FLAI Protocol: Decentralized, Privacy-Preserving, Contribution-Aware Federated Learning and Analytics

Balkeum Labs

April, 2025

Abstract

The **FLAI Protocol (Federated Learning & Analytics Infrastructure)** is a decentralized framework for training and monetizing machine learning models across data silos without compromising privacy. Built natively on Web3 principles, FLAI leverages **secure multi-party computation (sMPC)** to enable private, trustless collaboration while introducing governance and incentive structures through **DAOs**, **SubDAOs**, and tokenized economic primitives.

Each machine learning model within the FLAI ecosystem is governed by its own **SubDAO**, where participants earn **soul-bound governance tokens (SBGTs)** through verified contributions of data, compute, and validation. These SBGTs empower contributors to vote on critical model parameters—such as data standards, validation protocols, and hyperparameter schedules—ensuring that governance remains tied to active participation.

In parallel, every model issues a **tradable SubDAO token**, which represents ownership rights over future inference revenue and protocol-level decisions. These tokens form the foundation of a decentralized **model marketplace**, where models are discoverable, auditable, and accessible through a permissionless API.

Two core innovations distinguish FLAI Protocol from legacy FL platforms:

1. **Contribution-Aware Federated Learning**: Leveraging peer validation and score-based evaluation inside the sMPC runtime, FLAI equitably distributes rewards via SubDAO token emissions. Contributors are compensated proportionally to their *true marginal impact* on the global model.
2. **Pay-Per-Inference**: Because the final model resides entirely within an sMPC circuit, no party—including the SubDAO—has access to the full model weights. This enables inference-as-a-service monetization, where users pay per query without ever accessing the model itself, preserving its proprietary status.

Through its modular architecture, FLAI Protocol enables composable, secure, and economically aligned collaboration across untrusted parties, offering a powerful substrate for data-driven applications in healthcare, finance, science, and beyond.

1 Introduction

In an era increasingly shaped by data-driven technologies, the centralized model of machine learning is facing mounting challenges. Legal frameworks such as the General Data Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act (HIPAA), along with data sovereignty laws and the growing public demand for privacy-preserving systems, have rendered traditional approaches to data aggregation and model training both impractical and ethically fraught. Consequently, sectors such as healthcare, finance, and public policy—each reliant on sensitive, siloed datasets—require new paradigms for machine learning and analytics.

Federated Learning (FL) and **Federated Analytics (FA)** have emerged as promising alternatives. FL facilitates collaborative training across distributed data silos without requiring the exchange of raw data, while FA enables the derivation of aggregate insights under similar privacy constraints. Yet, despite their promise, these approaches remain hindered by fundamental limitations. Existing FL systems often depend on centralized aggregators or trusted execution environments (TEEs), both of which constitute single points of failure and trust. Moreover, equitable incentive structures are lacking, as participants are frequently undercompensated and mechanisms to detect free-riding or malicious behavior remain underdeveloped. Finally, most implementations offer limited support for transparent governance, making it difficult for communities to define and update policies regarding model training, data standards, or ownership.

FLAI Protocol: A New Design Paradigm

The **Federated Learning & Analytics Infrastructure (FLAI) Protocol** introduces a reimagined architecture that integrates FL and FA with decentralized technologies, particularly those native to the Web3 ecosystem. At its foundation, FLAI employs secure multi-party computation (sMPC) to facilitate training and inference processes that preserve data confidentiality—not only safeguarding raw inputs, but also obfuscating gradients and intermediate representations.

Central to the FLAI architecture is the notion of **SubDAOs**, or model-specific decentralized autonomous organizations. Each SubDAO governs a distinct model and is instantiated through smart contracts. Governance within a SubDAO is mediated via two complementary token systems. **Soul-Bound Governance Tokens (SBGTs)** are non-transferable credentials that signify meaningful contributions to data provision, computational resources, or model validation. These tokens empower holders to vote on model parameters, data schemas, and federation access policies. In parallel, **SubDAO Tokens** represent tradable ownership stakes tied to future inference revenues and broader strategic decisions. These tokens can be used for staking in model marketplaces or traded in open markets, aligning economic incentives with model success.

Web3 as a Necessity

FLAI does not merely transplant FL into a blockchain context; rather, it is architected from the ground up to operate within the economic and trust assumptions of a decentralized internet. Blockchain infrastructure provides immutable records of model evolution, contributor identity, and validation outcomes. Decentralized autonomous organizations (DAOs), including SubDAOs, facilitate cross-jurisdictional collaboration and collective stewardship over both technical and economic dimensions of model development. Smart contracts further automate critical protocol mechanisms such as revenue distribution, token issuance, and enforcement of governance policies.

Economic Alignment Through Contribution-Aware Design

Perhaps the most innovative component of FLAI lies in its commitment to **contribution-aware federated learning**. This principle is operationalized through peer validation mechanisms embedded within the sMPC pipeline. Rather than relying on static participation metrics, FLAI continuously evaluates and rewards nodes based on their verifiable impact on model performance. This ensures that remuneration is commensurate with actual contributions, governance power is earned rather than bought, and non-contributing or malicious actors are disincentivized through transparent, protocol-level accountability. By integrating model governance, training, and monetization into a cohesive trustless framework, FLAI fosters a sustainable, meritocratic ecosystem for privacy-preserving artificial intelligence.

2 Web3-Native Architecture

At the heart of the FLAI Protocol lies a fully decentralized system of governance and ownership, grounded in the principles of Web3. This architecture is implemented through a hierarchical structure of DAOs, SubDAOs, and specialized token primitives. Such a configuration enables scalable governance across varied data domains, while ensuring alignment between community incentives and protocol integrity.

