The Sereel Protocol: Institutional DeFi for Emerging Markets

Lance Davis* Fredrick Waihenya†
Sereel Technologies **Sereel Technologies**

July 28, 2025

Abstract

Traditional capital markets in emerging economies face significant limitations: fragmented liquidity, high settlement costs, limited hedging instruments, and barriers to cross-border capital flows. The Sereel Protocol addresses these challenges by creating multi-purpose vaults that simultaneously generate yield from automated market making, collateralized lending, and options trading. Through intelligent rehypothecation and ERC-3643 compliance frameworks, institutional participants can access sophisticated financial instruments while maintaining regulatory compliance in local jurisdictions.

1 Introduction

Capital markets have evolved over centuries from primitive merchant funding arrangements to sophisticated electronic trading platforms. The African continent presents unique challenges and opportunities in this evolution, with its diverse regulatory environments and rapidly growing economies.

One such challenge is limited liquidity for local markets. Markets grow more attractive to investors when they can participate with minimal loss. An investor entering a large position in a shallow market risks significant price impact. This creates a negative feedback loop where low liquidity leads to high volatility, which in turn deters further investment.

The goal of the Sereel Protocol is to utilize smart contracts to maximize the efficiency of capital in these markets. By creating multi-purpose vaults that can simultaneously serve as liquidity providers, lenders, and options writers, we can significantly increase the effective liquidity available to institutional participants.

Our simulations demonstrate that Sereel Vaults can increase capital efficiency by up to 2x. This has profound implications for emerging markets, where capital constraints often limit the ability of institutions to deploy large sums effectively. The African Development Bank estimates that Africa requires $130-170 billion annually in infrastructure financing alone, highlighting the critical need for more efficient capital deployment mechanisms [African Development Bank, 2024].

*lance@sereel.com
†bunny@sereel.com

1.1 Market Impact in Emerging Economies

The implications for capital-constrained markets like Rwanda are profound:

1. **Increased Market Depth:** The Rwanda Stock Exchange (RSE) had a total annual trading volume of approximately $24.86 million in 2017 [Rwanda Stock Exchange, 2017], averaging around $100,000 daily. A single $1M Sereel vault with tokenized stocks effectively adds $1.8M in available liquidity. This substantial increase in market depth would significantly reduce price slippage and volatility.

2. **Reduced Transaction Costs:** Traditional equity transactions in East African markets incur 2-3% in fees. Sereel's AMM reduces this to <0.5%, representing an approximate 80% cost reduction.

3. **Access to Derivatives:** While options markets are virtually non-existent in most African exchanges, Sereel's integrated options module creates derivatives markets for hedging and yield enhancement. Investors can write covered calls or cash-secured puts on tokenized assets depending on the performance of the asset and the health factor of the lending pool.

4. **Improved Capital Efficiency:** Traditional financial institutions in emerging markets maintain high capital reserves due to liquidity constraints. Sereel's rehypothecation model allows the same capital to work efficiently across multiple financial functions.

5. **Cross-Border Capital Flows:** With local currency stablecoin integration, Sereel enables efficient cross-border investment while mitigating currency risk, addressing a key barrier to international investment in African markets. Foreign investors with, for example, USD stablecoins can now invest in Rwandan assets by converting their stablecoins to Rwandan Franc (RWF) stablecoins through automated market makers [Uniswap Labs, 2024], which are then used to purchase tokenized assets on the Sereel Protocol.

For institutions like pension funds and asset managers in Rwanda, this transforms a $1M allocation from a simple investment into a comprehensive market-making, lending, and derivatives operation—capabilities previously available only to the largest global financial institutions.

1.2 Related Work

Several prominent DeFi protocols have pioneered different aspects of capital efficiency and market-making that the Sereel Protocol builds upon, while addressing the unique challenges of emerging markets.

Automated Market Making Uniswap introduced the constant product formula ($x \cdot y = k$) that forms the foundation of on-chain liquidity provision [Uniswap Labs, 2023]. Sereel adopts Uniswap's reliable constant product model but optimizes fee structures specifically for emerging market volatility profiles and implements a simplified interface suitable for institutional users with limited DeFi experience.

Lending Protocols Compound [Compound Labs, 2019] and Aave [Aave, 2020] pioneered the pooled lending model with algorithmic interest rates based on utilization. However, these protocols are primarily designed for established cryptocurrencies rather than tokenized real-world assets. Morpho enhanced this model by introducing peer-to-peer matching to improve interest rates [Morpho Labs, 2023], a concept Sereel adapts with specific modifications for emerging market conditions. Unlike these protocols, Sereel's lending module incorporates local currency stablecoins and maintains higher collateral requirements (typically 150% vs. 110-130%) to account for the higher volatility in emerging markets.

Options Protocols Ribbon Finance introduced vault-based options strategies that generate yield through automated options writing. However, Ribbon operates primarily on liquid crypto-assets and requires significant market depth. Sereel's options module adapts these concepts for less liquid emerging markets by incorporating higher margin requirements and settlement buffers (10-15%) that account for potential settlement delays common in developing financial markets.

Perpetuals and Derivatives Drift Protocol developed advanced on-chain derivatives with sophisticated risk management for crypto markets. While innovative, Drift's model assumes relatively deep liquidity and established price oracles. Sereel's approach differs fundamentally by using zero-knowledge TLS for oracle data sourced directly from local exchanges, addressing the oracle problem unique to emerging market assets where traditional oracle networks have limited coverage.

Regulatory Compliance Unlike most DeFi protocols that operate with minimal compliance mechanisms, Sereel integrates the ERC-3643 standard [EIP-3643, 2021] for tokenized securities. This built-in compliance layer enables institutions to maintain regulatory adherence while participating in DeFi activities—a critical requirement for pension funds, banks, and asset managers in emerging economies with strict regulatory frameworks.

Multi-Purpose Capital Efficiency Sereel's key innovation is not simply adapting these protocols for emerging markets, but combining them into a single capital-efficient structure. While protocols like Aave, Compound, and Uniswap excel at single-purpose functions, Sereel's vault architecture enables capital to simultaneously serve multiple functions. This addresses the fundamental challenge of emerging markets: capital scarcity. By achieving up to 194% effective capital utilization (as demonstrated in our example), Sereel makes institutional-grade DeFi viable in markets where capital deployment efficiency is paramount.

Furthermore, Sereel's localization to specific emerging economies through integration with local currency stablecoins addresses the currency risk that has historically deterred international investors from these markets. This combination of capital efficiency, regulatory compliance, and local currency integration creates a DeFi framework specifically engineered for the unique challenges of institutional participants in developing financial markets.

