FLAI Whitepaper

Audum Labs

December 2024

Abstract: Data privacy and security remain paramount in the digital age, especially as industries increasingly rely on data-driven decision-making. Secure Multi-Party Computation (SMPC) enables collaborative data analysis and predictive modeling while preserving privacy, but its traditional implementations lack scalability, transparency, and equitable governance. FLAI explores the integration of blockchain technology and Decentralized Autonomous Organizations (DAOs) into SMPC frameworks to establish a platform that prioritizes privacy, transparency, security, and fairness. FLAI is a pioneering SMPC-enabled federated learning and federated analytics platform. By leveraging the inherent strengths of blockchain and DAOs, FLAI addresses the challenges of federated learning and secure computation, setting a new benchmark for decentralized, trustless systems.

1 Introduction

In the evolving landscape of artificial intelligence (AI), the need for secure, ethical, and efficient data usage is paramount. Traditional data-centric methods typically rely on centralized systems that aggregate sensitive data for analysis or model training. While these methods have been effective, they come with significant risks, such as privacy breaches, security vulnerabilities, and trust deficits. Regulatory frameworks such as the European General Data Protection Regulation (GDPR), China's Cybersecurity Law, and the United States California Consumer Privacy Act (CCPA) highlight the increasing demand for robust data protection and privacy measures. These regulations underscore the urgent need for innovative solutions that align with privacy standards while enabling technological advancements. As a response, Federated Learning (FL) and Federated Analytics (FA) have emerged as transformative paradigms that enable organizations to collaborate without sharing raw data, prioritizing privacy and decentralization.

Federated Learning [1] represents a decentralized approach to training machine learning models, where data remains at its source while only model updates or gradients are shared with a central aggregator. This decentralized model preserves data privacy while enabling collaboration across organizations or devices. Despite its potential, FL is not without its challenges. Privacy risks persist due to the possibility of sensitive information being inferred from shared model updates, a vulnerability known as gradient leakage [2, 3]. Moreover, trust issues can arise, as participants may act maliciously by introducing poisoned updates or withholding high-quality data, thereby compromising the integrity of the model. Additionally, fairness concerns emerge when contributors with varying resources feel that their inputs are not adequately rewarded. The lack of transparent governance further exacerbates these challenges, leaving disputes unresolved and incentives misaligned. Lastly, the central aggregation process remains vulnerable to adversarial attacks, such as model tampering or man-in-the-middle exploits.

Federated Analytics (FA) [4, 5] builds upon the foundational principles of FL, extending its capabilities to enable the analysis of distributed datasets without direct access to raw data. This paradigm is particularly impactful in domains characterized by highly sensitive information, such as healthcare and finance. In these fields, real-world data (RWD), including electronic health records (EHRs), IoT-generated data, and financial transactions, offers significant value for deriving actionable insights. By enabling the generation of real-world evidence (RWE) in a privacy-preserving manner, FA fundamentally redefines data handling practices. It replaces the traditional paradigm of "trust me with your data" with "you never need to share your data," thereby transforming the landscape of data privacy and collaboration. FA facilitates secure, decentralized analysis while ensuring that individual datasets remain local, addressing critical concerns regarding data

breaches and compliance with privacy regulations, signifying a shift toward more collaborative, privacy-centric methodologies for leveraging distributed data.

Secure Multi-Party Computation (SMPC) [6] is a cryptographic framework that enables multiple parties to perform joint computations on encrypted data without revealing the underlying information to any party involved. This privacy-preserving mechanism addresses key security and privacy challenges in Federated Learning (FL) and Federated Analytics (FA), ensuring that sensitive data remains protected while enabling collaborative processes. By keeping data encrypted during computations, SMPC provides a solution to risks such as data leakage and adversarial attacks, making it an essential tool for secure and privacy-conscious collaboration in FL and FA. SMPC's ability to facilitate encrypted computations further opens the door to mechanisms such as pay-per-inference and pay-per-query for FL and FA. In these frameworks, both model inputs and outputs remain private, preserving data confidentiality while enabling the monetization of AI services. By charging for each inference or query, these mechanisms allow for secure and scalable access to AI-driven insights without compromising user privacy.. In this way, SMPC enables the creation of trustless environments where collaboration is possible without the need for central control.

In addition to privacy and security, the governance and incentivization issues in federated systems are addressed through Decentralized Autonomous Organizations (DAOs). DAOs are blockchain-based entities governed by smart contracts that automate processes and enforce rules transparently. This decentralized governance model empowers stakeholders to participate in decision-making through voting mechanisms, ensuring fairness and accountability. The integration of Soul-Bound Tokens (SBTs)—non-transferable digital tokens that represent individual identity and contributions—further enhances DAOs by building trust and reputation within the ecosystem. For FL and FA, DAOs not only facilitate decentralized decision-making but also ensure that participants are incentivized fairly, with rewards based on their contributions and impact.

