

# Intenus: Intent-Based DeFi Agent Infrastructure

Wynn Chill Lab  
hello@intenus.xyz

November 22, 2025

## Abstract

Intenus Protocol introduces a universal intent-based trading infrastructure powered by autonomous AI agents that transform natural language trading expressions into executable blockchain transactions. These intent-based AI agents operate within a decentralized network of verified solvers, coordinating through standardized representations defined by the Intenus General Standard (IGS). Each agent interprets, validates, and optimizes user intents, fostering competition to produce the most economically efficient execution strategy.

To ensure trust-minimized coordination, solution verification and ranking are executed within Trusted Execution Environments (TEEs) utilizing the Nautilus Framework. By integrating Walrus for decentralized storage and Seal for programmable access control, Intenus establishes a unified, secure, and verifiable agent network that transcends traditional protocol boundaries and delivers optimal on-chain execution for users.

**Keywords:** Intent-based AI agents, Intent-centric trading, Trusted execution environment, Decentralized solver network, AI-powered ranking, Programmable access control

# Contents

<b>1</b>	<b>Introduction</b>	<b>3</b>
1.1	Key Contributions . . . . .	3
<b>2</b>	<b>Background and Motivation</b>	<b>3</b>
2.1	Current State of Intent-Based Architectures . . . . .	3
2.2	Technical Opportunity . . . . .	4
<b>3</b>	<b>System Architecture</b>	<b>4</b>
3.1	High-Level Overview . . . . .	4
3.2	Core Workflow . . . . .	4
<b>4</b>	<b>Standards and Specifications</b>	<b>5</b>
4.1	Intenus General Standard (IGS) . . . . .	5
4.1.1	Core Primitive Definitions . . . . .	5
4.1.2	Intent Specification . . . . .	5
4.1.3	Solution Specification . . . . .	6
4.2	Decentralized AI Data Standards . . . . .	6
4.2.1	Training Dataset Schema . . . . .	6
<b>5</b>	<b>Core Components</b>	<b>6</b>
5.1	Universal Solver Network (USN) . . . . .	6
5.1.1	Solver Registration and Staking . . . . .	6
5.1.2	Solution Strategies . . . . .	6
5.2	AI-Powered Ranking Engine . . . . .	7
5.2.1	Intent Classification . . . . .	7
5.2.2	Multi-Factor Ranking . . . . .	7
5.2.3	Verifiable Computation . . . . .	7
5.3	Privacy-Preserving Data Management . . . . .	7
5.3.1	Seal Integration for Access Control . . . . .	7
5.3.2	Walrus Storage Integration . . . . .	7
<b>6</b>	<b>Security Model</b>	<b>8</b>
6.1	Trust Assumptions . . . . .	8
6.2	Attack Vectors and Mitigations . . . . .	8
6.2.1	Solver Misbehavior . . . . .	8
6.2.2	Privacy Attacks . . . . .	8
6.3	Slashing and Appeals . . . . .	8
<b>7</b>	<b>Economic Model</b>	<b>9</b>
7.1	Incentive Structure . . . . .	9
7.1.1	Solver Incentives . . . . .	9
7.1.2	User Benefits . . . . .	9
7.2	Fee Distribution . . . . .	9
7.3	Token Economics . . . . .	9
<b>8</b>	<b>Related Work and Positioning</b>	<b>9</b>
8.1	Comparison with Existing Protocols . . . . .	9
8.2	Academic Foundations . . . . .	9
<b>9</b>	<b>Conclusion</b>	<b>10</b>

# 1 Introduction

The decentralized finance ecosystem has evolved into a fragmented landscape where users must navigate multiple protocols, understand complex parameters, and execute transactions across disparate interfaces. Current intent-based protocols address specific use cases—primarily DEX aggregation—but lack the standardization and cross-protocol capability needed for comprehensive DeFi interactions.

Intenus Protocol addresses these limitations by introducing a Universal Solver Network (USN) that operates on standardized intent representations, enabling solvers to compete across all DeFi categories while maintaining verifiable execution quality through AI-powered ranking in trusted environments.

## 1.1 Key Contributions

The protocol introduces several foundational innovations to the DeFi landscape. The Intent General Standard (IGS) provides a comprehensive, extensible schema designed to standardize intent representation across spot trading, limit orders, lending, bridging, and complex DeFi operations.