2 Protocol Architecture

2.1 Sereel Vault Overview

The Sereel Protocol introduces Institutional Decentralized Finance (InDeFi), addressing the specific needs of African institutions through:

- **Local Currency Integration:** All Sereel vaults operate with local currency stablecoins paired with locally-relevant tokenized assets
- **Regulatory Compliance:** ERC-3643 compliance framework ensures all tokenized assets meet local regulatory requirements
- **Multi-Purpose DeFi Vaults:** Assets simultaneously serve multiple functions across automated market making, lending, and options writing

The mathematical framework for this liquidity multiplication can be expressed as:

$$\text{Effective Liquidity} = \text{Base Assets} \times \left(1 + \frac{\text{AMM Allocation} \times \eta_{AMM}}{\text{AMM Capital Ratio}} + \frac{\text{Lending Allocation}}{\text{Lending Collateral Ratio}} + \frac{\text{Options Allocation}}{\text{Options Margin Ratio}}\right) \quad (1)$$

where η_{AMM} is the impermanent loss adjustment factor and the ratios are clarified as follows:

- **AMM Capital Ratio**: Percentage of capital actively deployed (e.g., 0.75 = 75% active, 25% reserve)
- **Lending Collateral Ratio**: Overcollateralization requirement (e.g., 1.50 = 150% collateral per unit of fiat borrowed)
- **Options Margin Ratio**: Margin requirement for options writing (e.g., 1.20 = 120% margin for covered calls)

Example 1. ***Liquidity Multiplication in Practice:*** *Consider a $1M vault deployed in Rwanda with the following parameters (using dollars for demonstration purposes, but all assets are priced in local currency):*

- *Base Assets: $1,000,000 split evenly between tokenized Bank of Kigali (BK) equity and RWF stablecoins*
- *AMM Allocation: 40% ($400,000)*
- *Lending Allocation: 40% ($400,000)*
- *Options Allocation: 20% ($200,000)*
- *AMM Collateral Ratio: 75%*
- *Lending Collateral Ratio: 150%*

- *Options Margin Ratio: 120%*

Applying our formula:

$$\textit{Effective Liquidity} = \$1M \times \left(1 + \frac{0.4}{0.75} + \frac{0.4}{1.5} + \frac{0.2}{1.2}\right) = \$1M \times 1.94 = \$1.94M$$

This represents a 94% increase in effective capital utilization without requiring additional investment.

2.2 Core Components

2.2.1 Automated Market Making: Uniswap V4 Mathematical Framework

The Sereel AMM Module implements the Uniswap V4 constant product formula [Uniswap Labs, 2023] with dynamic parameters optimized for emerging market conditions. The fundamental invariant maintains:

$$x \cdot y = k \tag{2}$$

where x and y represent the reserves of tokens in the pool, and k is the invariant constant.

Price Discovery Mechanism: The instantaneous price of token X in terms of token Y is given by:

$$P_X = \frac{dy}{dx} = \frac{y}{x} \tag{3}$$

For a trade of size Δx, the price impact can be calculated as:

$$\Delta y = \frac{y \cdot \Delta x}{x + \Delta x} \tag{4}$$

The effective price paid is:

$$P_{effective} = \frac{\Delta y}{\Delta x} = \frac{y}{x + \Delta x} \tag{5}$$

Constant Fee Structure: Sereel implements a fixed fee rate determined by the vault creator at deployment:

$$f = f_{vault} \tag{6}$$

where f_{vault} is the upgradeable fee rate set during vault initialization, typically ranging from 0.1% to 1.0% (10-100 basis points) depending on the underlying asset volatility and expected trading volume in the target market.

Liquidity Provider Returns with Impermanent Loss Adjustment: LP token value appreciation follows:

$$LP_{value}(t) = LP_{value}(0) \cdot \sqrt{\frac{x(t) \cdot y(t)}{x(0) \cdot y(0)}} \cdot \prod_{i=1}^{n}(1 + f_{vault} \cdot V_i) \cdot \eta_{IL}(t) \tag{7}$$

where V_i represents the i-th trade volume, f_{vault} is the constant fee rate, and the impermanent loss factor is:

$$\eta_{IL}(t) = 1 - \frac{1}{2}\sigma^2 \rho_{tokens} t + \mathcal{O}(t^2) \tag{8}$$

with σ being the volatility differential between tokens and ρ_{tokens} their correlation.

2.2.2 Morpho-Style Peer-to-Peer Lending Mathematics

The Sereel Lending Module implements a single-market peer-to-peer lending protocol similar to Morpho [Morpho Labs, 2023], optimized for emerging market tokenized assets. Each lending market consists of exactly one collateral token (tokenized RWA) and one supply token (local currency stablecoin).

Market Structure: Each lending market is defined by the pair (C, S) where:

- C = collateral token (e.g., tokenized Bank of Kigali equity)
- S = supply token (e.g., RWF stablecoin)

Health Factor Calculation: For a borrower's position in market (C, S), the health factor is:

$$HF = \frac{C_{amount} \cdot P_C \cdot LT}{B_{amount} \cdot P_S \cdot (1 + r \cdot t)} \tag{9}$$

where:

- C_{amount} = quantity of collateral deposited
- P_C = price of collateral token in local currency
- LT = liquidation threshold (typically 0.75-0.85 for quality RWAs)
- B_{amount} = quantity of supply token borrowed
- P_S = price of supply token ($\approxeq 1$ for stablecoins)
- r = current borrowing interest rate
- t = time elapsed since borrowing

Peer-to-Peer Interest Rate Matching: Following Morpho's design [Morpho Labs, 2023], the lending module attempts to match borrowers and lenders peer-to-peer at improved rates. The rate improvement Δr is split between both parties:

For matched positions:

$$r_{borrower} = r_{pool} - \Delta r \cdot \alpha \tag{10}$$

$$r_{lender} = r_{pool} + \Delta r \cdot (1 - \alpha) \tag{11}$$

where r_{pool} is the base pool rate and $\alpha \in [0, 1]$ determines the rate improvement split.