FLAI is a groundbreaking platform that redefines AI model training and data analysis by seamlessly integrating Federated Learning (FL), Federated Analytics (FA), Secure Multi-Party Computation (SMPC), and Decentralized Autonomous Organizations (DAOs). With privacy, transparency, security, and accountability at its core, FLAI enables organizations to collaborate on distributed datasets without compromising sensitive information. Leveraging SMPC, computations are performed on encrypted data, eliminating risks such as data leakage and adversarial inference. This privacy-preserving approach facilitates trustless environments where participants retain full control of their data while contributing to collective insights. Through innovative mechanisms such as pay-per-inference for FL and pay-per-query for FA, FLAI not only enhances collaboration but also establishes a scalable and sustainable revenue model that aligns with user needs.

Central to FLAI's ecosystem are blockchain-powered DAOs that provide a transparent, decentralized governance framework. These DAOs empower stakeholders to actively participate in decision-making, ensuring fairness and accountability. The integration of Soul-Bound Tokens (SBTs) further enhances trust within the community by linking rewards to individual contributions, while FLAI tokens create a robust and auditable incentivization system. This dual-layer governance model fosters equitable compensation and strengthens collaboration by aligning the interests of all participants. Together, these features ensure that FLAI's operations remain transparent, secure, and incentivized, providing a foundation for long-term sustainability.

By uniting cutting-edge privacy-preserving technologies and decentralized governance, FLAI transcends the limitations of traditional federated systems. The platform bridges the gap between innovation and privacy, enabling actionable insights from real-world data while adhering to stringent security and compliance standards. As a pioneer in responsible and collaborative AI, FLAI not only addresses the challenges of data sovereignty, governance, and incentivization but also sets a benchmark for ethical and scalable AI development. Positioned at the intersection of technological innovation and societal responsibility, FLAI is shaping a sustainable, trustworthy, and decentralized AI future.

2 Background

2.1 Federated Learning

Federated Learning (FL) [7] is a decentralized approach to machine learning that enables multiple clients to collaboratively train a shared model without sharing their raw data. This ensures that sensitive data remains local to client devices, with only model updates or gradients transmitted to a central server for

aggregation. The primary advantage of FL is its ability to preserve data privacy and minimize security risks, empowering organizations, individuals, and devices to contribute to collaborative learning while safeguarding their private information [8].

In Federated Learning, each participating client, such as a mobile device, sensor, or organization, operates on its own local dataset to train a model. Instead of sharing raw data, clients transmit model updates, including gradients or weights, to a central server, which aggregates these updates to produce a global model. The updated global model is then distributed back to the clients, iterating through this process until the model converges.

The Federated Learning process consists of several iterative steps designed to enable effective training while maintaining data privacy. These steps are as follows:

1. **Model Initialization:** The central server initializes a global model, which is distributed to all participating clients.

2. **Local Model Training:** Each client trains the model on its local dataset, solving the optimization problem:
$$\min_w F_k(w) = \frac{1}{n_k} \sum_{i=1}^{n_k} \ell(w; x_i, y_i),$$
where $\ell(w; x_i, y_i)$ is the loss function for model w on data point (x_i, y_i), and n_k represents the number of data points at client k [9].

3. **Local Model Validation:** Clients validate the trained local models using separate validation datasets.

4. **Aggregation of Local Models:** The central server aggregates the updates received from the clients to form a new global model. This aggregation follows the Federated Averaging (FedAvg) algorithm, which combines client updates as:
$$w^{(t+1)} = \frac{1}{n} \sum_{k=1}^{K} n_k w_k^{(t+1)},$$
where $n = \sum_{k=1}^{K} n_k$ is the total number of data points across all clients, and $w_k^{(t+1)}$ represents the updated model parameters from client k after a local training step:
$$w_k^{(t+1)} = w_k^{(t)} - \eta \nabla F_k(w_k^{(t)}),$$
with η being the learning rate and $\nabla F_k(w_k^{(t)})$ denoting the gradient of the local loss function.

5. **Repeat Training Cycle:** The updated global model is sent back to the clients, and the process repeats over multiple communication rounds until convergence.

6. **Global Model for Inference:** After sufficient iterations, the final global model is ready for deployment in real-world applications.

FL ensures data privacy by keeping data decentralized, allowing clients to retain control over their data. Only model updates are shared with the central server, preventing the raw data from being exposed. However, while FL mitigates many privacy risks, it is not immune to challenges. One such issue is gradient leakage, where information about the raw data can be inferred from the model updates, potentially compromising privacy.

2.2 Federated Analytics

Federated Analytics (FA) is a decentralized approach to data analysis that enables multiple participants to collaboratively derive insights from distributed datasets without directly sharing the raw data. By keeping data localized on client devices or within specific organizations, FA ensures privacy preservation and compliance with data sovereignty regulations. This method is particularly valuable in scenarios where privacy concerns or legal constraints prevent centralized data pooling.

