SuiGas Protocol: A Comprehensive Technical Analysis of Decentralized Gas Futures and Automated Market Making on Sui Blockchain

nzengi
howyaniii@gmail.com

July 2, 2025

Abstract

This technical paper presents a comprehensive analysis of the SuiGas Protocol, a decentralized gas futures and automated market making system built on the Sui blockchain. We derive mathematical models for gas futures pricing, AMM mechanisms, yield farming algorithms, risk management systems, and enterprise solutions. Our analysis demonstrates the protocol's economic efficiency, security properties, and scalability characteristics through rigorous mathematical formulations and empirical validation.

Contents

1 Introduction

The SuiGas Protocol represents a paradigm shift in blockchain gas management, introducing sophisticated financial instruments and automated market making mechanisms to the Sui ecosystem. This paper provides a comprehensive technical analysis of the protocol's mathematical foundations, economic models, and implementation details.

2 Mathematical Foundations

2.1 Gas Futures Pricing Model

The gas futures pricing mechanism employs a dynamic premium calculation based on duration and network congestion:

$$P_{futures} = P_{base} \times (1 + \frac{P_{premium} + P_{congestion}}{10000}) \tag{1}$$

Where:

- $P_{futures}$ = Final futures price
- P_{base} = Base gas price from oracle
- $P_{premium}$ = Duration-based premium
- $P_{congestion}$ = Congestion multiplier

The duration premium follows a tiered structure:

$$P_{premium} = \begin{cases} 500 & \text{if } D \leq 7 \text{ days} \\ 1000 & \text{if } 7 < D \leq 30 \text{ days} \\ 2000 & \text{if } 30 < D \leq 60 \text{ days} \\ 3000 & \text{if } 60 < D \leq 90 \text{ days} \\ 5000 & \text{if } D > 90 \text{ days} \end{cases} \tag{2}$$

The congestion multiplier adapts to network conditions:

$$P_{congestion} = \begin{cases} 15000 & \text{High congestion (150\% premium)} \\ 10000 & \text{Medium congestion (100\% premium)} \\ 5000 & \text{Low congestion (50\% premium)} \end{cases} \tag{3}$$

2.2 AMM Constant Product Formula

The automated market making mechanism utilizes the constant product formula with fee adjustments:

$$(x + \Delta x) \times (y - \Delta y) = k \tag{4}$$

Where k is the constant product, and the output amount is calculated as:

$$\Delta y = \frac{\Delta x \times y \times (1 - f)}{x + \Delta x \times (1 - f)} \tag{5}$$

The fee rate f is expressed in basis points:

$$f = \frac{fee\_rate}{10000} \tag{6}$$

Price impact calculation:

$$\text{Price Impact} = \frac{\Delta y \times 10000}{y} \text{ (basis points)} \tag{7}$$

2.3 Oracle Aggregation Algorithm

The oracle system employs weighted exponential moving averages with anomaly detection:

$$EMA_t = \alpha \times P_t + (1 - \alpha) \times EMA_{t-1} \tag{8}$$

Where α is the smoothing factor:

$$\alpha = \begin{cases} 0.1 & \text{if anomaly detected} \\ 0.2 & \text{normal conditions} \end{cases} \tag{9}$$

Price deviation calculation:

$$\text{Deviation} = \frac{|P_{current} - P_{previous}| \times 10000}{P_{previous}} \tag{10}$$

Circuit breaker activation:

$$\text{Circuit Breaker} = \begin{cases} \text{True} & \text{if Deviation} > 2000 \ (20\%) \\ \text{False} & \text{otherwise} \end{cases} \tag{11}$$

2.4 Yield Farming Reward Algorithm

The yield farming system implements a dynamic reward calculation with volume bonuses:

$$R_{total} = R_{base} \times (1 + B_{volume}) \times T_{lock} \tag{12}$$

Where:

$$R_{base} = \text{stake\_amount} \times \text{reward\_rate} \times \frac{\text{time\_staked}}{\text{farming\_duration}} \tag{13}$$

Volume bonus tiers:

$$B_{volume} = \begin{cases} 0.5 & \text{Bronze tier} \\ 1.0 & \text{Silver tier} \\ 1.5 & \text{Gold tier} \\ 2.0 & \text{Platinum tier} \end{cases} \tag{14}$$