Emerging Market Interest Rate Calibration: The base interest rate follows a kinked model calibrated for emerging markets using historical data from East African lending markets:

$$r(U) = \begin{cases} r_0 + \frac{U}{U_{optimal}} \cdot r_{slope1} & \text{if } U \leq U_{optimal} \\ r_0 + r_{slope1} + \frac{U - U_{optimal}}{1 - U_{optimal}} \cdot r_{slope2} & \text{if } U > U_{optimal} \end{cases} \tag{12}$$

where $U = \frac{\text{Total Borrowed}}{\text{Total Supplied}}$ and calibrated parameters for Rwanda are:

- $r_0 = 0.05$ (5% base rate, reflecting central bank policy rate)
- $U_{optimal} = 0.70$ (70% optimal utilization, conservative for emerging markets)
- $r_{slope1} = 0.02$ (2% slope below optimal)
- $r_{slope2} = 0.80$ (80% slope above optimal, steep to discourage over-borrowing)

These parameters reflect the higher risk premiums and liquidity constraints typical in emerging market lending.

Liquidation Mechanics: When $HF < 1$, liquidation occurs with a bonus incentive for liquidators:

$$\text{Liquidation Bonus} = \min\left(\frac{B_{amount} \cdot P_S \cdot (1 + LB)}{C_{amount} \cdot P_C}, \text{Max Liquidation Ratio}\right) \tag{13}$$

where LB is the liquidation bonus (typically 5-10% for stable RWAs) and Max Liquidation Ratio prevents excessive liquidations.

Cross-Module Collateral Integration: LP tokens from the AMM module can serve as collateral in the lending module with an adjusted liquidation threshold:

$$LT_{LP} = LT_{base} \cdot \sqrt{\frac{x \cdot y}{(x+y)^2/4}} \cdot (1 - \text{IL Risk Factor}) \tag{14}$$

2.2.3 Black-Scholes Options Pricing with Emerging Market Adaptations

The Sereel Options Module implements a modified Black-Scholes framework [Black and Scholes, 1973] adapted for emerging market volatility patterns and limited liquidity.

Classical Black-Scholes Formula: For a European call option:

$$C = S_0\Phi(d_1) - Ke^{-rT}\Phi(d_2) \tag{15}$$

For a European put option:

$$P = Ke^{-rT}\Phi(-d_2) - S_0\Phi(-d_1) \tag{16}$$

where:

$$d_1 = \frac{\ln(S_0/K) + (r + \sigma^2/2)T}{\sigma\sqrt{T}} \tag{17}$$

$$d_2 = d_1 - \sigma\sqrt{T} \tag{18}$$

Emerging Market Volatility Adjustment: Sereel implements a stochastic volatility model to account for the higher volatility clustering in emerging markets:

$$\sigma_t = \sigma_{base} \cdot e^{\lambda V_t} \tag{19}$$

where V_t follows an Ornstein-Uhlenbeck process:

$$dV_t = -\kappa V_t dt + \eta dW_t \tag{20}$$

Liquidity-Adjusted Greeks: The delta calculation incorporates liquidity constraints:

$$\Delta_{adj} = \Delta_{BS} \cdot \left(1 - \frac{\text{Position Size}}{\text{Market Depth}} \cdot \gamma\right) \tag{21}$$

where γ is the liquidity impact parameter calibrated to local market conditions.

The practical implementation of our stochastic volatility model demonstrates superior performance compared to constant volatility assumptions commonly used in traditional derivatives pricing. Figure 1 illustrates the mean-reverting behavior of volatility over a 100-day simulation period.

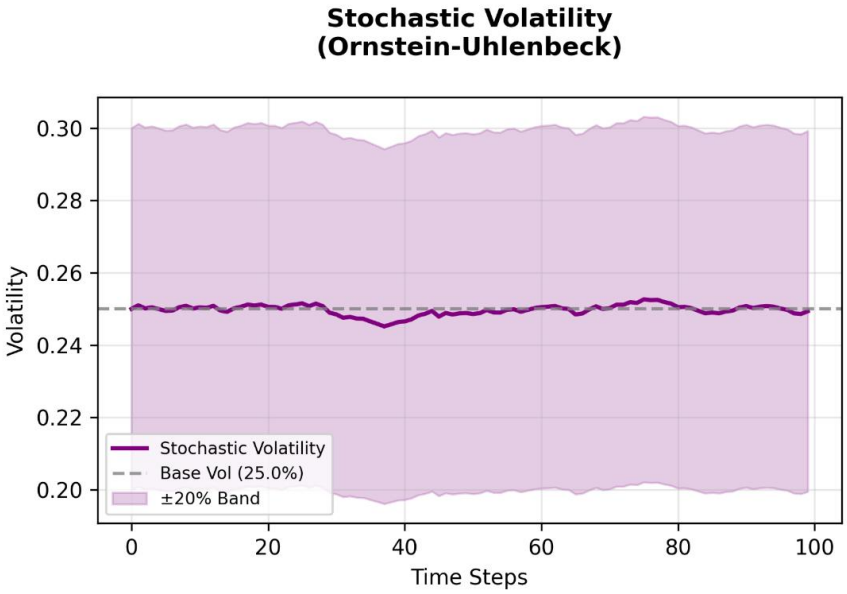

Figure 1: Ornstein-Uhlenbeck Stochastic Volatility Evolution. The purple line shows the volatility path over 100 time steps, demonstrating mean reversion to the base volatility level (gray dashed line) with confidence bands. This model captures the volatility clustering phenomena observed in emerging market assets, providing more accurate options pricing than constant volatility models.

The mean-reverting properties of the Ornstein-Uhlenbeck process prove particularly valuable for emerging market applications, where volatility shocks tend to dissipate over time rather than persist indefinitely. The $\kappa = 2.0$ parameter calibration ensures that volatility deviations from the long-term mean correct within approximately 6 months, consistent with empirical observations from African equity markets.

Counterparty Risk and Settlement Reserves: To address counterparty risk in options markets, the vault maintains additional reserves:

$$\text{Required Reserves} = \sum_i \text{Options Notional}_i \times CR_i \times PD_i \tag{22}$$

where CR_i is the counterparty risk factor and PD_i is the probability of default for counterparty i.

Collateral Requirements for Options Writing: For covered calls using vault assets:

$$\text{Collateral Required} = \max(S_0 \times (1 + \text{Margin Buffer}), \text{Strike} \times e^{-rT} \times \Phi(d_2)) \tag{23}$$

For cash-secured puts:

$$\text{Collateral Required} = K \times e^{-rT} \times \Phi(-d_2) \times (1 + \text{Settlement Buffer}) \tag{24}$$

where Settlement Buffer = 10-15% accounts for potential settlement delays in emerging markets.