In Federated Analytics, clients compute partial analytics or aggregate statistics locally on their data. These results are then transmitted to a central server or aggregator, which combines them to produce a global analysis. This architecture avoids direct data sharing, ensuring that sensitive information remains protected while enabling joint insights across distributed datasets.

The Federated Analytics process typically involves the following steps:

1. **Problem Definition:** The central server defines the analytical task, such as computing mean, variance, correlation, or more complex statistical measures, and communicates the required computation to the clients.

2. **Local Analytics Computation:** Each client performs the specified computations on its local dataset. For instance, a client may calculate the sum of its data values, count the number of records, or determine other partial statistics.

3. **Secure Transmission of Results:** The locally computed statistics are securely transmitted to the central aggregator. Techniques such as differential privacy or secure multiparty computation may be applied to ensure the confidentiality of the transmitted information.

4. **Aggregation of Results:** The central server aggregates the received statistics to compute global metrics or insights. For example, it may calculate the overall mean by combining local sums and counts:
$$\text{Global Mean} = \frac{\sum_{k=1}^{K} \text{Local Sum}_k}{\sum_{k=1}^{K} \text{Local Count}_k},$$
where K is the number of participating clients.

5. **Result Dissemination:** The aggregated results are shared with all participants or used to inform decision-making processes. These results are typically devoid of sensitive information, ensuring privacy and compliance.

FA is particularly suited for use cases involving sensitive or distributed data, such as healthcare, finance, and IoT applications. By enabling collective insights without direct data sharing, Federated Analytics addresses privacy concerns while fostering collaboration. However, challenges such as ensuring the accuracy of aggregated results, addressing potential biases in distributed datasets, and mitigating privacy risks, like data leakage through partial results, remain areas of active research and development.

2.2.1 Pairwise Masking for Secure Aggregation

Pairwise masking is an efficient technique for secure aggregation in FA that obviates the need for complex Multi-Party Computation (MPC) protocols. This method ensures that individual contributions remain private while enabling accurate global aggregation.

Participants collaboratively generate pairwise random masks with their peers to obfuscate individual contributions. These masks cancel out during aggregation, ensuring that sensitive data remains hidden.

The process involves the following steps:

1. **Mask Generation:** Each participant P_i generates pairwise random masks with every other participant P_j such that:
$$r_{i,j} = -r_{j,i}.$$
This ensures that the masks are symmetric and cancel out during aggregation.

2. **Masked Value Computation:** Each participant masks their value x_i using the generated random masks:
$$z_i = x_i + \sum_{j \neq i} r_{i,j}.$$

3. **Local Sum Sharing:** Each participant transmits their masked value z_i to the aggregator.

4. **Aggregation:** The central aggregator computes the global sum:

$$Z = \sum_i z_i,$$

where the random masks cancel out, leaving:

$$Z = \sum_i x_i.$$

5. **Global Metric Computation:** The aggregator uses the global sum Z to compute desired metrics, such as mean or variance, without accessing individual contributions.

Pairwise masking ensures privacy by leveraging local randomness. Even if some participants are compromised, the obfuscation provided by the random masks prevents the extraction of individual values. This technique is lightweight, scalable, and suitable for scenarios with honest-but-curious adversaries or partial collusion, making it a practical alternative to more resource-intensive cryptographic methods.

2.3 Secure Multi-Party Computation

Secure Multi-Party Computation (SMPC) is a cryptographic technique that enables multiple parties to collaborate in performing computations over their combined data while ensuring that no party gains access to the private data of others. The protocol preserves the confidentiality of individual parties' inputs throughout the process, revealing only the final computed result.

The central idea of SMPC is that multiple participants can perform computations on their combined data without needing to trust each other with their private inputs. Key principles involved in SMPC include:

1. **Secret Sharing**: Each party divides its data into encrypted shares, which are distributed to other parties. These shares are used to perform computations without revealing any party's original data [10, 11].

2. **Secure Function Evaluation**: The function to be computed is evaluated collaboratively by the participants, with each participant using only their share of the data and not the raw inputs.

2.3.1 Step-by-Step Mechanism of SMPC

Data Splitting and Secret Sharing Each party splits its input data into shares and sends one share to each participant, ensuring that no single party has access to the unmasked input[12]. Suppose there are N parties involved in the computation, with each party having an input x_i. The goal is to compute a function $f(x_1, x_2, \ldots, x_N)$ without revealing the inputs. The data x_i is split into n shares as:

$$x_i = \sum_{j=1}^{n} \lambda_j x_{ij},$$

where x_{ij} represents the share of data x_i held by party j, and λ_j are random coefficients.