2.1 The FLAI-SuperDAO: Protocol-Level Governance

The apex of the FLAI governance structure is the **FLAI-SuperDAO**, which serves as the primary steward of protocol-wide coordination. It is tasked with managing critical operations such as protocol upgrades—including the evolution of aggregation algorithms and secure multi-party computation (sMPC) circuits—and the calibration of token emission schedules and incentive mechanisms. Additionally, the SuperDAO oversees the global model registry and administers the Request-for-Model (RFM) system, a marketplace for soliciting and funding new model proposals. It also allocates funding for research, development, and the bootstrapping of emerging SubDAOs.

Membership in the SuperDAO is accessible to stakeholders holding staked platform tokens, along with early contributors who possess legacy credentials that reflect historical engagement with the protocol.

2.2 SubDAOs: Federated, Model-Centric Entities

Every model developed within the FLAI ecosystem is governed by a dedicated **SubDAO**, instantiated upon the approval and funding of an RFM proposal. These SubDAOs operate autonomously, exercising authority over key aspects of the model's lifecycle. This includes the specification of model configurations—such as hyperparameters, data schemas, and privacy budgets—as well as determining eligibility criteria for participants, including validator selection and dataset standardization. SubDAOs are also responsible for managing inference-related economics, such as setting per-inference pricing and royalty distribution policies.

2.3 Token Primitives: SBGTs and SubDAO Tokens

The FLAI Protocol defines a dual-token structure to facilitate both governance and economic alignment within SubDAOs.

Soul-Bound Governance Tokens (SBGTs)

SBGTs are non-transferable tokens that denote verified contributions to the lifecycle of a model—ranging from data provisioning and model training to validation. They are earned through peer-validated mechanisms and grant the holder rights to participate in governance decisions. These decisions may involve selecting appropriate data ontologies (such as OMOP or HL7 FHIR), initiating new training cycles, or modifying model architectures and optimization strategies. SBGTs may be revoked in instances of inactivity, contributor exit, or detected malicious behavior, thereby maintaining a high-integrity governance cohort.

SubDAO Tokens

In contrast, SubDAO Tokens are liquid and tradable, representing fractional ownership of a model's projected economic output. These tokens may be freely exchanged or staked in vaults native to the FLAI Protocol. Holders accrue shares of inference revenue and marketplace royalties, and participate in financially oriented decisions including treasury allocations, licensing terms, and broader ecosystem strategy. Token issuance typically occurs during RFM-based crowdfunding campaigns or is distributed as reward emissions to early contributors and validators.

2.4 Model-First Governance Philosophy

FLAI's governance paradigm is explicitly model-centric. Unlike generalized protocol DAOs that govern multiple systems or products, each SubDAO within FLAI is tailored to a single machine learning model. This ensures that governance remains domain-relevant and contextually specific—whether for a healthcare model predicting diabetes risk or a financial model forecasting asset prices. By constraining scope, FLAI ensures agile, informed decision-making, while also reducing susceptibility to governance capture. SubDAOs are indexed and discoverable through a protocol-wide registry, categorized by application domain, data format, and operational context.

2.5 Smart Contract Execution Layer

The procedural and economic logic of both SubDAOs and the SuperDAO is codified and enforced via smart contracts deployed on a public blockchain. These contracts oversee operations such as token minting, staking, and vote execution, while also finalizing outcomes of governance processes. Moreover, the smart contract layer serves as an immutable ledger for inference metrics, contributor performance scores, and payment histories. Integration with the off-chain sMPC layer ensures that all on-chain records correspond to verified and privacy-preserving computation, thereby maintaining the integrity and auditability of the system.

3 FLAI Pipeline Overview

The FLAI Protocol orchestrates a fully decentralized lifecycle for machine learning models, encompassing training, validation, deployment, and monetization. This process is collaboratively executed across untrusted participants, leveraging **secure multi-party computation (sMPC)** for privacy preservation, and coordinated through SubDAO-mediated on-chain governance. Each iteration of the FLAI pipeline proceeds through a well-defined sequence of stages, ensuring the integrity and accountability of all contributions.

3.1 Local Training (Off-Chain)

The pipeline begins with localized model training performed by data custodians, such as hospitals, enterprises, or research consortia. Each custodian operates on its private dataset $\mathcal{D}_k = \{(x_i, y_i)\}_{i=1}^{n_k}$, generating gradients or weight updates $w_k^{(t)}$ during training. These updates are then encoded via secret sharing protocols and transmitted to the sMPC aggregation layer. Crucially, the use of secret-sharing ensures that no party, whether internal or external, can reconstruct either the update or the underlying raw data from any individual share.

3.2 Peer Validation via Contribution-Aware Federated Learning

Prior to aggregation, each submitted update undergoes a rigorous evaluation process to quantify its actual utility. This *peer validation* step is performed inside the sMPC runtime, using a contribution-aware framework that may include Shapley value approximations based on holdout data, gradient divergence analysis to reward complementary contributions, and delta-based performance comparisons against reference models.

The result of this validation is a scalar *contribution score* $\phi_k \in [0, 1]$ assigned to each participant. These scores play a dual role: they determine both the governance weight within the relevant SubDAO and the magnitude of token-based rewards for the epoch.

3.3 Secure Aggregation (sMPC)

Following validation, the sMPC layer executes a weighted aggregation of the local updates. This is achieved through additive or replicated secret-sharing schemes [3], ensuring that aggregation occurs without revealing any intermediate computations. Let $S = \sum_k \phi_k$ denote the sum of contribution scores. The global model is then updated as:

$$w^{(t+1)} = \sum_k \frac{\phi_k}{S} \cdot w_k^{(t)}. \tag{1}$$

The resultant model remains confined within the sMPC environment, never being materialized or exported in plaintext—thereby safeguarding its proprietary value and minimizing attack surfaces.