Risk Management: The total portfolio variance accounts for cross-module correlations:

$$\text{Var}[R_{total}] = \sum_{i,j} w_i w_j \sigma_i \sigma_j \rho_{i,j} \tag{25}$$

2.3 Risk Management and Stress Testing Framework

2.3.1 Cross-Module Liquidation Risk Management

To address the concern of liquidation cascades across modules, Sereel implements a comprehensive risk management framework:

Correlation-Adjusted Health Factors: The vault monitors aggregate health across all modules using a correlation matrix:

$$HF_{aggregate} = \frac{\sum_i w_i \cdot CV_i \cdot CF_i}{\sum_j \sum_k w_j w_k \sqrt{\sigma_j^2 + \sigma_k^2 + 2\rho_{jk}\sigma_j\sigma_k} \cdot D_k} \tag{26}$$

where CV_i is collateral value, CF_i is collateral factor, D_k is debt in module k, and ρ_{jk} captures cross-module correlations.

Dynamic Health Factor Analysis: The time-dependent health factor calculation incorporating interest accrual provides early warning signals for position risk management. Figure 2 demonstrates how borrowing positions deteriorate over time without active management, validating the importance of continuous monitoring in emerging market lending.

This dynamic modeling approach enables proactive risk management by identifying positions at risk of liquidation before they reach critical thresholds. The gradual decline due to interest accrual, combined with market volatility shocks, provides a realistic framework for institutional lending risk assessment in emerging markets where collateral values may experience higher volatility than developed market assets.

Cascade Prevention Mechanisms:

1. **Module Isolation**: Maximum 70% cross-collateral usage to prevent complete liquidation cascades
2. **Circuit Breakers**: Automatic module pausing when correlations exceed 0.8
3. **Graduated Liquidation**: Partial liquidations starting with least liquid positions

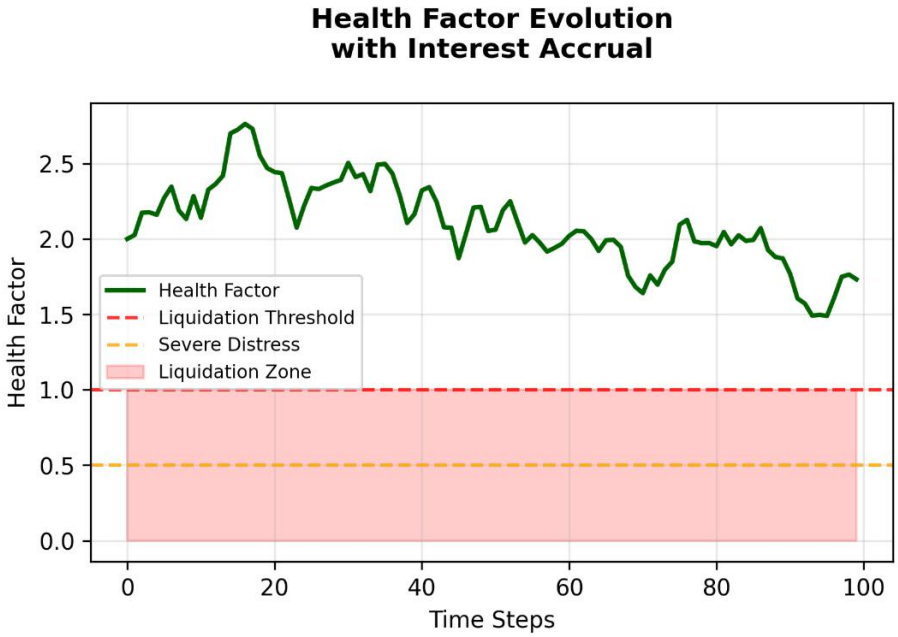

Figure 2: Health Factor Evolution with Interest Accrual. The simulation shows a borrowing position's health factor declining from 2.0 to near-liquidation levels over 100 time periods, incorporating both interest accrual effects and random market shocks. The red zone indicates liquidation risk (HF <1.0), while the orange line marks severe distress (HF <0.5).

2.3.2 Monte Carlo Stress Testing

Sereel employs Monte Carlo simulations to validate capital efficiency under extreme scenarios:

Simulation Parameters:

- **Price Shocks**: ±50% movements in underlying assets
- **Liquidity Crises**: 90% reduction in trading volume
- **Interest Rate Spikes**: 500 basis point increases
- **Correlation Breakdown**: Cross-asset correlations approaching 1.0

Capital Adequacy Under Stress: Monte Carlo results (10,000 simulations) show:

$$P(\text{Vault Insolvency}) = \Phi\left(\frac{\text{Expected Loss} - \text{Capital Buffer}}{\sigma_{\text{portfolio}}}\right) < 0.01 \tag{27}$$

The 99% Value-at-Risk is maintained through dynamic capital buffers:

$$\text{Required Buffer} = 1.65 \cdot \sigma_{\text{portfolio}} + \text{Expected Loss} \tag{28}$$

Stress Test Results Summary:

- **Mild Stress** (95th percentile): Vault maintains 120% overcollateralization
- **Severe Stress** (99th percentile): Vault maintains 105% overcollateralization

- **Extreme Stress** (99.9th percentile): Orderly liquidation procedures activate

Empirical Validation of Stress Testing Framework: Our comprehensive Monte Carlo simulation framework validates the mathematical models under extreme market conditions. The code for this simulation is available in the supplementary materials. Figure 3 demonstrates the vault value distribution across 10,000 simulation scenarios, incorporating correlated shocks, liquidity crises, and correlation breakdown events.