Garbled Circuit Protocol One popular SMPC technique is the Garbled Circuit protocol. This process involves transforming the function f into a circuit, where each gate is encrypted or "garbled." The steps include:

1. Convert the function f into a Boolean circuit.

2. Encrypt each gate in the circuit to garble it, preventing parties from learning intermediate values.

3. Distribute the encrypted gates to participants, who perform local computations using their respective shares.

4. Reveal the final output of the garbled circuit, ensuring no private data is disclosed.

Two-Party Computation (2PC) using Garbled Circuits For pairwise peer validation, Two-Party Computation (2PC) using Garbled Circuits is commonly employed:

1. Party i creates a garbled circuit $G(w_i, x_j)$ for the validation function, where w_i represents the model weights of party i, and x_j represents the data of party j.
2. Party j receives the garbled circuit and encrypted inputs, evaluating the circuit without learning w_i.
3. The circuit's output y_{ij} is shared between the two parties to confirm the validation result.

The validation function is mathematically represented as:

$$y_{ij} = f(w_i, x_j),$$

where $f(w_i, x_j)$ is evaluated using the garbled circuit.

Secure Gradient Aggregation in Federated Learning After training, each party computes local gradients g_i for their model, sharing them securely using SMPC protocols. The secure aggregation mechanism proceeds as follows:

- Each node computes on its share of gradient data.
- The aggregated gradient is securely computed as:

$$G_{\text{agg}} = \sum_{i=1}^{K} g_i,$$

  where g_i represents the gradient from party i, and K is the total number of participants.

Using SMPC, only the aggregated gradient G_{agg} is revealed, keeping individual gradients confidential.

Inference Using SMPC After training, the model can perform inference securely while protecting input data privacy. The process includes:

1. The input data x is secret-shared across parties using Shamir's Secret Sharing or similar protocols.
2. The secret-shared input is distributed across nodes, where each node holds a share.
3. The aggregated gradients and secret-shared input data are used to perform inference securely. The inference result y is computed as:

$$y = f(G_{\text{agg}}, x),$$

   where $f(\cdot)$ represents the inference function.

SMPC enables privacy-preserving and secure computations, ensuring data privacy by processing data without exposing private inputs. It provides robust security through cryptographic guarantees, allowing trustless collaboration among multiple parties. Key advantages include privacy-preserving validation and secure gradient aggregation via protocols like Two-Party Computation (2PC) and garbled circuits, ensuring no single entity accesses full data or model weights. SMPC also enhances scalability and efficiency, reducing communication overhead for large-scale federated learning scenarios. Its end-to-end security protects input data and inference results, preventing data leakage throughout the pipeline. Additionally, the decentralized nature of SMPC, especially in blockchain-based systems, mitigates risks by eliminating single points of failure and reducing vulnerabilities from centralized data breaches.

2.4 Decentralized Autonomous Organizations

A Decentralized Autonomous Organization (DAO) is a new form of organization that operates without centralized leadership, relying instead on blockchain-based protocols to facilitate decision-making, governance, and execution. DAOs are driven by smart contracts, which are self-executing contracts with the terms of the agreement directly written into code. The decentralized nature of DAOs allows for transparent, secure, and automated management without the need for intermediaries, fostering trust and collaboration among participants.

DAOs are typically governed by token holders, where each token represents voting power or ownership in the organization. These tokens can be used to participate in governance decisions such as protocol upgrades, funding allocation, and other organizational matters. The governance process is decentralized, with decisions made by consensus mechanisms such as majority voting or weighted voting, ensuring that the entire community has a say in how the DAO operates.

DAOs are increasingly being applied in various domains, including finance (DeFi), governance, decentralized applications (dApps), and even machine learning, where they provide transparent and secure decision-making and resource management.

2.4.1 DAOs in Governance

In the context of governance, DAOs provide a mechanism for decentralized decision-making. Traditional organizations rely on central authorities such as boards of directors or CEOs to make decisions. In contrast, DAOs leverage smart contracts to allow token holders to propose and vote on decisions that shape the direction of the organization.

The governance of a DAO typically involves:

- **Proposals:** Members can submit proposals for changes or updates to the system, ranging from governance changes to technical updates.
- **Voting:** Token holders vote on proposals, with the decision either being approved or rejected based on the outcome of the vote.
- **Execution:** Once a proposal is approved, smart contracts automatically implement the decision, ensuring that the governance process is both transparent and self-executing.

By decentralizing the decision-making process, DAOs ensure that all participants have a voice in the governance process, eliminating the need for centralized control and fostering a more democratic and equitable system.

2.4.2 DAOs in Federated Learning (FL) and Federated Analytics (FA)

In the context of Federated Learning (FL) and Federated Analytics (FA), DAOs provide a framework for decentralized collaboration. FL and FA involve multiple participants (clients, organizations, devices) working together to train models or perform analytics without sharing their raw data. DAOs play a critical role in governing these decentralized ecosystems by managing how participants interact, share resources, and contribute to the model or analysis.