Furthermore, Intenus implements Verifiable AI Ranking, utilizing advanced machine learning models for Intent Classification and reinforcement learning to determine primary actions and define scoring strategies for solution selection. This evaluation process is securely executed within Trusted Execution Environments (TEEs) using the Nautilus Framework, ensuring unbiased and optimal decision-making.

To ensure security and privacy, the system employs Programmable Access Control, integrating with Seal’s encryption framework to enforce privacy-preserving mechanisms for handling sensitive intents and solver solutions. Finally, Decentralized Data Management is achieved by leveraging Walrus decentralized storage as a secure and efficient repository for archiving intents, solutions, and AI training data, ensuring cost-effective availability without compromising data integrity.

# 2 Background and Motivation

## 2.1 Current State of Intent-Based Architectures

Existing intent-based protocols suffer from several fundamental limitations that hinder broader adoption and efficiency. Protocol Fragmentation and Liquidity Silos remain a significant hurdle, as each protocol typically targets specific DeFi categories (e.g., CoW Protocol for DEX trading), requiring users to interact with multiple specialized platforms.

Additionally, the industry faces a Lack of Standardized Schema. The absence of a unified intent representation standard creates compatibility barriers, restricting solvers to specific protocols, stifling cross-protocol competition, and limiting the innovation of generalized solution strategies.

The ecosystem is also plagued by the Verifiability Dilemma, a trade-off between security and cost. On-chain verification of complex, non-deterministic solutions incurs prohibitive computational overhead and gas costs, while off-chain verification typically lacks trust guarantees, relying heavily on centralized intermediaries.

Finally, current systems rely on One-Dimensional Optimization. Solver selection mechanisms primarily optimize for simple deterministic metrics like lowest gas or maximum output. They lack sophisticated, multi-dimensional ranking mechanisms capable of evaluating qualitative factors such as historical solver reliability, complex user preferences, and risk-adjusted returns.

## 2.2 Technical Opportunity

The convergence of several Sui ecosystem technologies creates an opportunity for a fundamentally new approach. Sui's Programmable Transaction Blocks (PTBs) enable complex, atomic transaction composition that can execute multi-protocol strategies efficiently. The Nautilus TEE Infrastructure provides verifiable off-chain computation capabilities essential for AI-powered solution ranking. Walrus Decentralized Storage offers cost-effective storage for intent data, solutions, and training datasets while maintaining verifiability. Finally, Seal's Programmable Access Control enables sophisticated privacy controls for intent data and solver strategies.

## 3 System Architecture

### 3.1 High-Level Overview

Intenus Protocol operates as a four-layer architecture comprising the Application Layer (User-facing interfaces and Intent Agents), the Coordination Layer (Intent registry and solution orchestration), the Solver Layer (Decentralized network of competing solution providers), and the Infrastructure Layer (Nautilus TEE, Walrus storage, and Seal encryption).