3.4 SubDAO Governance and Update Approval

Upon completion of aggregation, SubDAO members—represented by holders of Soul-Bound Governance Tokens (SBGTs)—conduct an on-chain vote to determine whether the new model version should be accepted. Approval criteria may include surpassing performance thresholds on validation datasets, achieving consensus through peer-review processes, and satisfying interpretability or fairness audits.

Votes are cast and finalized through smart contracts, with successful approvals triggering the commencement of a new inference epoch. In the case of rejection, the pipeline returns to retraining, optionally with revised configurations or participant rosters.

3.5 Privacy-Preserving Pay-per-Inference Serving

Approved models are exposed via the **FLAI Inference API**, allowing external users to submit encrypted inputs x_{inf} and receive encrypted outputs $\hat{y}$. This inference process is conducted entirely within the sMPC runtime, preserving confidentiality of both inputs and model parameters. The inference output is defined as:

$$\hat{y} = \text{sMPC-Inference}(x_{\text{inf}}, w^*), \tag{2}$$

where w^* denotes the latest approved model. Every query is monetized through a predefined per-inference fee, governed by the SubDAO and enforced via smart contract.

3.6 Revenue Distribution and Incentive Mechanisms

The inference revenue accumulated during each epoch, denoted R_{cycle}, is distributed across three primary stakeholder groups. First, SBGT holders receive compensation proportional to their validated contribution scores ϕ_k. Second, a portion of the revenue is allocated to holders of tradable SubDAO tokens, based on their token stakes. Finally, a residual fund is directed to the SubDAO treasury, earmarked for reinvestment into model development or future contributor incentives.

The reward r_k allocated to participant k is computed as:

$$r_k = \frac{\phi_k}{\sum_j \phi_j} \cdot R_{\text{cycle}}. \tag{3}$$

This automated and transparent distribution mechanism ensures that economic value flows in alignment with verifiable contributions.

3.7 Lifecycle Continuation and Dynamic Governance

Each inference epoch concludes with a governance checkpoint. Contribution scores may be decayed or reweighted based on sustained engagement or strategic recalibration. New applicants may be admitted to the SubDAO, contingent on meeting domain-specific eligibility criteria. Additionally, SubDAO members may vote on protocol actions such as model fine-tuning, retraining on updated data distributions, or the formal retirement of obsolete models.

This cyclical design fosters continuous innovation while upholding the principles of privacy, decentralization, and meritocratic governance.

4 Federated Learning and Analytics

The FLAI Protocol facilitates two complementary paradigms for decentralized data collaboration: **Federated Learning (FL)** and **Federated Analytics (FA)**. Both approaches operate under strict privacy constraints, enabled through secure multi-party computation (sMPC) and governed by SubDAOs, but they diverge in their computational objectives, operational flows, and monetization strategies.

4.1 Federated Learning (FL)

Federated Learning within the FLAI framework allows multiple data custodians to collaboratively train machine learning models without transferring or exposing their raw datasets. Each participant independently trains on local data and generates model updates, which are subsequently aggregated using sMPC protocols to ensure privacy preservation throughout the learning process.

This paradigm is particularly applicable in domains where centralized data pooling is legally or ethically infeasible. Use cases include predictive modeling for disease risk using electronic health records (EHRs), real-time detection of financial fraud across disparate banking systems, and the training of natural language processing models on institutional text corpora.

The revenue model for FL is structured around a *pay-per-inference* mechanism. External users access the trained models through the FLAI Inference API, submitting encrypted queries and receiving encrypted responses. SubDAOs autonomously determine pricing per inference—such as $0.25 per prediction—and smart contracts ensure that revenue is distributed to contributors and token stakers according to validated contribution scores and staking positions.

4.2 Federated Analytics (FA)

Federated Analytics extends the protocol's capabilities to include the computation of global statistical metrics across distributed data silos, again without any raw data leakage. This mode enables the calculation of population-level insights such as the mean and variance of clinical biomarkers across hospitals, demographic profiling in rare disease cohorts, or longitudinal trend analysis in Internet of Things (IoT) deployments.

All analytical operations are conducted within the privacy-preserving confines of the sMPC environment. For instance, given K participating sites, each with a dataset of size n_k, FLAI securely computes:

$$\mu = \frac{\sum_{k=1}^{K} \sum_{i=1}^{n_k} x_i^{(k)}}{\sum_{k=1}^{K} n_k}, \quad \sigma^2 = \frac{\sum_{k=1}^{K} \sum_{i=1}^{n_k} (x_i^{(k)} - \mu)^2}{\sum_{k=1}^{K} n_k - 1}. \tag{4}$$

Beyond basic statistical operations, the protocol supports more sophisticated computations such as correlation matrices, differential cohort analyses, and stratified population summaries, all governed by custom SubDAO-registered circuits.

The FA revenue model follows a *pay-per-query* structure, in which clients—including regulators, insurers, and academic institutions—pay for one-time reports or recurring analytics streams. The resulting payments are algorithmically divided among contributing data nodes and circuit validators, with SubDAOs retaining authority over query frequency, data access permissions, and audit compliance protocols.

4.3 Unified Execution and Governance Framework

Despite their operational differences, Federated Learning and Federated Analytics are unified within FLAI through a shared technological and governance substrate. Both modes rely on the same sMPC backend, ensuring cryptographic guarantees of privacy and verifiability. Governance and configuration decisions are made through SubDAOs, leveraging a common token economy: Soul-Bound Governance Tokens (SBGTs) represent active contributions and confer voting rights, while tradable SubDAO tokens capture economic claims on revenue streams.

Furthermore, FL and FA coexist within a shared model and analytics marketplace, enabling end users to seamlessly access both predictive models and analytical reports through a single protocol layer. This unification empowers FLAI to support a diverse array of privacy-preserving AI and data science applications, all within a decentralized, economically aligned, and trust-minimized infrastructure.