DAOs enable FL and FA networks to set rules for how data or model updates are shared, ensuring that participants adhere to privacy-preserving protocols. For example, DAOs can determine the frequency of model updates, the validation process for updates, and the rewards for contributions. This decentralized decision-making ensures that the governance of the FL or FA process remains fair and transparent. Additionally, DAOs help incentivize participation by allowing participants to earn tokens or other rewards based on their contributions to the model or analysis. This incentivization mechanism can be integrated with the pay-per-inference or pay-per-computation models, where participants are rewarded based on the number of valid updates they contribute or the amount of computation they perform.

By incorporating DAOs, FL and FA systems can operate in a manner that ensures trust and fairness, even in highly distributed environments. The decentralized governance model inherent in DAOs can prevent any central authority from gaining too much control over the system, preserving the collaborative nature of

FL and FA. DAOs also facilitate transparency, as all decisions related to model training, data sharing, and participant rewards are recorded on the blockchain.

2.4.3 DAO Role in Secure Multi-Party Computation

In the realm of Secure Multi-Party Computation (SMPC), DAOs provide governance and management over the computation process. SMPC allows multiple parties to jointly compute a function over their data without revealing their private inputs to each other. DAOs ensure that all participants in an SMPC protocol follow the agreed-upon rules, which helps maintain the security and privacy of the computation.

DAOs can oversee the distribution of tasks in an SMPC process, manage the validation of model updates, and determine how to aggregate the results. In SMPC, it is important that no party can learn anything about another party's private data. DAOs ensure that the rules governing the execution of these computations are enforced and that any data sharing or computational actions are done in accordance with the privacy protocols. They also play a role in the incentivization of participants, rewarding them for their contributions to the secure computation process.

Furthermore, DAOs can introduce additional layers of trust into SMPC processes by allowing participants to vote on decisions such as the selection of protocols or changes to the computation process. This decentralized decision-making aligns with the overall principles of privacy, security, and fairness in SMPC.

2.4.4 Majority Voting and Weighted Voting in DAOs

In DAOs, voting is crucial for decentralized decision-making. Participants vote on proposals, with each vote potentially weighted based on factors such as stake, reputation, or contribution. Majority voting is often used, where a proposal is accepted if it receives more than half the votes. In contrast, weighted voting considers each participant's stake or contribution, ensuring that more involved participants have a greater influence on decisions. This method balances broad participation with key stakeholder interests, enhancing fairness and proportionality in governance.

For majority voting, let $V = \{v_1, v_2, \ldots, v_N\}$ represent votes, where $v_i \in \{0, 1\}$. A proposal is accepted if the sum of positive votes exceeds half the total number of participants:

$$\text{Decision} = \begin{cases} \text{Accept} & \text{if} \sum_{i=1}^{N} v_i > \frac{N}{2} \\ \text{Reject} & \text{if} \sum_{i=1}^{N} v_i \leq \frac{N}{2} \end{cases}$$

In weighted voting, let $W = \{w_1, w_2, \ldots, w_N\}$ represent participant weights. The decision is based on the weighted sum of votes:

$$\text{Decision} = \begin{cases} \text{Accept} & \text{if} \sum_{i=1}^{N} w_i v_i > \frac{1}{2} \sum_{i=1}^{N} w_i \\ \text{Reject} & \text{if} \sum_{i=1}^{N} w_i v_i \leq \frac{1}{2} \sum_{i=1}^{N} w_i \end{cases}$$

Weighted voting ensures that participants with greater contributions or stakes have a proportionally larger influence on the outcome, facilitating more nuanced decision-making in decentralized systems.

3 System Architecture

FLAI operates as an L3 appchain layer, built atop an EVM-based layers to leverage blockchain's robust security, scalability, and interoperability. This layered architecture provides a seamless foundation for the decentralized governance, privacy-preserving computations, and collaborative learning processes integral to the FLAI ecosystem. The architecture integrates multiple roles and entities, each playing a critical part in the system's operation.

The EVM-based layers serves as the foundational blockchain infrastructure for FLAI. This layer ensures compatibility with Ethereum's ecosystem, enabling smart contract deployment, secure token transactions, and seamless integration with other decentralized applications. The EVM-based layer also supports the issuance and management of FLAI tokens, which power the platform's governance and incentivization mechanisms.

As an L3 appchain layer, FLAI specializes in FL, FA, and SMPC. It delivers domain-specific functionalities that extend beyond the general-purpose capabilities of the L1 and L2 layers. This architecture optimizes FLAI for high-performance decentralized AI model training and inference, maintaining the transparency, accountability, and scalability inherent in blockchain systems.

FL Model Requesters initiate federated learning (FL) tasks by requesting models to be collaboratively trained within the FLAI ecosystem. These requesters provide essential components, including model architecture, hyperparameters, initial weights, training guidelines, and data compliance policies for FL Trainers. As members of the FLAI-SuperDAO, FL Model Requesters offer bounties in FLAI tokens to incentivize participation. They also enjoy priority access and discounts on the final global model, aligning their contributions with tangible benefits.