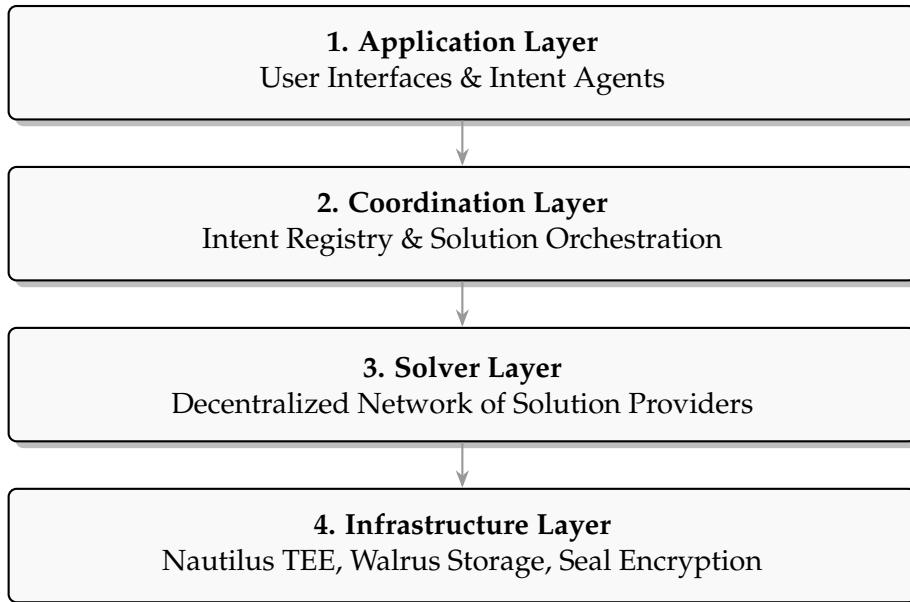


Figure 1: Intenus Protocol Architectural Stack

### 3.2 Core Workflow

The system operates through a defined sequence of stages. First, Intent Submission occurs when users articulate trading goals via the Intent Agent, which transforms natural language or structured parameters into the standardized Intent General Standard (IGS) schema. This is immediately followed by Privacy Protection, where raw intent data is encrypted via Seal's programmable access control framework, enforcing granular visibility permissions to ensure only authorized solvers can decrypt specific fields.

During Solver Competition, registered solvers query available intents and compete to construct optimal execution paths, submitting their proposed solutions within a discrete auction window. Subsequently, AI-Powered Ranking is conducted within a Trusted Execution Environment (TEE) utilizing the Nautilus Framework. Inside this secure enclave, AI models execute Intent Classification and apply reinforcement learning-based scoring strategies to

validate and rank solutions against multi-dimensional metrics such as profitability, risk, and reliability.

Finally, the process concludes with Verifiable Execution, where the protocol selects the optimal solution backed by a verifiable ranking proof. The transaction is executed on-chain, and relevant execution data is archived on Walrus for transparency and future model training.

## 4 Standards and Specifications

To ensure seamless interoperability between the Application Layer (User Intents), the Solver Network, and the AI Training Infrastructure, Intenus Protocol enforces strict data standardization. These standards are defined using JSON Schema Draft 07, ensuring that all system actors—from wallet clients to TEE-based ranking engines—adhere to a unified communication protocol.

### 4.1 Intenus General Standard (IGS)

The IGS Framework acts as the universal language for the protocol. It is composed of three hierarchical schema definitions designed to maximize modularity and extensibility.

#### 4.1.1 Core Primitive Definitions

This schema defines the foundational data types used across the entire protocol. By standardizing primitives such as asset identifiers, numeric precision, and cryptographic signatures, we eliminate ambiguity in data parsing. The Purpose of this schema is to define reusable types (e.g., SuiAddress, BigInt, Timestamp, Signature). Validation enforces strict regex patterns for addresses and range checks for numeric values.

```
1 {
2     "igs_version": "1.0.0",
3     "intent_type": "swap.exact_input",
4     "operation": {
5         "mode": "exact_input",
6         "inputs": [
7             {
8                 "asset_id": "0x2::sui::SUI",
9                 "amount": {"type": "exact", "value": "1000000000"}
10            },
11            "outputs": [
12                {
13                    "asset_id": "0x....::usdc::USDC",
14                    "amount": {"type": "range", "min": "950000", "max": "1000000"}
15                }
16            },
17            "constraints": {
18                "max_slippage_bps": 50,
19                "deadline_ms": 1699123456000
20            }
21        }
22    }
```

Snippet 1: IGS Core Primitive Example

#### 4.1.2 Intent Specification

The Intent Schema governs how user requirements are expressed. It decouples the "what" (user goal) from the "how" (execution path). This schema supports polymorphism, allowing for various intent types (Swap, Limit, Bridge, Lending) within a single structure. Key features include Conditional Logic, which supports constraints like `min_output`, `deadline`, and `max_gas_price`, and Access Control, which integrates Seal-specific fields for encrypted payloads.

### 4.1.3 Solution Specification

Solvers must submit solutions strictly adhering to this schema. This standardization is critical for the Nautilus TEE to deterministically simulate, validate, and rank competing solutions without bias. The components include an Execution Plan (the sequence of Move calls or PTBs), Simulation Results (expected output amounts and gas estimation), and a Solver Commitment (cryptographic signatures binding the solver to specific performance guarantees).

## 4.2 Decentralized AI Data Standards

To fuel the autonomous evolution of the Intenus AI Agents, all interaction data is archived on Walrus decentralized storage. This data serves as the ground truth for model retraining and performance auditing.