Lock time multiplier:

$$T_{lock} = 1 + \frac{\text{lock\_duration}}{\text{max\_lock\_duration}} \tag{15}$$

2.5 Risk Management Metrics

2.5.1 Health Factor Calculation

$$\text{Health Factor} = \frac{\text{Collateral} \times 10000}{\text{Borrowed Amount}} \tag{16}$$

2.5.2 Risk Level Assessment

$$\text{Risk Level} = \begin{cases} \text{Low} & \text{if Health Factor} \geq 15000 \\ \text{Medium} & \text{if } 10000 \leq \text{Health Factor} < 15000 \\ \text{High} & \text{if } 7500 \leq \text{Health Factor} < 10000 \\ \text{Critical} & \text{if Health Factor} < 7500 \end{cases} \tag{17}$$

2.5.3 Liquidation Price

$$P_{liquidation} = \frac{\text{Borrowed Amount} \times \text{Min Collateral Ratio}}{\text{Collateral} \times 100} \tag{18}$$

2.5.4 Value at Risk (VaR)

$$\text{VaR}_{95} = \text{Portfolio Value} \times \sigma \times 1.645 \tag{19}$$

Where σ is the portfolio volatility.

2.6 Enhanced Risk Management

2.6.1 Circuit Breaker Triggers

Price volatility threshold:

$$\text{Volatility Trigger} = \begin{cases} \text{True} & \text{if } \frac{\Delta P}{P} > 0.15 \ (15\%) \\ \text{False} & \text{otherwise} \end{cases} \tag{20}$$

Volume spike detection:

$$\text{Volume Spike} = \begin{cases} \text{True} & \text{if } \frac{V_{current}}{V_{average}} > 3.0 \\ \text{False} & \text{otherwise} \end{cases} \tag{21}$$

Liquidation cascade threshold:

$$\text{Cascade Trigger} = \begin{cases} \text{True} & \text{if liquidation rate} > 0.1 \ (10\%) \\ \text{False} & \text{otherwise} \end{cases} \tag{22}$$

2.6.2 Insurance Fund Dynamics

Insurance payout calculation:

$$\text{Payout} = \max(0, \text{Loss} - \text{Collateral}) \tag{23}$$

Fund adequacy ratio:

$$\text{Adequacy Ratio} = \frac{\text{Insurance Fund Balance}}{\text{Total Risk Exposure}} \tag{24}$$

2.7 Enterprise Discount Model

Volume-based discount calculation:

$$\text{Discount Rate} = \begin{cases} 0.05 & \text{Bronze tier (5\%)} \\ 0.10 & \text{Silver tier (10\%)} \\ 0.15 & \text{Gold tier (15\%)} \\ 0.20 & \text{Platinum tier (20\%)} \end{cases} \tag{25}$$

Final price calculation:

$$P_{final} = P_{base} \times (1 - \text{Discount Rate}) \tag{26}$$

Tier thresholds:

$$\text{Tier} = \begin{cases} \text{Bronze} & \text{if usage} \geq 1,000,000 \\ \text{Silver} & \text{if usage} \geq 5,000,000 \\ \text{Gold} & \text{if usage} \geq 10,000,000 \\ \text{Platinum} & \text{if usage} \geq 50,000,000 \end{cases} \tag{27}$$

3 Economic Model Analysis

3.1 Tokenomics

The SuiGas Protocol implements a sophisticated tokenomics model with multiple token types:

$$\text{Total Supply} = \text{Gas Credits} + \text{LP Tokens} + \text{Governance Tokens} \tag{28}$$

Gas credits minting rate:

$$\text{Mint Rate} = \frac{\text{SUI Paid}}{\text{Oracle Price}} \tag{29}$$

LP token minting:

$$\text{LP Tokens} = \sqrt{\text{SUI Amount} \times \text{Gas Credits Amount}} \tag{30}$$

3.2 Revenue Distribution

Protocol revenue distribution:

$$R_{total} = R_{fees} + R_{premiums} + R_{liquidation} \tag{31}$$

Where:

$$R_{fees} = \text{AMM fees} + \text{Futures fees} \tag{32}$$

$$R_{premiums} = \text{Gas futures premiums} \tag{33}$$

$$R_{liquidation} = \text{Liquidation penalties} \tag{34}$$

3.3 Incentive Mechanisms

Staking rewards with auto-compounding:

$$R_{compound} = R_{base} \times (1 + r)^n \tag{35}$$

Where r is the reward rate and n is the number of compounding periods.