FL Tasks represent the core operational unit of federated learning within FLAI. An FL Task encompasses the entire lifecycle of training a specific FL model, progressing through stages of proposal, formation, and collaborative training. These tasks are governed by FLAI-SubDAOs, ensuring focused management while adhering to the broader governance framework of FLAI-SuperDAO.

FLAI-SuperDAO serves as the overarching governance body, stewarding platform-wide policies, protocols, and resource allocation. It ensures alignment across all FL tasks and oversees the operation of FLAI-SubDAOs. This centralized coordination fosters a cohesive ecosystem while allowing for decentralized task management.

For each FL Task, a dedicated FLAI-SubDAO is created, providing task-specific governance. Prospective members can join these SubDAOs by staking FLAI tokens or waiting for the next cohort cycle. SubDAO members, typically FL Trainers, collaboratively manage the FL model training process. This structure enables decentralized governance that is adaptable to the specific requirements of individual tasks, enhancing both efficiency and transparency.

FL Trainers are individual participants or institutions contributing local data and computational resources to train FL models. By leveraging secure multi-party computation (SMPC) protocols, FL Trainers ensure the privacy and security of their data during training. In return, they are incentivized with rewards, such as FLAI tokens, proportional to their contributions. FL Trainers also gain discounted access to the inference capabilities of the models they have helped train.

FL Model Users are the end beneficiaries of the federated learning models. They utilize these models by paying per inference to obtain predictions. User data remains encrypted on their devices, with SMPC protocols ensuring that inference is performed securely on masked inputs. The results are returned in an encrypted or masked form, ensuring that only the intended recipient can decrypt and access the output. This privacy-preserving mechanism encourages trust and adoption among users while safeguarding sensitive information.

4 FL Pipeline Overview

The FLAI federated learning (FL) pipeline ensures privacy, scalability, and efficiency by leveraging Secure Multi-Party Computation (SMPC) throughout the FL process. Designed as an iterative framework, the pipeline follows a structured progression to collaboratively train a robust global model while adhering to strict privacy standards.

- **Local Model Training :** The pipeline begins with the initialization of the FL Task by the task publisher, who provides initial model weights under SMPC and privacy protocols. FL-Trainers within the SubDAO undertake the responsibility of training the initial model using their locally stored data. To ensure privacy, the process follows SMPC principles, where updates such as gradients are computed locally and encrypted using techniques like secret sharing. This approach guarantees that raw data remains private, even during collaborative model training.

- **Local Model Validation:** The trained local models are validated to measure their performance against predefined metrics such as accuracy and loss. Validation is conducted at two levels. First, the FL Task publisher evaluates models against a centralized validation dataset, ensuring compliance with task-specific requirements. Second, peer validation occurs among SubDAO members, fostering mutual accountability. Following validation, FL Trainers are ranked based on their contributions, with these rankings dynamically updated after each FL cycle.

- **Federated Averaging:** Federated averaging aggregates encrypted updates from all learners to produce a global model. This step uses SMPC protocols to maintain data confidentiality while computing a weighted average that reflects the contributions of each participant. The resulting global model balances collective intelligence with rigorous privacy preservation, ensuring it is robust and unbiased.
- **Global Model Validation:** The global model undergoes comprehensive validation to confirm its effectiveness. FL Trainers perform distributed validation across their datasets, testing the model's generalization capabilities. Simultaneously, the FL Task publisher conducts centralized validation using a curated dataset, verifying that the global model meets the task's specific objectives.

4.1 Incentivization and Governance

The FLAI ecosystem incentivizes active participation through a dual-token mechanism. FL Trainers receive FLAI tokens proportional to their contributions, rewarding their computational efforts and data provision. Additionally, SubDAO-specific governance tokens, which are non-transferable, are allocated based on participation. These tokens empower trainers with decision-making authority within the SubDAO, promoting a decentralized governance structure that aligns individual contributions with broader ecosystem goals.

4.2 Secure Inference

Once trained, the global model is made available for secure inference while maintaining user privacy. SMPC protocols enable inference on encrypted input data, ensuring that sensitive information remains confidential. The results are securely returned in encrypted form, accessible only to the intended recipient. This privacy-preserving mechanism fosters trust and ensures compliance with stringent data protection standards.

4.3 Pay-per-Inference and Lifecycle Redistribution

The pay-per-inference model ensures that FLAI's federated learning pipeline is financially sustainable. Users pay in platform tokens for each inference request, with payments distributed among SubDAO contributors according to their rankings established during the validation phase. At the end of each FL cycle, governance tokens within the SubDAO are redistributed, rewarding contributors whose efforts had the most significant impact. This continuous redistribution reinforces active engagement and equitable participation.