5 Secure Multi-Party Computation (sMPC) Layer

The cryptographic foundation of the FLAI Protocol is built upon **Secure Multi-Party Computation (sMPC)**, a class of techniques that enable multiple, potentially adversarial parties to jointly compute a function over their private inputs without revealing those inputs to one another. In FLAI, sMPC forms the computational backbone for every stage of the machine learning lifecycle—including training, validation, aggregation, analytics, and inference—ensuring that neither raw data nor intermediate values are ever exposed.

5.1 Rationale for sMPC Adoption

FLAI's preference for sMPC over alternative privacy-preserving technologies is grounded in four core advantages. First, sMPC eliminates the need for hardware-based trust assumptions; unlike Trusted Execution Environments (TEEs), it does not depend on proprietary chips or secure enclaves that may be vulnerable to side-channel attacks. Second, it offers native decentralization: no centralized coordinator is required, as all parties contribute partial computations and jointly reconstruct outputs. Third, sMPC is inherently compatible with the Web3 ecosystem, enabling integration with on-chain governance, tokenized incentives, and event-logging systems. Finally, it provides fine-grained policy control, empowering SubDAOs to define precisely which functions are computed, under what conditions, and on what data types.

5.2 sMPC for Federated Training

During each training cycle, participating clients locally compute updates to a shared model. These updates, denoted w_k for client k, are secret-shared using additive or Shamir-based schemes [2]. The model update is partitioned into n cryptographic shares:

$$w_k \to \{w_k^{(1)}, w_k^{(2)}, \ldots, w_k^{(n)}\}, \quad \text{such that } \sum_{j=1}^{n} w_k^{(j)} = w_k \tag{5}$$

Each share is distributed to a different node within the sMPC network. These nodes collaboratively compute the peer-weighted aggregate update using contribution scores ϕ_k, resulting in a global model w^*:

$$w^* = \sum_{k=1}^{K} \frac{\phi_k}{\sum_j \phi_j} \cdot w_k \tag{6}$$

The model w^* exists solely within the sMPC runtime and is never reconstructed in plaintext, preserving the confidentiality of all intermediate representations.

5.3 sMPC for Peer Validation

FLAI's commitment to contribution-aware learning is operationalized through a peer validation mechanism that also runs within the sMPC layer. Validators, who possess private holdout datasets $\mathcal{D}_{\text{val}}$, evaluate each participant's update w_k without revealing data or models to one another. The sMPC circuit computes a contribution score:

$$\phi_k = \text{Validate}_{\text{sMPC}}(w_k, \mathcal{D}_{\text{val}}) \tag{7}$$

This enables secure, fair, and interpretable assignment of influence to each participant, while maintaining the privacy guarantees of the system. Additional validation tasks, such as score normalization and consensus weighting, are also performed within this secure environment.

5.4 sMPC for Inference

A defining feature of the FLAI Protocol is its ability to deliver encrypted, privacy-preserving inference. Upon SubDAO approval, models are registered in the FLAI Inference API, where users can submit encrypted queries x_{query} under a public key. The sMPC circuit then evaluates:

$$\hat{y} = f(w^*, x_{\text{query}}) \tag{8}$$

where f is the model function and w^* is the approved model residing entirely within the sMPC runtime. The output $\hat{y}$ is returned in encrypted form to the user, ensuring that neither the input, the model, nor the output is ever exposed. This mechanism underpins FLAI's pay-per-inference monetization strategy while simultaneously safeguarding model intellectual property and user data confidentiality.

5.5 Protocol-Level Guarantees

The use of sMPC within FLAI confers a robust set of cryptographic guarantees. Foremost among these is **privacy**, which ensures that no party learns another's data or model parameters. The protocol also guarantees **correctness**, as the computed outputs are mathematically bound to the specified function over the provided inputs. **Verifiability** is achieved via cryptographic proofs or commitments that attest to compliance with agreed-upon procedures and can be logged on-chain. Finally, the system offers **resilience** against network churn or adversarial behavior, tolerating faults in up to $t < n/2$ parties, contingent on the specific secret-sharing scheme employed.

5.6 Implementation Architecture

The FLAI sMPC layer is built atop a modular cryptographic stack, integrating both circuit-based and instruction-based computation paradigms. The implementation supports additive and replicated secret sharing, fixed-point arithmetic optimized for machine learning workloads, and extensible domain-specific languages (DSLs) for secure protocol definition. The runtime leverages performance-optimized environments including Rust and WebAssembly, ensuring low-latency execution and cross-platform compatibility.

All circuits and computation protocols are transparently open-sourced, with deployment governed by SubDAO votes and anchored via smart contract registries. This design ensures both auditability and democratic control over privacy-preserving computation at scale.

6 Governance and Tokenomics

The governance and incentive architecture of the FLAI Protocol is designed to anchor both decision-making authority and economic rewards to verified **contributions**, rather than mere capital investment. Central to this architecture are two distinct token primitives: **Soul-Bound Governance Tokens (SBGTs)** and **SubDAO Tokens (SDTs)**. Together, they facilitate a dual-layered system of participatory governance and decentralized value accrual.

6.1 Soul-Bound Governance Tokens (SBGTs)

SBGTs represent non-transferable credentials issued to individuals who actively contribute to a model's lifecycle. Contributions qualifying for issuance include the provisioning of curated data in approved ontologies, participation in local model training with subsequent submission of updates, and engagement in peer validation or community model review.

These tokens possess several critical properties. First, they are non-transferable and cannot be sold or exchanged on secondary markets, ensuring that governance power is tied to genuine, verifiable engagement. Second, they are dynamic and revocable: contribution scores ϕ_k are recalculated at the end of each training cycle, with point balances updated or decayed based on recent participation. Third, SBGTs confer governance rights in model-specific SubDAOs, where holders vote on technical and ethical issues, including modifications to model architecture, adjustments to hyperparameters, contributor eligibility, and inference pricing policies.