### 4.2.1 Training Dataset Schema

This schema defines the structure of historical data blobs stored on Walrus. It aggregates the Intent, the winning Solution, the execution outcome, and market context at the time of execution. Its Utility enables the AI to learn from past solver performance and user behaviors via Reinforcement Learning from Human Feedback (RLHF). Furthermore, Anonymization ensures that sensitive user data is stripped or hashed before being added to the public training set, compliant with privacy standards.

## 5 Core Components

### 5.1 Universal Solver Network (USN)

The USN enables heterogeneous solver strategies to compete on standardized intent representations.

#### 5.1.1 Solver Registration and Staking

Solvers must register with minimum stake requirements and undergo reputation tracking:

Field	Description
solver_address	Uniquely identifies the solver on-chain.
stake_amount	The minimum stake required to participate in auctions.
reputation_score	A dynamic score reflecting historical performance reliability.
total_batches_participated	Count of auction batches the solver has engaged in.
accuracy_score	Metric measuring the precision of solver's past solutions.
status	Current operational status (e.g., Active, Suspended).

Table 1: Solver Profile Data Structure

#### 5.1.2 Solution Strategies

Unlike constrained systems (e.g., CoW's P2P focus), USN supports diverse approaches. DEX Aggregation provides multi-hop routing optimization across AMMs, while P2P Matching performs intent coincidence of wants analysis for peer-to-peer settlement. The system also

supports Hybrid Strategies combining on-chain execution with MEV capture, and AI-Driven Solutions utilizing machine learning-based strategy selection.

## 5.2 AI-Powered Ranking Engine

The ranking engine operates within Nautilus TEE infrastructure to ensure verifiable, unbiased solution evaluation.

### 5.2.1 Intent Classification

Machine learning models classify intents to determine optimal ranking strategies based on intent type, complexity, and market conditions.

### 5.2.2 Multi-Factor Ranking

Solutions are evaluated across multiple dimensions. Economic Efficiency is measured by surplus generation relative to benchmark expectations. Execution Quality assesses gas optimization and slippage minimization. Speed Metrics evaluate expected execution time and confirmation probability, while Solver Reputation considers historical performance and stake-weighted reliability.

### 5.2.3 Verifiable Computation

All ranking computations occur within attested TEE environments. This provides Attestation Proofs for cryptographic verification of computation integrity, ensures Deterministic Results for reproducible ranking given identical inputs, and guarantees Privacy Preservation so solution details remain confidential during evaluation.

## 5.3 Privacy-Preserving Data Management

### 5.3.1 Seal Integration for Access Control

Intenus leverages Seal's programmable access control for sophisticated privacy management:

Field	Description
solver_access_window	Defines the start and end timestamps for allowed access.
requires_solver_registration	Boolean flag enforcing verified solver status.
min_solver_stake	Minimum stake threshold required for decryption access.
auto_revoke_time	Timestamp for automatic revocation of access rights.

Table 2: Intent Policy Data Structure

Access policies ensure that only qualified solvers can decrypt intent data. They enforce time-bounded access to prevent stale solution submissions and implement automatic revocation to protect user privacy post-execution.

### 5.3.2 Walrus Storage Integration

Intent and solution data utilize Walrus's decentralized storage to achieve Cost Efficiency, as off-chain storage reduces transaction costs for large intent schemas. Data Integrity is maintained via cryptographic proofs ensuring data authenticity, while Availability Guarantees provided by distributed storage ensure access for time-sensitive intents.

## 6 Security Model

### 6.1 Trust Assumptions

Intenus operates under a defined trust model. On-Chain Security relies on Sui's consensus mechanism for transaction finality and state consistency. TEE Security trusts the Nautilus infrastructure for computation integrity, verified through remote attestation. Economic Security depends on solver stake amounts and slashing mechanisms to prevent malicious behavior, while Cryptographic Security utilizes Seal's encryption protocols for data confidentiality and access control.

### 6.2 Attack Vectors and Mitigations

#### 6.2.1 Solver Misbehavior

The protocol actively mitigates solver misbehavior. MEV Extraction, where solutions extract value without benefiting users, is mitigated by AI ranking that detects unusual surplus patterns and penalizes violations via slashing. Stale Data Attacks, involving outdated market data, are prevented through timestamp validation in the TEE environment and strict recency requirements. Solution Copying is thwarted by requiring encrypted solution submissions and time-bounded access.