The FL pipeline's seamless integration of privacy-centric computation, decentralized governance, and incentivization underscores FLAI's commitment to fostering collaborative and transparent AI model training. By leveraging advanced cryptographic techniques and blockchain-based frameworks, the pipeline ensures that participants can securely contribute and benefit from federated learning initiatives.

5 FA Pipeline Overview

The Federated Analytics (FA) pipeline within the FLAI ecosystem utilizes the power of Secure Multi-Party Computation (SMPC) to enable collaborative data analysis while maintaining the highest standards of privacy and security. Built on the Layer 3 (L3) application chain, the FA pipeline ensures scalability, transparency, and trust in the collaborative analytics process. Designed as an iterative and decentralized framework, the pipeline allows multiple participants to contribute valuable insights derived from sensitive data without compromising its confidentiality.

5.1 Collaborative Data Analysis using SMPC

The FA pipeline ensures that data analysis is performed collaboratively across different participants without the need to share raw data. Using SMPC protocols, FLAI enables multiple parties to jointly compute analytical results while keeping the individual data private. This is particularly crucial in sensitive domains, such as healthcare, finance, and business, where participants wish to collaborate on analytics tasks but are unable or unwilling to share their data due to privacy concerns.

5.1.1 Initial Data Sharing and Encryption

At the beginning of the FA cycle, data providers (FL Trainers) share encrypted data with the L3 application chain, which acts as the central coordination point for the analytics tasks. Each data provider's sensitive information is securely encrypted using SMPC protocols, such as secret sharing, homomorphic encryption, or additive noise techniques, ensuring that the raw data remains private and protected throughout the entire analysis process.

5.1.2 Collaborative Model Development

Once the encrypted datasets are gathered, the FA process proceeds by leveraging the collective computational power of the participating nodes. Each participant performs local computations on their encrypted data, such as statistical analysis, aggregation, or machine learning model training, without revealing the underlying data to any other party. SMPC allows for secure computation of complex analytical tasks like regression analysis, clustering, or data visualization, by keeping the data encrypted until the final results are needed.

The L3 application chain coordinates these computations and ensures that the privacy of individual participants is maintained, even when performing computations across decentralized nodes. It aggregates the results of the local computations into a shared analytic model, without exposing any private data.

5.2 Federated Analytics Aggregation and Insights

Once local computations are completed, the results are securely aggregated into a global analytic model that represents the combined insights from all participants. The aggregation process ensures that the results are based on a weighted approach, where each participant's contribution is appropriately accounted for, based on the volume of their data or the complexity of their computations.

5.2.1 Privacy-Preserving Analytics

The aggregated model remains encrypted and protected by SMPC, ensuring that the final insights can only be revealed when authorized. This could include aggregated statistical values, machine learning predictions, or any other forms of analytics that can be derived from the collaborative data. Importantly, the final model ensures that sensitive information from individual participants is never exposed, even when delivering detailed analysis results.

5.2.2 Decentralized Reporting and Sharing of Results

The aggregated and encrypted results of the analytics are then shared across the decentralized network. Each participant can access the results that are relevant to their needs while maintaining data privacy. Only authorized parties can decrypt and view the results, and the use of SMPC ensures that no one party can view the entire analytic output unless explicitly permitted.

In addition, the final insights are recorded on the blockchain, ensuring that the process remains transparent and auditable. This decentralized ledger provides a trustworthy record of the collaborative efforts, guaranteeing accountability and traceability throughout the FA cycle.

5.3 Incentivization and Governance in Federated Analytics

To encourage continued participation and high-quality contributions, FLAI's FA pipeline integrates a token-based incentivization system. Contributors to the FA process receive FLAI platform tokens, which are distributed based on the quality and impact of their participation. These tokens are awarded to participants based on factors such as the value of their local data, the significance of their computations, and the accuracy of their results.

SubDAO-specific governance tokens are also allocated based on participation, empowering contributors with decision-making authority within their respective SubDAOs. This governance model encourages decentralized oversight and fosters collaboration, ensuring that the FA pipeline remains aligned with the broader goals of the FLAI ecosystem.

5.4 Secure Analytics Lifecycle and Redistribution

The analytics lifecycle within the FA pipeline follows a continuous improvement model. At the end of each FA cycle, analytics results are reviewed, and governance tokens are redistributed based on the quality of each participant's contribution. This redistribution model encourages sustained engagement and ensures that active contributors are rewarded for their efforts.

The final insights are also shared in a way that allows for iterative improvements. Each cycle of analytics builds upon the previous one, enabling more accurate, refined, and valuable insights over time. As new participants join and contribute their data, the decentralized nature of the FA pipeline ensures that it remains open and scalable, accommodating an increasing number of collaborators.