The voting weight v_k of a participant is proportional to their point score π_k:

$$v_k = \frac{\pi_k}{\sum_j \pi_j}, \tag{9}$$

where π_k is derived from ϕ_k and decays over time for inactive contributors.

6.2 SubDAO Tokens (SDTs)

In parallel, SDTs constitute the tradable economic tokens associated with individual models, each governed by its own SubDAO. These tokens are liquid, fungible assets that confer rights over financial policy decisions and entitlements to future revenue streams. SDTs may be listed on decentralized exchanges (DEXs), staked in liquidity pools, or held for passive income from model usage.

Holders of SDTs are entitled to a share of income generated from pay-per-inference or pay-per-query operations, proportional to their token holdings. Additionally, SDTs carry economic governance rights, allowing holders to influence fee structures, token emission policies, treasury expenditures, and marketplace interactions.

The emission of SDTs is governed by the respective SubDAO. A predetermined fraction of the total token supply is allocated to contributors—via SBGT-to-SDT conversion mechanisms—as well as to early sponsors of approved Requests-for-Model (RFMs) and to the SubDAO treasury for future upgrades. Token issuance parameters are subject to SubDAO votes, providing flexibility and adaptability over time.

6.3 Reward Mechanics and Revenue Sharing

Revenue generated during each operational cycle, denoted R_{cycle}, is distributed across three stakeholder classes: SBGT holders, SDT holders, and the SubDAO treasury.

For SBGT holders, earnings are allocated based on validated contribution scores:

$$r_k^{\text{SBGT}} = \frac{\phi_k}{\sum_j \phi_j} \cdot R_{\text{SBGT}}. \tag{10}$$

For SDT holders, rewards are distributed according to token holdings:

$$r_i^{\text{SDT}} = \frac{T_i}{\sum_j T_j} \cdot R_{\text{SDT}}, \tag{11}$$

where T_i denotes the SDT balance of stakeholder i. The remaining portion, R_{treasury}, is retained by the SubDAO for strategic use, including bounty programs, contributor onboarding, or protocol upgrades.

To further align incentives, SDT holders may stake their tokens in protocol-native vaults. This not only enhances their share of future revenue but also unlocks governance privileges such as early access to newly trained models, permission to propose model forks, and eligibility to sponsor RFMs.

6.4 Lifecycle Management and Rebalancing

The governance system incorporates dynamic lifecycle mechanisms to ensure sustainability and discourage token hoarding or passive governance. SBGTs are recalibrated at the end of each federated learning cycle. Inactive participants incur a decay in voting power, formalized as:

$$\pi_k^{(t+1)} = \lambda \cdot \pi_k^{(t)}, \quad \text{with } \lambda \in (0,1), \tag{12}$$

where λ represents the decay coefficient. Similarly, SDT reward entitlements are periodically rebalanced based on updated participation levels and staking ratios, preserving a fair and competitive ecosystem.

6.5 Governance Flow: From Proposal to Execution

All governance activities adhere to a standardized procedural flow. Any holder of SBGTs or SDTs who meets a predefined quorum threshold is permitted to submit a governance proposal. These proposals are then subject to on-chain voting during a fixed window. Votes are tallied based on token balances, with separate calculations for SBGT-weighted and SDT-weighted decisions. Upon meeting quorum and approval thresholds, smart contracts execute the resolution autonomously.

FLAI's **dual-layered governance model** explicitly distinguishes between technical and financial oversight. SBGT holders govern decisions related to data stewardship, model architecture, and ethical compliance, while SDT holders control policies around monetization, licensing, and capital allocation. This separation of powers preserves long-term model integrity while enabling responsive financial innovation.

7 Model Marketplace and Monetization

At the heart of the FLAI Protocol's economic layer lies a decentralized **model marketplace**—a permissionless, privacy-preserving registry through which trained models and analytical circuits are made available as on-demand services. Each listing is governed by its corresponding SubDAO and monetized through transparent smart contract infrastructure, all while maintaining strict confidentiality guarantees through secure multi-party computation (sMPC).

7.1 Model Listing and Discovery

Upon approval via SubDAO governance, a model is cryptographically sealed within the sMPC runtime and registered on-chain through a dedicated smart contract interface. The model is then indexed according to descriptive metadata, including its functional domain, model class (e.g., classifier, forecaster, regressor), validation metrics, and licensing terms.

Discovery mechanisms are designed to support a wide range of users—from researchers to decentralized science (DeSci) collectives and enterprise agents. Listings are accessible via the FLAI Explorer DApp, which serves as the graphical frontend to the on-chain model registry. Additionally, models can be queried through smart contract interfaces, enabling integration with third-party protocols, or accessed via oracle-compatible feeds for cross-chain referencing.

Each listing includes links to the associated SubDAO token, current pricing terms, contributor audit logs, and a standardized interface for privacy-preserving inference.

7.2 Encrypted Model Access: Pay-Per-Inference

In Federated Learning (FL) mode, models are accessible through encrypted APIs that accept confidential input data from users. Encrypted inputs x_{query} are evaluated against the sealed model w^* within the sMPC environment, producing encrypted outputs $\hat{y}$:

$$\hat{y} = \text{sMPC\_Inference}(w^*, x_{\text{query}}),$$

ensuring that neither model parameters nor input/output data are ever exposed in plaintext.

SubDAOs define the pricing schedule for inference services, which may include flat fees (e.g., \$0.25 per query), discounted subscription tiers for high-volume usage, or custom pricing constraints specified during the Request-for-Model (RFM) phase. Revenue generated from inference is algorithmically distributed among stakeholders: SBGT holders receive payments based on validated contribution scores, SDT holders receive shares proportional to their stake, and a fixed percentage (e.g., 10–15%) is reserved for the SubDAO treasury to fund future model upgrades and contributor bounties.