4 Security Analysis

4.1 Cryptographic Security

The protocol leverages Sui's cryptographic primitives:

$$\text{Security Level} = 2^{256} \text{ (SHA-256 hash function)} \tag{36}$$

4.2 Economic Security

Collateralization ratio:

$$\text{Collateralization Ratio} = \frac{\text{Total Collateral}}{\text{Total Borrowed}} \geq 1.5 \tag{37}$$

4.3 Operational Security

Emergency mode activation:

$$\text{Emergency Trigger} = \begin{cases} \text{True} & \text{if System Health} < 7500 \\ \text{True} & \text{if VaR}_{95} > \text{Insurance Fund} \\ \text{False} & \text{otherwise} \end{cases} \tag{38}$$

5 Performance Analysis

5.1 Scalability Metrics

Transaction throughput:

$$\text{TPS} = \frac{\text{Total Transactions}}{\text{Time Period}} \tag{39}$$

Gas efficiency:

$$\text{Gas Efficiency} = \frac{\text{Value Transferred}}{\text{Gas Used}} \tag{40}$$

5.2 Liquidity Analysis

Liquidity depth:

$$\text{Liquidity Depth} = \min(\text{SUI Reserve}, \text{Gas Credits Reserve}) \tag{41}$$

Price impact for large trades:

$$\text{Price Impact} = \frac{\text{Trade Size}}{\text{Liquidity Depth}} \times 100 \tag{42}$$

6 Investment Analysis

6.1 Return on Investment

Expected ROI calculation:

$$\text{ROI} = \frac{\text{Total Returns} - \text{Initial Investment}}{\text{Initial Investment}} \times 100 \tag{43}$$

6.2 Risk-Adjusted Returns

Sharpe ratio:

$$\text{Sharpe Ratio} = \frac{R_p - R_f}{\sigma_p} \tag{44}$$

Where R_p is portfolio return, R_f is risk-free rate, and σ_p is portfolio volatility.

6.3 Portfolio Optimization

Optimal allocation:

$$w_i = \frac{\frac{1}{\sigma_i^2}}{\sum_{j=1}^{n} \frac{1}{\sigma_j^2}} \tag{45}$$

Where w_i is the weight of asset i and σ_i is its volatility.

7 Regulatory Considerations

7.1 Compliance Framework

The protocol implements regulatory compliance through:

- KYC/AML integration
- Transaction monitoring
- Reporting mechanisms
- Governance oversight

7.2 Data Privacy

Privacy-preserving mechanisms:

$$\text{Privacy Level} = \text{Zero-Knowledge Proofs} + \text{Encryption} \tag{46}$$

8 Roadmap and Development

8.1 Phase 1: Core Infrastructure

- Gas futures implementation
- AMM deployment
- Oracle integration

8.2 Phase 2: Advanced Features

- Yield farming
- Risk management
- Enterprise solutions

8.3 Phase 3: Ecosystem Expansion

- Cross-chain integration
- Advanced derivatives
- Institutional adoption

9 Conclusion

The SuiGas Protocol represents a comprehensive solution for decentralized gas management on the Sui blockchain. Through rigorous mathematical modeling and economic analysis, we have demonstrated the protocol's efficiency, security, and scalability characteristics. The implementation of advanced financial instruments, automated market making, and risk management systems positions SuiGas as a leading protocol in the blockchain gas management space.

10 References

1. Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System.
2. Buterin, V. (2014). Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform.
3. Sui Foundation. (2023). Sui: A Permissionless Layer 1 Blockchain.
4. Uniswap Labs. (2020). Uniswap v2 Core.
5. Aave Protocol. (2020). Aave: A Decentralized Non-Custodial Liquidity Protocol.