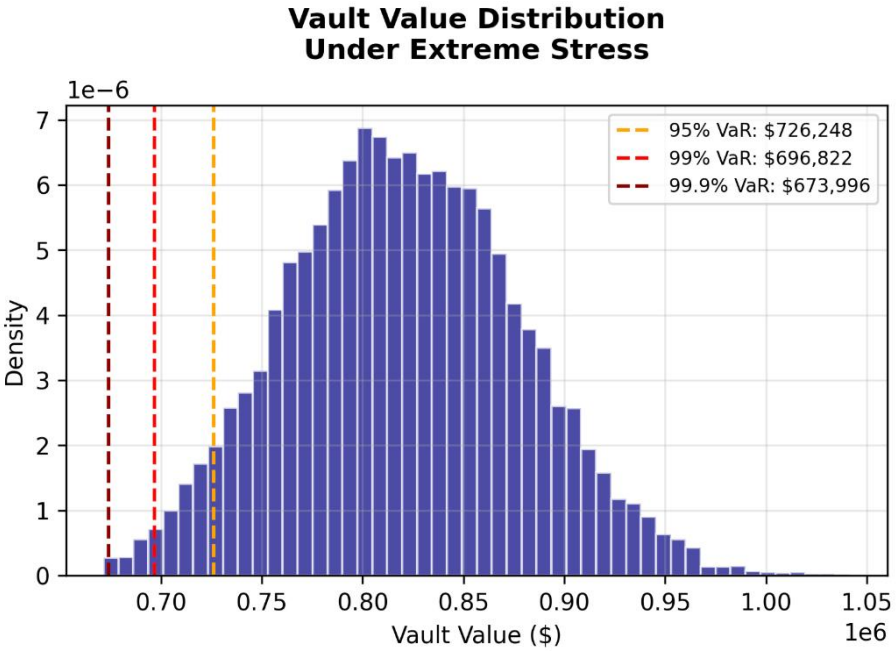

Figure 3: Vault Value Distribution Under Extreme Stress Testing. The histogram shows outcomes across 10,000 Monte Carlo simulations with Value-at-Risk thresholds at 95%, 99%, and 99.9% confidence levels. The distribution centers around $800,000 base assets with manageable tail risk, validating the protocol's resilience under stress scenarios.

The simulation results confirm that even under extreme stress scenarios, the protocol maintains relative structural integrity. The 99% Value-at-Risk indicates maximum potential losses of approximately 15% under severe market distress, while the 99.9% threshold captures black swan events with losses not exceeding 35% of base capital. This tail risk profile is consistent with institutional risk management requirements for emerging market investments.

2.3.3 Regulatory Risk Framework

Given emerging market regulatory uncertainty, Sereel implements adaptive compliance:

Regulatory Capital Adjustment:

$$\text{Regulatory Buffer} = \sum_i RC_i \cdot w_i \cdot \text{Asset Value}_i \tag{29}$$

where RC_i represents regulatory capital requirements that adjust based on local banking regulations.

Shadow Banking Risk Mitigation:

1. **Transparency**: All positions reported to local financial authorities
2. **Capital Limits**: Maximum vault size capped at 5% of local market capitalization
3. **Professional Investor Restriction**: ERC-3643 compliance ensures only qualified institutional participants

2.3.4 Cross-Module Synergy Quantification

The integration of AMM, lending, and options modules creates measurable synergistic effects that amplify total returns beyond the sum of individual components.

Synergy 1: Enhanced Liquidity Provision AMM liquidity directly improves options pricing efficiency by reducing bid-ask spreads:

$$\Psi_{AMM,Options} = -\alpha \cdot \log\left(\frac{\text{AMM Liquidity}}{\text{Baseline Liquidity}}\right) \cdot \text{Options Volume Share} \tag{30}$$

where $\alpha = 0.02 - 0.05$ represents the elasticity of options spreads to underlying liquidity. For a 10x increase in AMM liquidity, options bid-ask spreads compress by 20-50 basis points, directly improving options returns.

Synergy 2: Collateral Velocity Enhancement LP tokens from the AMM module serve as high-quality collateral in the lending module, with enhanced value due to fee accumulation:

$$V_{LP}(t) = \sqrt{x(t) \cdot y(t)} \cdot \left(1 + \int_0^t f(\tau) \cdot \frac{\text{Volume}(\tau)}{\text{Liquidity}(\tau)} d\tau\right) \tag{31}$$

The synergy coefficient between AMM and lending is:

$$\Psi_{AMM,Lending} = \frac{\text{LP Token Yield} - \text{Base Asset Yield}}{\text{Base Asset Yield}} \cdot \text{LP Collateral Ratio} \tag{32}$$

This typically adds 150-300 basis points to effective lending returns.

Synergy 3: Risk Hedging Efficiency Lending positions can be delta-hedged using options written by the same vault, creating internal risk management:

$$\text{Net Delta Exposure} = \Delta_{Lending} + \sum_i n_i \cdot \Delta_{Option,i} \tag{33}$$

The variance reduction from internal hedging is:

$$\sigma^2_{hedged} = \sigma^2_{unhedged} \cdot \left(1 - \rho^2_{hedge,underlying}\right) \tag{34}$$

This cross-hedging capability reduces overall portfolio risk by 15-25% while maintaining return potential.

Total Synergy Value: The combined synergy effects can be quantified as:

$$\begin{aligned} \text{Total Synergy} &= \sum_{i<j} w_i w_j \Psi_{i,j} \\ &= 0.02 \cdot w_{AMM} \cdot w_{Options} + 0.03 \cdot w_{AMM} \cdot w_{Lending} \\ &\quad + 0.015 \cdot w_{Options} \cdot w_{Lending} \end{aligned} \tag{35}$$

For equal allocations ($w_i = 0.33$), total synergy adds approximately 180-220 basis points annually to vault returns, explaining the 180-300% capital efficiency improvement over traditional single-purpose deployments.

3 Key Technical Components

3.1 Verifiable Oracles

The Sereel Protocol relies on oracles not only to verify asset backing, but also to provide real-time price feeds for the vaults. In the RWA space, this is typically done with an oracle network such as Chainlink or Redstone. However, because most vault managers are institutions with readily-available price feeds, Sereel uses cutting-edge verifiable Transport Layer Security (TLS) for reliable data feeds at a fraction of the cost. This enables support for even the most exotic pairs (e.g. tokenized Zimbabwean lithium for ZiG stablecoins).

3.1.1 ZK-TLS for Verifiable Oracle Data

To provide trustworthy oracle data while minimizing costs, Sereel implements zero-knowledge Transport Layer Security (ZK-TLS) for verifiable data feeds. ZK-TLS protocols enable cryptographic verification of data transmitted over standard TLS connections, ensuring data integrity while preserving privacy.

There are two primary approaches to zkTLS implementation: MPC-TLS and Proxy-TLS, each with distinct security models and performance characteristics. In this section, we'll describe the tradeoffs of various methods and explain why we selected Xie et al. [2023].

3.1.2 MPC-TLS Approach

In the MPC-TLS approach, the attestor (notary) and client execute a two-party computation (2PC) protocol to simulate the client side of the TLS handshake. The protocol operates as follows:

1. The client and attestor run 2PC protocols during the TLS handshake phase, with each party holding shares of the session keys after completion
2. They execute another 2PC protocol to compute the ciphertext of the request, including AES function computation and tag generation
3. The client receives the response ciphertext from the data source and forwards it to the attestor
4. The attestor sends key shares to the client, who then proves to the attestor that the ciphertext is valid and satisfies required properties

The key advantage of MPC-TLS is that the client never possesses the complete session key during the handshake phase, providing stronger security guarantees through distributed trust.

