits.



Decentralized Limit Orders

A fully on-chain limit order book ('limit_orders.move') that allows users to place orders to be filled at a target price.

- Permissionless Execution:** Anyone can execute a filled order, creating an open ecosystem for keepers.
- Time-Bound**
Orders include expiry timestamps for certainty.
- Indexed & Queryable**
Efficiently look up active orders per-pool and per-user ('get_user_orders').

Place Limit Order

Amount to Sell	Amount to Receive
1,000 USDC	995 USDT
Target Price	Expiry
0.995 USDC/USDT	Oct 26, 2024, 12:00 PM

Place Order

Engineered for Security: A Multi-Layered Defense Strategy

Security is not an afterthought, but a core design principle woven into every module.



Governance Timelock

Critical changes (e.g., fee adjustments, pausing) require a **24-hour** delay before execution.



Minimum Liquidity Burn

The first depositor burns 1,000 shares, permanently locking liquidity to prevent price manipulation attacks on new pools.



Arithmetic Safety

All calculations use checked arithmetic with **u128** precision to prevent overflows on large values.



Reentrancy Guards

Fee debt accounting mechanism prevents any double-claiming of rewards.



Economic DoS Protection

Pool creation requires a **10 SUI fee** and is subject to per-token (500) and global (50,000) limits.



Slippage & Deadline Protection

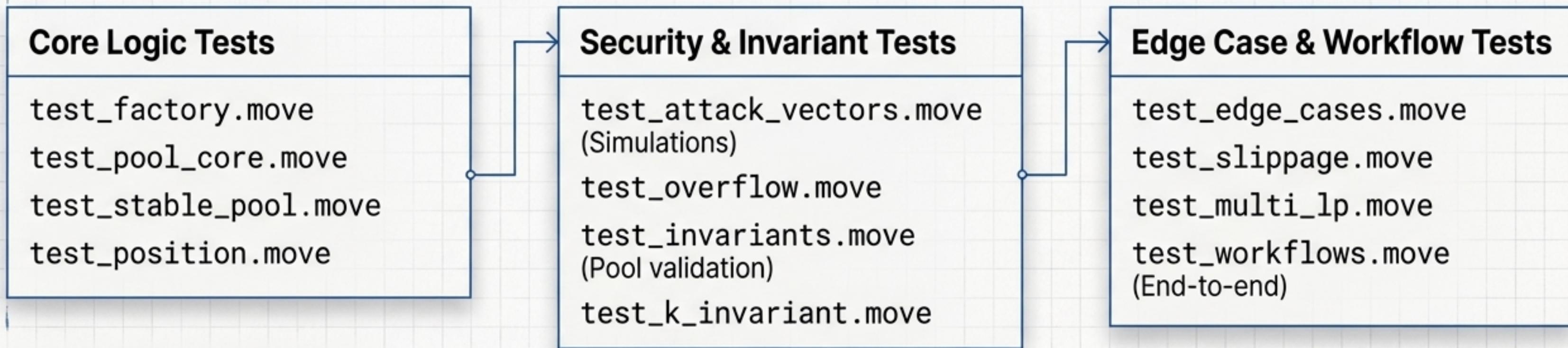
All swaps enforce user-defined minimum outputs and transaction deadlines to mitigate front-running.

Audited Vulnerabilities Fixed

The protocol incorporates fixes for common DeFi exploits identified through internal review and audit simulations, including LP minting precision, fee debt tracking, and IL calculation accuracy (upgraded to 1e12).

Verification and Validation: A Culture of Rigorous Testing

>80% Code Coverage Across All Core Modules



Key Areas of Coverage

- AMM mathematics and fee calculation accuracy.
- Boundary conditions with large and small amounts.
- Concurrent operations from multiple LPs.
- Gas benchmarking and performance profiling.

Includes 24 comprehensive test modules designed to validate correctness, security, and performance under diverse scenarios.

Under the Hood: Mathematical Precision and Gas Efficiency

Core Mathematics

Constant Product

$$\text{amount_out} = \frac{\text{amount_in} * \text{fee_multiplier} * \text{reserve_out}}{\text{reserve_in} + \text{amount_in} * \text{fee_multiplier}}$$

StableSwap Invariant

$$A * n^n * \text{sum}(x_i) + D = A * D * \frac{n^n + D^{(n+1)}}{n^{(n)} * \text{prod}(x_i)}$$

Fee Distribution

$$\text{acc_fee_per_share} += \frac{\text{fee_amount} * \text{ACC_PRECISION}}{\text{total_liquidity}}$$

Impermanent Loss

IL% = ... ****1e12 precision****

Gas Optimization & Performance

Optimizations Implemented

- Batch Operations, Efficient Storage, Conditional U128 Arithmetic, Event Pruning, Table Indexing.

Table of Typical Gas Costs

Operation	Estimated Gas
Create Pool	~2M gas
Add Liquidity	~500K gas
Swap	~300K gas
Claim Fees	~200K gas
Compound Fees	~600K gas

*Actual costs vary based on pool state and transaction complexity.

Developer-First: An Intuitive and Powerful API

The protocol is designed with clear, well-defined functions for easy integration.

```
// Add liquidity and receive an LP NFT

use sui_ammm::pool;

let (position, refund_a, refund_b) =
pool::add_liquidity<USDC, USDT>(
    pool,
    coin_a,
    coin_b,
    min_liquidity, // minimum LP shares
    clock,
    deadline_ms, // transaction deadline
    ctx
);

transfer::public_transfer(position,
    user_address);
```

```
// Swap with built-in slippage protection

use sui_ammm::pool;

let output_coin =
pool::swap_a_to_b<USDC, USDT>(
    pool,
    input_coin,
    min_output, // slippage protection
    ctx, // slippage protection
    option::none(), // no price limit
    clock,
    deadline_ms,
    ctx
);
```

```
// Reinvest all earned fees in a single
transaction

use sui_ammm::fee_distributor;

let (refund_a, refund_b) =
fee_distributor::compound_fees<USDC,
USDT>(
    pool,
    position, // your LP position NFT
    min_liquidity,
    clock,
    deadline_ms,
    ctx
);
```

From Blueprint to Reality: Project Status & Testnet Deployment

Development Roadmap (Completed)

Core AMM with $x*y=k$

StableSwap Pools

NFT LP Positions with SVG

Fee Auto-compounding

Limit Orders

Governance with Timelocks

Comprehensive Test Suite (>80% coverage)

Security Audit Fixes & Gas Optimizations

Live on Sui Testnet

Network: Sui Testnet

Key Addresses:

- Package ID: `0x6ddd...d0ad3dc148001`
- PoolRegistry: `0xa3f0...f94216a8e0`
- GovernanceConfig: `0x36d7...f31fc1aa87`

Deployment Digest:

`5iMW4cq1M7sULbEG2PgD295HwyTRZg4N3vaPpYdD1Yq
Y`

[View on Sui Explorer](#) 

SUI AMM: Complete, Secure, and Ready for Mainnet

A Dual-Engine Architecture:
Supporting both volatile and stable asset trading with optimized, distinct pool types.

Security as a Core Principle:
Fortified by design with timelocks, economic guards, and a verifiable, high-coverage test suite.



Truly Dynamic Liquidity:
NFT positions provide a superior, composable, and data-rich user experience.

Feature-Complete for Modern DeFi:
Equipped with advanced tools like limit orders and fee auto-compounding, built on a gas-optimized foundation.

The blueprint is complete. The foundation is solid. The protocol is built.