7.3 Federated Analytics: Pay-Per-Query Access

In Federated Analytics (FA) mode, models return population-level insights rather than individual predictions. These outputs may take the form of statistical reports, cohort-level visualizations, or anonymized trends. Queries can include one-time requests or continuous streams, enabling diverse applications from academic research to public health surveillance.

Each FA SubDAO is responsible for defining acceptable query schemas, data access constraints, report granularity, and pricing structures. Usage restrictions—such as limiting access to credentialed researchers or institutions—can also be enforced at the governance level. Consumers interact with these models through streaming dashboards, scheduled reports, or synthetic data pipelines, all orchestrated under strong cryptographic protections.

7.4 SubDAO Tokens: Liquidity, Governance, and Valuation

Each model is economically represented by a unique **SubDAO Token (SDT)**, which serves as both a governance asset and a financial instrument. These tokens are tradable on decentralized exchanges and can be staked in yield-generating vaults, enabling passive revenue accrual from model usage.

High-performing models—those with robust governance, validated outcomes, and trusted data sources—are expected to attract higher token demand, increased liquidity, and greater adoption across downstream Web3 ecosystems such as decentralized science (DeSci), regenerative finance (ReFi), and autonomous agent networks. In this context, SDTs function not only as participation rights but also as a proxy for market-based valuation of machine learning assets.

7.5 Lifecycle Operations: Forking, Retirement, and Upgrades

To accommodate model evolution, FLAI supports a full lifecycle management suite. SubDAO members may vote to **fork** a model, creating a new SubDAO with a modified governance or tokenomic structure while preserving architectural lineage. Poorly performing or deprecated models can be **retired**, ceasing monetization and optionally redirecting residual funds toward archival support. Routine **upgrades** to model parameters, architectures, or operational standards may be proposed and enacted through the SubDAO voting process.

These lifecycle features ensure that models remain aligned with emerging standards, user needs, and ethical norms, while also empowering contributors to adapt to shifting market and scientific landscapes.

7.6 Design Goals of the Marketplace

The FLAI marketplace is designed to uphold the following principles:

- **Openness**: All models are publicly discoverable and accessible without gatekeeping.
- **Permissionlessness**: Any user may query, integrate, or stake in the marketplace without requiring institutional affiliation.
- **Composability**: Model outputs are interoperable with DAOs, dashboards, or smart contracts, enabling modular integration into diverse pipelines.

- **Fairness**: Contributors are compensated proportionally to their validated impact, with scoring and distribution governed transparently via sMPC and SubDAO logic.

This architecture creates a trustless and economically sustainable environment for deploying, governing, and monetizing privacy-preserving AI.

8 Request-for-Model (RFM) Process

The **Request-for-Model (RFM)** mechanism constitutes the primary gateway for initiating new models within the FLAI Protocol. It provides a structured and permissionless framework for specifying machine learning or analytics objectives, mobilizing contributor communities, and catalyzing the formation of model-specific SubDAOs. By aligning token issuance with verifiable demand and incentivizing decentralized participation, the RFM process bridges model intent with collective execution.

8.1 Proposal Submission and Specification

An RFM begins as a formal proposal submitted by any actor—individuals, DAOs, enterprises, or research institutions. Each submission defines the desired model or analytics pipeline with precision. The RFM includes:

- A clearly articulated objective, such as predicting treatment response, generating synthetic patient cohorts, or detecting macroeconomic trends across chains.
- Model constraints, including architectural preferences (e.g., classification, regression, neural networks) or interpretability requirements.
- Data format and schema compatibility, with references to standards such as HL7 FHIR, OMOP, GA4GH, or financial time-series protocols.
- Performance metrics for validation (e.g., AUC, precision, recall, fairness thresholds).
- Governance parameters including minimum validator set sizes, epoch durations, and quorum thresholds.
- A proposed initial pricing structure for inference or analytics access.

Upon submission, RFMs are published to the on-chain FLAI registry and indexed within the decentralized model marketplace, where they become discoverable to potential contributors and validators.

8.2 SubDAO Instantiation and Crowdfunding

Once an RFM is either approved by the FLAI-SuperDAO or accumulates sufficient community support, it enters the bootstrapping phase. At this stage, a new **SubDAO** is instantiated and initialized through a series of foundational actions:

1. A crowdfunding campaign is launched to attract early stakeholders, including data custodians, validators, and backers. These stakeholders fund the initial resource pool and receive newly minted SubDAO Tokens (SDTs).

2. Preallocation of Soul-Bound Governance Tokens (SBGTs) is determined off-chain, based on verifiable contributions such as committed datasets, compute resources, or validator infrastructure. These SBGTs are minted upon model launch.

3. The SubDAO's governance logic is codified in smart contracts, which define rules for proposal submission, voting dynamics, epoch scheduling, and revenue distribution.

This process establishes the initial economic and governance infrastructure for the model's lifecycle.

8.3 Contributor Onboarding and Validation Readiness

Prospective contributors signal intent to participate in the RFM by submitting metadata that attest to dataset compatibility, confirming that local infrastructure supports sMPC protocols, and optionally staking FLAI or SubDAO tokens as collateral.

SubDAO SBGT holders, now acting as provisional stewards, vote to whitelist participants based on technical eligibility and strategic alignment. Initial validator cohorts are also elected during this phase to ensure that peer validation mechanisms can commence under secure and trustworthy conditions.

8.4 Execution of the Federated Pipeline

Following SubDAO activation and completion of the whitelisting process, model training begins. Contributors perform local training tasks and submit encrypted model updates using sMPC-compatible sharing schemes. These updates are validated and scored via the protocol's contribution-aware peer evaluation framework, before being aggregated and subjected to SubDAO governance approval.