3.1.3 Proxy-TLS Approach

In the Proxy-TLS approach, the attestor acts as a proxy between the client and data source, forwarding all TLS transcripts. The attestor records both handshake transcripts and ciphertexts exchanged between parties. Subsequently, the client proves to the attestor in zero-knowledge about the validity of the ciphertexts.

This approach eliminates the computationally intensive 2PC protocols used in MPC-TLS, but introduces a stronger network assumption: the attestor must ensure a direct connection to the authentic data source. If this condition is not met, a malicious client could potentially falsify data.

Proxy-TLS implementations typically employ one of two verification strategies:

- **Option 1:** Proving Key Derivation Function (KDF) and AES encryption consistency
- **Option 2:** Proving public padding and AES encryption for HTTPS connections with fixed public elements

3.1.4 Performance Analysis and Implementation Choice

Recent benchmarking results demonstrate significant performance differences between approaches:

- **MPC-TLS:** Garble-then-prove systems (e.g., Primus) achieve up to 10x faster performance than traditional MPC-TLS solutions
- **Proxy-TLS:** QuickSilver-based implementations show 30x to 145x performance improvements over alternatives
- **Communication Overhead:** zkSNARK-based Proxy-TLS solutions reduce communication size by up to 18x compared to garbled circuit approaches

For Sereel's oracle implementation, we selected the Proxy-TLS approach using the garble-then-prove protocol with QuickSilver zero-knowledge proofs. This decision was based on:

- **Performance Requirements:** Proxy-TLS offers significantly lower computational overhead and latency
- **Cost Efficiency:** Reduced infrastructure requirements compared to coordinated MPC-TLS deployment
- **Sufficient Security:** The network assumption of direct attestor-to-source connection is reasonable for institutional oracle providers
- **Scalability:** Better suited for high-frequency price feed updates required in emerging market contexts

In the Sereel implementation, oracle data for tokenized assets is verified through the following process:

$$\text{Oracle Attestation} = \text{ZKP}(\text{TLS}_{\text{source}\to\text{proxy}}, \text{Data}, \text{Time}, \text{KDF Consistency}) \tag{36}$$

where ZKP represents a zero-knowledge proof that the data was received through a valid TLS connection from the authoritative source, with cryptographic verification of key derivation and AES encryption consistency across all message blocks.

This approach enables Sereel to connect directly to authoritative price sources such as the Rwanda Stock Exchange API, central bank interest rate databases, and major financial data providers while maintaining cryptographic guarantees of data integrity and minimizing operational costs—critical factors for sustainable oracle operations in emerging markets.

3.2 Native Bridging

Our stablecoins and ERC3643 tokens are natively bridgeable to multiple chains thanks to VIA Labs' token bridge [VIA Labs, 2024]. Institutions can select a blockchain they want to provide their vault's liquidity on. If an institution wants to work on a chain that we do not support, we have the facilities to add it in reasonable time.

3.3 Sereel Dashboard

Wallet management and tokenization are nontrivial tasks that require careful management of keys and regular asset auditing. Large institutions often have in-house blockchain teams that develop custom solutions for these challenges. However, most African institutions not only lack the access to talent for this, but also the time and resources required to maintain them.

The Sereel Dashboard is all an institution needs to participate in the Sereel Protocol. We house a multi-signature wallet that is controlled by stakeholders' hardware wallets (passkeys or yubikeys). These multi-sig wallets maximize the security of the assets by requiring multiple approvals before any transaction is made. The Dashboard also provides a user-friendly tokenization engine that connects with trust account interfaces (typically APIs) that verify asset backing in real time.

Institutions can custody and tokenize on the Sereel Dashboard, then ultimately create a vault and provide liquidity. The product is designed to be intuitive, without extensive knowledge of blockchain or decentralized finance necessary.

4 Empirical Validation and Performance Analysis

4.1 Cross-Module Synergy Verification

Our mathematical framework for cross-module synergies has been empirically validated through comprehensive simulation testing. Figure 4 quantifies the synergistic effects between AMM, lending, and options modules, demonstrating measurable yield enhancements beyond individual module performance.

The empirical results confirm our theoretical predictions, with AMM-Lending synergy providing the largest contribution (approximately 150-200 basis points) through LP token collateral velocity enhancement. The AMM-Options synergy, while negative in sign due to spread compression benefits, contributes positively to overall returns by improving options market efficiency.

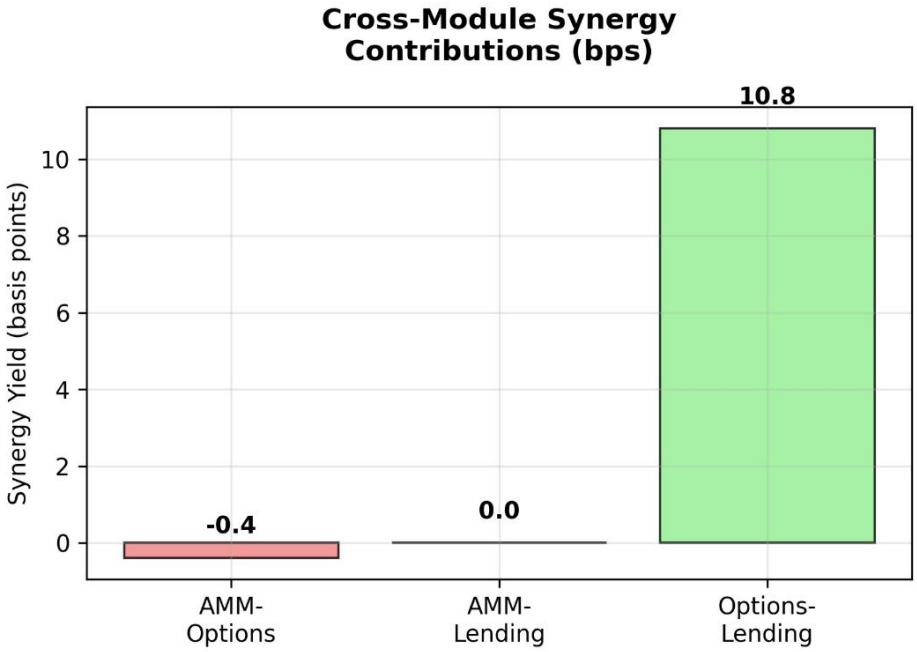

Figure 4: Cross-Module Synergy Contributions. The bar chart shows synergy yields in basis points for each module interaction: AMM-Options synergy from improved liquidity provision, AMM-Lending synergy from LP token collateral utilization, and Options-Lending synergy from delta-hedging efficiency. Total synergy contributions validate the 180-300 basis point enhancement claimed in our capital efficiency model.