#### 6.2.2 Privacy Attacks

Privacy attacks are addressed through robust encryption. Intent Frontrunning, using intent information for adversarial trading, is mitigated by Seal encryption with time-bounded solver access and automatic revocation. Solution Correlation, enabling the inference of strategies from public solution patterns, is prevented by privacy-preserving ranking in the TEE and differential privacy techniques.

### 6.3 Slashing and Appeals

The protocol implements sophisticated slashing mechanisms:

Field	Description
batch_id	Unique identifier for the auction batch involved.
solver_address	The on-chain address of the accused solver.
severity	Level of the infraction (e.g., Low, Medium, Critical).
attestation	Cryptographic proof of the violation from the TEE.
tee_measurement	Verification of the TEE code state during execution.

Table 3: Slashing Evidence Data Structure

An appeals process allows solvers to challenge slashing decisions within 24-hour windows, with resolution provided by protocol governance.

## 7 Economic Model

### 7.1 Incentive Structure

#### 7.1.1 Solver Incentives

Solvers are incentivized through Performance Rewards, where top-ranked solutions receive proportional fees from executed intents. They also engage in Reputation Building, as consistent performance increases reputation scores, leading to higher solution visibility. Furthermore, Stake Multipliers ensure that higher stake amounts provide competitive advantages in ranking algorithms.

#### 7.1.2 User Benefits

Users gain significant advantages, including Optimized Execution via AI-powered ranking that ensures superior execution compared to direct protocol interaction. The system offers a Simplified UX, where natural language intent expression abstracts complex DeFi mechanics, and robust Privacy Protection, as encrypted intents prevent frontrunning and sandwich attacks.

### 7.2 Fee Distribution

Total fees collected from intent execution are distributed strategically, with Solver Rewards accounting for 90% to selected solution providers, and 10% allocated to the Protocol Treasury for infrastructure maintenance and development.

### 7.3 Token Economics

While Intenus operates on existing tokens (SUI for gas, individual assets for trading), the protocol introduces Reputation NFTs, which are soulbound tokens representing solver performance history, and Achievement Badges for recognition of milestone performance metrics. Future developments will include Governance Tokens for community governance of protocol parameters and upgrades.

## 8 Related Work and Positioning

### 8.1 Comparison with Existing Protocols

Protocol	Scope	Standardization	AI Integration	Privacy
CoW Protocol	DEX Trading	None	No	Limited
1inch	DEX Aggregation	None	No	No
Anoma	General Intents	Partial	No	Yes
<b>Intenus</b>	<b>Universal DeFi</b>	<b>IGS Standard</b>	<b>TEE-based AI</b>	<b>Seal Integration</b>

Table 4: Protocol Comparison

### 8.2 Academic Foundations

The protocol builds upon research in Intent-Based Programming by extending declarative transaction models to DeFi contexts, and Mechanism Design through optimal auction theory for solution selection and fee distribution. It also leverages Trusted Computing via TEE applications in blockchain infrastructure and Privacy-Preserving ML for secure computation in ranking algorithms.

## 9 Conclusion

Intenus Protocol marks a paradigm shift in decentralized finance, transitioning the ecosystem from fragmented, manual interaction models to a unified, intent-centric infrastructure. By successfully harmonizing the Intenus General Standard (IGS) with autonomous AI agents, the protocol resolves the critical "Verifiability Dilemma," proving that complex, off-chain computation can be trusted, audited, and seamlessly executed on-chain.

The protocol's architecture serves as a testament to the power of the Sui ecosystem. By orchestrating the Nautilus Framework for TEE-based solution ranking, Walrus for immutable data availability, and Seal for programmable privacy, Intenus delivers a level of security and efficiency that existing EVM-based intent bridges cannot replicate. This technological convergence ensures that users no longer have to choose between the optimal execution of a centralized exchange and the self-custody of a decentralized network.