The full federated training pipeline, as detailed in Section **??**, is enacted within this secure and auditable workflow.

8.5 Governance-Driven Model Evolution

As the model matures, its scope may evolve through SubDAO-approved amendments. This includes the ability to fork the model into domain-specific derivatives (e.g., separate SubDAOs for cancer subtypes), extend the data intake criteria to new formats or geographies, or tune governance parameters such as pricing, quorum thresholds, or epoch cadence. Each change is executed through a community-driven proposal and vote, ensuring that the model remains responsive to emerging needs and discoveries.

8.6 RFM Submitter Incentives and Privileges

To incentivize the creation of high-quality RFMs, original submitters receive preferential privileges. These may include early access to the deployed model or inference API, rebates on usage fees, or SDT airdrops proportional to early contributions. Although the RFM submitter initiates the model specification, all substantive decisions are subject to SubDAO governance, preserving collective ownership and meritocratic oversight.

8.7 RFMs as Programmable Governance Primitives

Within the FLAI Protocol, the RFM is more than a technical specification—it is a **programmable governance primitive**. Each RFM is executed as a smart contract-bound commitment to a machine learning objective, instantiated through on-chain coordination and enacted via decentralized compute. RFMs thus enable:

- **Permissionless model creation**, powered by market-driven contributor engagement.
- **Composability**, allowing seamless interaction between protocol primitives, data standards, and financial incentives.
- **Scalable coordination**, wherein globally distributed participants collectively develop, validate, and monetize privacy-preserving AI.

In doing so, RFMs operationalize a Web3-native framework for crowd-sourced machine intelligence—trustless, auditable, and economically aligned.

9 Use Case: Pharmaceutical Company and Hospital SubDAO

To concretize the FLAI Protocol's architecture, we present an end-to-end use case involving a pharmaceutical company and a federated network of hospitals. This scenario illustrates the lifecycle of a model—from the initial Request-for-Model (RFM) submission through federated training, monetization, and long-term SubDAO governance—while demonstrating the interplay between secure computation, tokenized incentives, and decentralized coordination.

9.1 Phase 1: RFM Submission by the Pharmaceutical Entity

A pharmaceutical company initiates the process by submitting an RFM to the FLAI Protocol. The objective is to develop a machine learning model capable of predicting patient response to an immunotherapy drug, utilizing electronic health record (EHR) data across global hospitals. The proposal includes the following specifications:

- **Goal**: To predict binary treatment response with a focus on interpretability.
- **Model Type**: Binary classifier with constraints on model explainability.
- **Data Schema**: Structured HL7 FHIR-compliant data, encompassing labs, diagnoses, and demographics.
- **Validation Metric**: A minimum area under the curve (AUC) of 0.85, stratified across geographic regions.
- **Suggested Pricing**: $0.50 per inference query.

Upon submission, the RFM is posted to the on-chain registry and receives quorum support from the FLAI-SuperDAO, along with endorsements from interested data custodians.

9.2 Phase 2: SubDAO Instantiation and Contributor Onboarding

Following RFM approval, a dedicated SubDAO is instantiated for the immunotherapy model. Multiple hospitals, spanning diverse geographic regions, express interest in contributing to the model's lifecycle. These prospective participants engage through:

- Uploading attestations of data compatibility and computational readiness.
- Staking FLAI or stablecoins (e.g., USDC) into the model's crowdfund pool.
- Registering validator nodes responsible for peer evaluation.

Initial SBGT allocations are issued based on pre-committed resources and validator slashing deposits. Smart contracts defining governance logic, reward distribution, and epoch dynamics are deployed to govern the SubDAO's operational lifecycle.

9.3 Phase 3: Federated Training and Contribution Scoring

Each hospital, denoted H_k, locally trains a model on its private dataset $\mathcal{D}_k$ and generates a parameter update $w_k^{(t)}$. These updates are:

- Encoded via secret-sharing and submitted to the sMPC training interface.
- Evaluated using peer validation mechanisms to compute utility scores ϕ_k.

The FLAI sMPC runtime aggregates the updates into a global model:

$$w^{(t+1)} = \sum_k \frac{\phi_k}{\sum_j \phi_j} w_k^{(t)}.$$

Contributors' governance weights π_k are subsequently adjusted according to their normalized contribution scores.

9.4 Phase 4: Governance and Model Deployment

Upon achieving performance benchmarks defined in the RFM—such as AUC thresholds and fairness criteria—the SubDAO initiates a governance vote among SBGT holders. Following approval:

- The finalized model is sealed within the sMPC inference runtime.
- Revenue logic, pricing structures, and royalty allocations are activated via smart contracts.
- The model is listed in the public FLAI marketplace for permissionless access.

9.5 Phase 5: Encrypted Inference and Revenue Sharing

External users, including researchers, payers, and policy analysts, interact with the deployed model by submitting encrypted inputs via the FLAI Inference API. Each query:

- Triggers a fee of \$0.50, payable in tokens or stablecoins.
- Is processed securely in the sMPC runtime, without exposing the model or user data.

- Returns an encrypted prediction $\hat{y}$ to the requester.

Revenue generated from each query is programmatically distributed as follows:

$$r_k = \frac{\phi_k}{\sum_j \phi_j} \cdot R_{\text{SBGT}}, \quad r_i = \frac{T_i}{\sum_j T_j} \cdot R_{\text{SDT}},$$

where r_k rewards SBGT holders based on contribution, and r_i compensates SDT holders according to their stake.

9.6 Phase 6: Lifecycle Evolution and Governance Adaptability

As the model matures, the SubDAO retains authority to adapt its direction through governance votes. These actions may include:

- **Forking**: Launching derivative SubDAOs to model specific cancer subtypes.
- **Extension**: Incorporating new modalities such as genomic sequences or medical imaging.
- **Upgrades**: Adjusting pricing tiers, inference rate limits, or retraining intervals.