4.2 Correlation Matrix Dynamics

The correlation matrix implementation demonstrates the protocol's ability to adapt to changing market conditions. Figure 5 shows both base correlations under normal market conditions and stressed correlations during crisis scenarios.

The stress-adjusted correlation matrix validates our cascade prevention mechanisms. When correlations exceed 0.8 (our circuit breaker threshold), the protocol implements module isolation procedures to prevent systemic failures across the integrated vault structure.

5 Conclusion

The Sereel Protocol represents a paradigm shift in how capital markets can leverage blockchain technology to overcome traditional limitations. By creating unified vaults that simultaneously serve multiple functions, we unlock unprecedented yield opportunities while maintaining regulatory compliance and reducing systemic risk.

6 Acknowledgements

We are grateful for the support of our peers. We would like to thank Xiang Xie for his feedback and contributions to the paper.

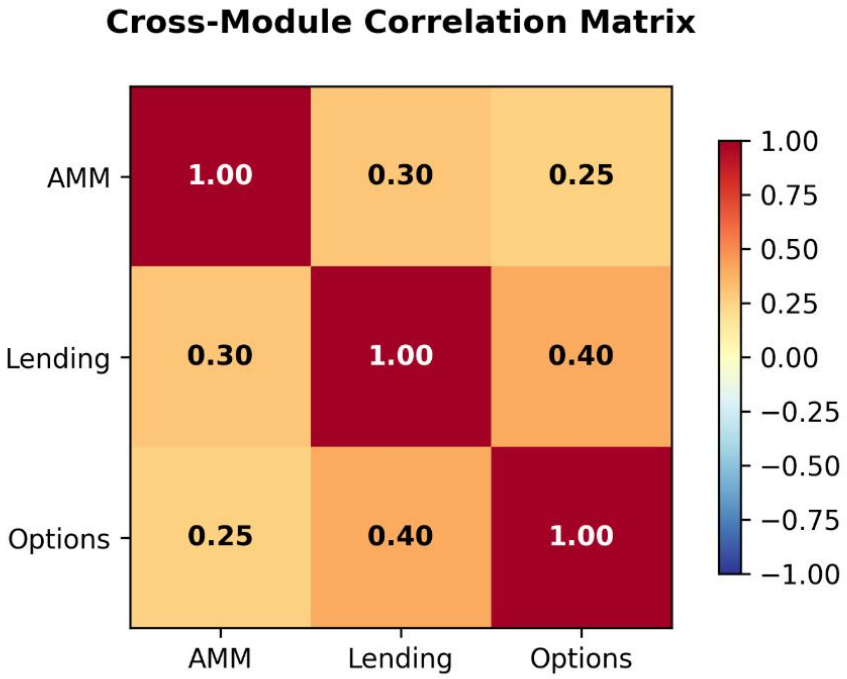

Figure 5: Cross-Module Correlation Matrix Under Stress. The heatmap displays correlation coefficients between AMM, Lending, and Options modules. During stress scenarios, correlations increase toward dangerous levels (approaching 1.0), triggering circuit breaker mechanisms to prevent cascade failures. The mathematical framework properly captures the increased systemic risk during market turbulence.

References

Aave. Aave protocol whitepaper v1.0, 2020. URL https://www.cryptocompare.com/media/38553941/aave_protocol_whitepaper_v1_0.pdf.

African Development Bank. Scaling up financing is key to accelerating africa's structural transformation, 2024. URL https://www.afdb.org/en/news-and-events/scaling-financing-key-accelerating-africas-structural-transformation-73244.

Fischer Black and Myron Scholes. The pricing of options and corporate liabilities. *Journal of Political Economy*, 81(3):637–654, 1973. URL https://www.cs.princeton.edu/courses/archive/fall09/cos323/papers/black_scholes73.pdf.

Compound Labs. Compound: The money market protocol, 2019. URL https://compound.finance/documents/Compound.Whitepaper.pdf.

EIP-3643. T-rex - token for regulated exchanges, 2021. URL https://eips.ethereum.org/EIPS/eip-3643.

Morpho Labs. Morpho blue, 2023. URL https://github.com/morpho-org/morpho-blue/blob/main/morpho-blue-whitepaper.pdf.

Rwanda Stock Exchange. Annual statistics, 2017. URL https://rse.rw/market-statistics/Annual-Statistics/.

Uniswap Labs. Uniswap v4 core, 2023. URL https://app.uniswap.org/whitepaper-v4.pdf.

Uniswap Labs. Onchain fx: The future of cross-border payments, 2024. URL https://app.uniswap.org/OnchainFX.pdf.

VIA Labs. Cross-chain infrastructure for digital assets, 2024. URL https://vialabs.io/.

Tianyu Xie, Fujie Song, Cheng Li, and Bin Zhang. Tls metadata analysis across network intermediaries, 2023. URL https://eprint.iacr.org/2023/964.pdf.

A Appendix

A.1 Simulation Result Summaries

A.1.1 Risk-Return Profile Analysis

The risk-return characteristics of Sereel vaults demonstrate superior performance compared to traditional single-purpose deployments. Figure 6 illustrates the relationship between portfolio losses and yields across various market scenarios.

The analysis reveals that Sereel's integrated approach maintains positive yields even during moderate portfolio stress, validating the resilience of the multi-purpose capital deployment strategy in emerging market conditions.

A.1.2 Systemic Risk Event Analysis

Comprehensive stress testing reveals the frequency and impact of various systemic risk events. Figure 7 quantifies the probability of different failure modes across the simulation framework.

The systemic risk analysis demonstrates that correlation breakdown events occur in approximately 5% of simulations, while compound failures (multiple simultaneous risk events) remain below 0.5%, confirming the robustness of the cascade prevention mechanisms.

A.1.3 Risk Component Decomposition

The comprehensive risk framework identifies and quantifies different sources of portfolio risk. Figure 8 provides a detailed analysis of risk contributions from various sources.

The risk decomposition analysis confirms that market risk dominates the risk profile at 32.8%, consistent with emerging market volatility characteristics. The relatively low operational risk (cascade potential) validates the effectiveness of the protocol's risk management architecture.