As the industry evolves towards an agent-centric economy, Intenus is positioned not merely as a trading tool, but as the foundational middleware for automated finance. The protocol's modular design and open SDKs invite developers to build atop a verified liquidity layer, fostering a positive feedback loop where solver competition drives down costs and enhances execution quality. Ultimately, Intenus establishes the gold standard for how AI agents and blockchain protocols coordinate to deliver value, setting the stage for the mass adoption of intelligent, automated DeFi.

## Glossary

Term	Definition
<b>CoW</b> (Coincidence of Wants)	A situation where two parties each have what the other wants, enabling direct peer-to-peer exchange without intermediate transactions.
<b>IGS</b> (Intenus General Standard)	The universal schema framework that standardizes intent representation across all DeFi operations within the Intenus Protocol.
<b>Intent</b>	A declarative expression of a user's desired outcome without specifying the execution path.
<b>MEV</b> (Maximum Extractable Value)	The maximum value that can be extracted from block production in excess of standard block rewards and gas fees.
<b>PTB</b> (Programmable Transaction Block)	Sui's atomic transaction composition feature that enables complex multi-operation transactions in a single execution.
<b>RLHF</b> (Reinforcement Learning from Human Feedback)	A machine learning technique that incorporates human feedback to improve model performance and alignment.
<b>Slashing</b>	The penalty mechanism that deducts staked tokens from misbehaving solvers as punishment for protocol violations.
<b>Solver</b>	An entity that competes to provide optimal execution strategies for user intents within the protocol.
<b>Soulbound Token</b>	A non-transferable NFT that represents identity, credentials, or reputation that cannot be sold or transferred.
<b>TEE</b> (Trusted Execution Environment)	A secure area of a processor that ensures code and data loaded inside are protected with respect to confidentiality and integrity.
<b>USN</b> (Universal Solver Network)	The decentralized network of competing solvers that operate on standardized intent representations within Intenus Protocol.

## References

- [1] Sui Foundation. (n.d.). *Sui Move Programming Language Reference*. Retrieved November 22, 2025, from <https://docs.sui.io/>
- [2] Danezis, G., Giuliani, G., Kokoris Kogias, E., Legner, M., Smith, J.-P., Sonnino, A., & Wüst, K. (2025). *Walrus: An Efficient Decentralized Storage Network* (v2.0). Mysten Labs. <https://docs.wal.app/walrus.pdfdocs.wal.app+2arXiv+2>
- [3] Mysten Labs. (2024, June 18). *Announcing Walrus: A Decentralized Storage and Data Availability Protocol*. Mysten Labs Blog. <https://www.mystenlabs.com/blog/announcing-walrus-a-decentralized-storage-and-data-availability-protocol>
- [4] Mysten Labs. (2025, March 27). *Walrus Launches on Mainnet, Unlocking Programmable Storage for All*. Mysten Labs Blog. <https://www.walrus.xyz/blog/public-mainnet-launch>
- [5] Mysten Labs. (2025, September 3). *Seal Mainnet Launch: Bringing Data Privacy and Access Control to Web3*. Mysten Labs Blog. <https://www.mystenlabs.com/blog/seal-mainnet-launch-privacy-access-control>
- [6] Mysten Labs. (n.d.). *Seal: Data Encryption and On-chain Access Control*. Retrieved November 22, 2025, from <https://seal.mystenlabs.com/>
- [7] Sui Foundation. (2025, May 8). *Introducing Nautilus: Bringing Verifiable Off-chain Privacy to Sui*. Sui Blog. <https://blog.sui.io/nutilus-offchain-security-privacy-web3/>
- [8] Sui Foundation. (n.d.). *Nautilus: Trusted Execution Environment*. Retrieved November 22, 2025, from <https://docs.sui.io/concepts/cryptography/nautilus>
- [9] Anoma Research. (2023, September 28). *An Introduction to Intents and Intent-Centric Architectures*. <https://anoma.net/blog/an-introduction-to-intents-and-intent-centric-architectures>
- [10] Heuer, M., & Reusche, D. (2024, August 26). *Intent-centric Applications for the Anoma Resource Machine*. Zenodo. <https://doi.org/10.5281/zenodo.13340448>
- [11] Anoma project. (n.d.). *Anoma: A Unified Architecture for Full-Stack Decentralised Applications*. Retrieved November 22, 2025, from the Anoma whitepaper: <https://media.githubusercontent.com/media/anoma/whitepaper/main/whitepaper.pdf>