New contributors can be onboarded by submitting validation datasets or running fairness audits across demographic subgroups, earning SBGTs in proportion to their contributions.

9.7 Impact and Implications

This use case illustrates the core tenets of the FLAI Protocol in action:

- **Privacy-preserving collaboration**: Data remains siloed while utility is maximized through sMPC.
- **On-demand monetization**: Models are queried without being exposed, enabling IP protection.
- **Contributor-centric governance**: Power accrues to those who drive utility, not those who merely hold capital.
- **Web3-aligned infrastructure**: Coordination, computation, and compensation are fully decentralized, transparent, and programmable.

Through this framework, the FLAI Protocol operationalizes a scalable, privacy-preserving, and economically sustainable model for decentralized machine learning in high-stakes industries such as healthcare and pharmaceuticals.

10 Conclusion

The **FLAI Protocol** (Federated Learning & Analytics Infrastructure) marks a foundational advancement in the design and deployment of decentralized, privacy-preserving artificial intelligence systems. By unifying federated learning and analytics with secure multi-party computation (sMPC) and Web3-native governance, FLAI redefines how machine learning models are trained, governed, and monetized across organizational and jurisdictional boundaries.

At its core, FLAI integrates three complementary technologies:

- **Federated Learning and Analytics**, which enable collaborative computation without raw data exposure, ensuring compliance with global privacy standards.

- **Secure Multi-Party Computation (sMPC)**, which provides a cryptographically secure execution environment for all stages of the ML lifecycle—training, validation, and inference—without requiring trusted third parties.

- **Web3-Native Governance**, implemented through SubDAOs, Soul-Bound Governance Tokens (SBGTs), and SubDAO Tokens (SDTs), to create an economically aligned and contributor-driven coordination layer.

Key Innovations

FLAI introduces two novel primitives that fundamentally differentiate it from centralized AI platforms and legacy federated learning solutions:

1. **Contribution-Aware Federated Learning**: Contributions are evaluated through peer validation within the sMPC layer, with reward allocations tied to provable utility rather than nominal participation. This mechanism enforces fairness, reduces the risk of free-riding, and incentivizes quality over quantity.

2. **Pay-Per-Inference Monetization**: FLAI enables perpetual monetization of machine learning models via encrypted, query-only access. The model itself is never revealed, but remains accessible through sMPC-secured endpoints—preserving intellectual property while supporting continuous, privacy-respecting usage.

Protocol Composability and System Interoperability

FLAI is designed not as a standalone application but as a modular protocol layer for decentralized AI systems. Its architecture is inherently composable and interoperable, enabling seamless integration with:

- Decentralized science collectives (DeSci), data unions, decentralized physical infrastructure networks (DePINs), and NFT-bound data ecosystems.

- Sovereign healthcare systems, actuarial engines in insurance, and regulatory-safe financial modeling platforms.

- Open-source AI agents and decentralized APIs for real-time inference and analytics.

This extensibility ensures that FLAI can serve as the cryptographic and economic backbone for a wide range of mission-critical applications across sectors.

A Vision for Decentralized AI

FLAI envisions a future in which AI is governed by distributed networks of contributors rather than centralized entities. In this future, models are conceptualized as **public goods with private rails**: their governance and monetization are decentralized, their usage is privacy-preserving, and their evolution is community-driven.

Incentivized. Private. Trustless. Scalable. These are not trade-offs; they are foundational principles embedded into every layer of the FLAI Protocol.

The protocol is live, modular, and extensible. RFMs are open for submission, and contributor networks are already forming across healthcare, finance, and research sectors. FLAI invites participation from data custodians, model developers, validators, and institutions committed to building the next generation of ethical, decentralized artificial intelligence.

11 References

References

[1] H. B. McMahan et al., "Communication-efficient learning of deep networks from decentralized data," in *Proc. 20th International Conference on Artificial Intelligence and Statistics (AISTATS)*, 2017.

[2] A. Shamir, "How to share a secret," in *Communications of the ACM*, vol. 22, no. 11, pp. 612–613, 1979.

[3] W. Du and M. J. Atallah, "Secure multi-party computation problems and their applications: A review and open problems," in *Proceedings of the 2001 Workshop on New Security Paradigms (NSPW)*, 2001.

[4] B. Ghorbani and J. Zou, "Data Shapley: Equitable valuation of data for machine learning," in *International Conference on Machine Learning (ICML)*, 2019.

[5] Y. Wang et al., "Principled evaluation of differential contributions in federated learning," in *IEEE Transactions on Big Data*, 2020.

[6] S. Jiang et al., "Contribution-Aware Federated Learning (CAFL): Accurate and robust model training," in *AAAI Conference on Artificial Intelligence*, 2023.

[7] M. Goudge, "Understanding HIPAA: The Health Insurance Portability and Accountability Act," *Health IT Security*, 2020.

[8] P. Kairouz et al., "Advances and open problems in federated learning," in *Foundations and Trends in Machine Learning*, 2021.

[9] V. Buterin, "DAOs, DACs, DAs and more: An incomplete terminology guide," *Ethereum Blog*, 2014. [Online]. Available: `https://ethereum.org/en/blog/dao/`

[10] Z. Gluchowski, "Soulbound: Building identity with non-transferable tokens," *Vitalik Buterin, Puja Ohlhaver, E. Weyl*, 2022.

[11] P. Mohassel and Y. Zhang, "SecureML: A system for scalable privacy-preserving machine learning," in *IEEE Symposium on Security and Privacy (SP)*, 2017.

[12] G. Hardman et al., "Zero Knowledge Federated Learning: Privacy-preserving model validation in Web3 environments," in *arXiv preprint arXiv:2303.12345*, 2023.