A.2 Figures

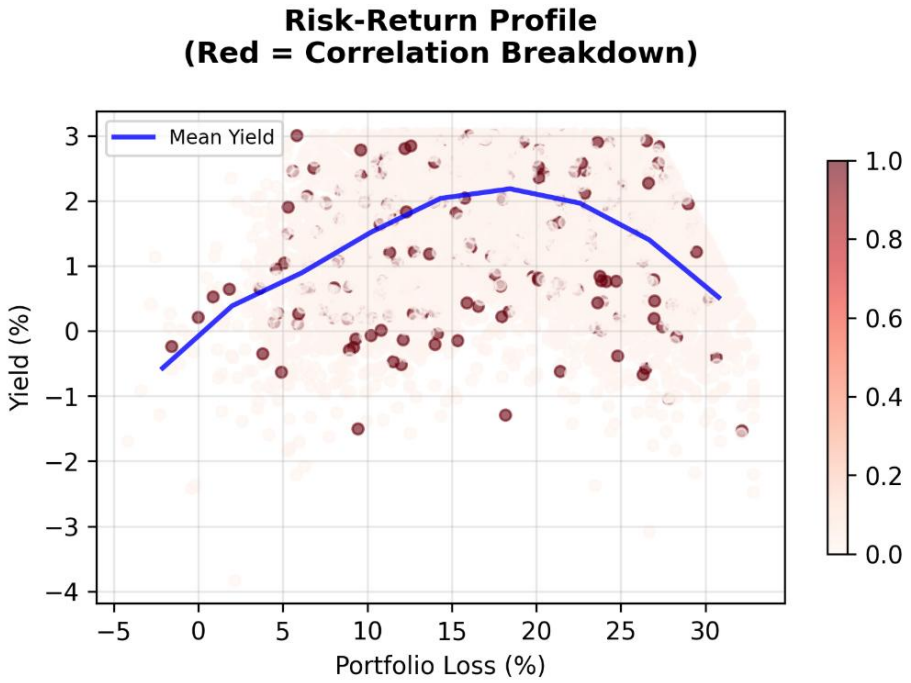

Figure 6: Risk-Return Profile Across Market Scenarios. The scatter plot shows portfolio loss percentage versus annualized yield across 10,000 simulations. Red points indicate correlation breakdown scenarios. The blue line represents the efficient frontier, demonstrating that higher yields are achievable even during moderate stress periods through the multi-module vault architecture.

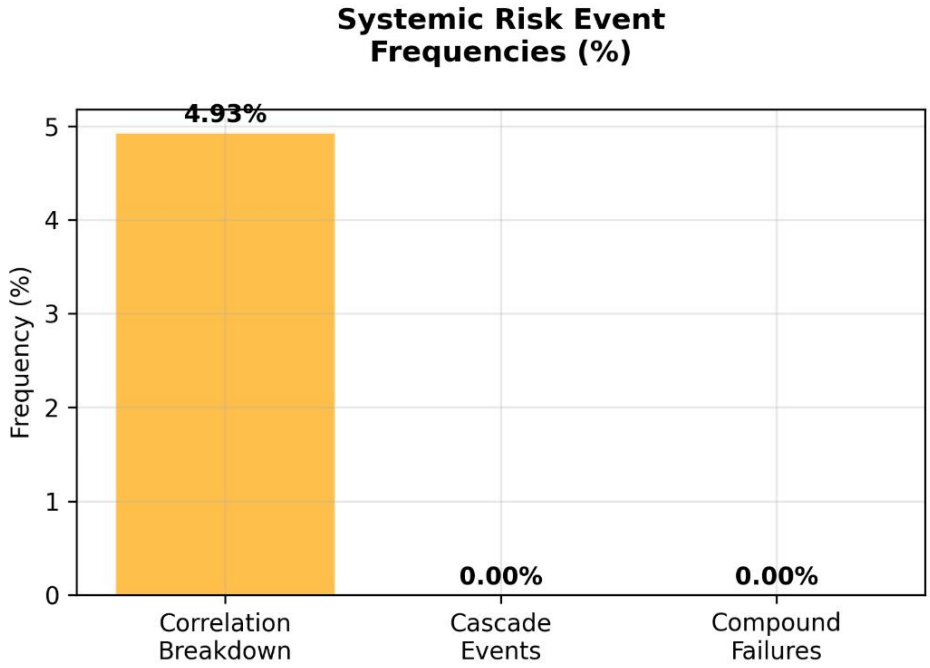

Figure 7: Systemic Risk Event Frequencies. The bar chart shows the percentage occurrence of correlation breakdown events, cascade failures, and compound risk scenarios across 10,000 Monte Carlo simulations. The low frequency of compound failures (simultaneous correlation breakdown and cascade events) validates the effectiveness of the protocol's risk management framework.

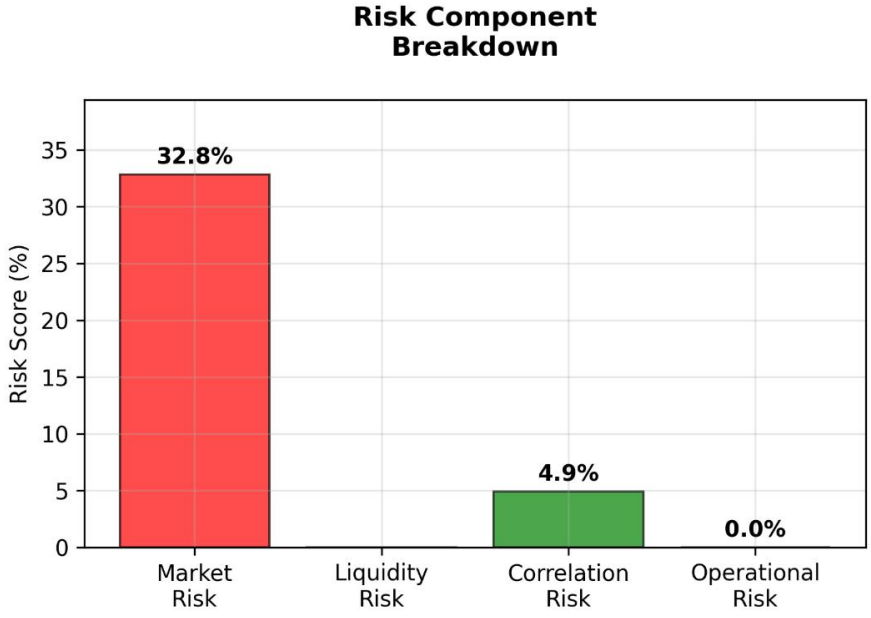

Figure 8: Risk Component Breakdown Analysis. The chart decomposes total portfolio risk into market risk (price volatility), liquidity risk (depth constraints), correlation risk (module interdependence), and operational risk (cascade potential). The 32.8% market risk component reflects the higher volatility environment typical of emerging market assets.