The FA pipeline within FLAI empowers secure and privacy-preserving collaborative data analysis, making it an ideal solution for industries where sensitive data must remain confidential. By integrating SMPC with the L3 application chain, FLAI ensures that participants can contribute to and benefit from shared analytics without compromising their data privacy. The decentralized, transparent, and incentivized nature of the pipeline fosters long-term engagement and collaboration, ultimately driving the development of more accurate and impactful analytics models.

6 Marketplace Design

The FLAI platform operates as a sophisticated double-sided marketplace, seamlessly connecting task publishers (model requestors) and FL Trainers (workers) to foster collaborative federated learning (FL) processes. By leveraging token-based incentive mechanisms, dynamic governance structures, and subscription models, the marketplace ensures equitable participation, sustainable revenue generation, and robust model deployment.

6.1 Overview of the FL Marketplace

The marketplace is designed to balance the interests of task publishers and FL Trainers while maintaining FLAI's overarching goals of privacy, security, and scalability. Task publishers propose federated learning tasks by specifying requirements, such as model architecture, data compliance, and computational needs. FL Trainers join SubDAOs to contribute their resources and local data for collaborative model training.

To ensure alignment of incentives, the marketplace employs token-based mechanisms. These mechanisms reward contributions based on data quality, computational resources, and adherence to SMPC protocols, creating a transparent and equitable ecosystem.

6.2 Joining and Exiting the FLAI-SuperDAO

Membership in the FLAI-SuperDAO is open to all stakeholders and governed through the use of FLAI tokens for governance and participation.

6.2.1 Joining the FLAI-SuperDAO

Individuals can join the FLAI-SuperDAO by holding and staking FLAI tokens. This process requires depositing FLAI tokens into the SuperDAO governance pool, which supports platform-wide governance and operational activities. The stake requirements may vary dynamically depending on the growth, demand, and other economic factors of the DAO, fostering a sustainable governance framework.

6.2.2 Exiting the SuperDAO

Members can exit SuperDAO by unstaking their FLAI tokens. Upon exit, the staked FLAI tokens are returned, subject to an exit fee. This fee ensures that the governance pool remains robust and discourages short-term participation. The FLAI token serves as a transferable asset, encouraging broad-based participation while maintaining alignment with the long-term goals of the SuperDAO.

6.3 FL Task Creation and Fees

Task publishers (or model requesters) are integral to the FLAI marketplace. To propose an FL task, publishers must pay a creation fee, which covers operational costs such as governance activities, SubDAO formation, and computational overhead. This fee structure discourages frivolous proposals while incentivizing meaningful contributions to the ecosystem.

Successful tasks—those resulting in actively used models—may qualify for partial fee refunds. This refund mechanism encourages task publishers to align their proposals with the platform's operational goals and fosters active engagement.

6.4 FL Model Subscription Plans

The FLAI platform offers subscription-based access to trained federated learning models, catering to users with recurring inference needs. These plans provide predictable revenue for the ecosystem while encouraging long-term relationships with model users.

For example, a subscription plan might offer unlimited inferences for up to X queries per month at a fixed price of Y. Model requestors and third-party organizations can opt for these plans to access reliable predictions while supporting the FLAI ecosystem's growth.

6.5 Inference and Payment Distribution

Once a global model is trained, it becomes available for inference under FLAI's pay-per-inference mechanism. This approach balances free-market dynamics with equitable distribution of revenue among SubDAO members.

6.5.1 Price Tiers and Payment Distribution

Inference pricing is determined by the SubDAO through collective decision-making. Prices are tiered based on the user's relationship with the platform:

- **External Third-Party Users:** Priced at $10x$ per inference.
- **Model Requestors:** Priced at $3x$ per inference.
- **SubDAO Members:** Priced between 0 and x, depending on their contribution ranking.

For each inference, payments are distributed as follows:

- A fixed portion (e.g., 30%) is sent to the FLAI treasury to fund platform development, revenue generation, and potential token buy-back or burn activities.
- The remaining payment is distributed unevenly among SubDAO members, weighted by their contributions during the FL cycle. Higher-ranked members receive a larger share, ensuring that contributions are adequately rewarded.

6.5.2 Special Privileges for SubDAO Members

SubDAO members can use their trained models under specific conditions. The highest-ranked contributor during the FL cycle may use the model for free, while others must pay a price inversely proportional to their reward ranking. This mechanism incentivizes active participation and recognizes valuable contributions.

6.6 Sustainability Through Marketplace Design

The FLAI marketplace design integrates privacy-preserving computation, dynamic tokenomics, and decentralized governance to create a thriving ecosystem. By balancing incentives and responsibilities among task publishers, SubDAO members, and external users, the platform ensures long-term sustainability and scalability in decentralized federated learning.

7 Governance Model

The governance model of FLAI is designed to balance decentralization, transparency, and accountability while enabling seamless coordination between platform-wide operations and task-specific governance. It is structured around two key entities: the FLAI-SuperDAO and FLAI-SubDAOs, each with distinct roles, responsibilities, and mechanisms for participation.

7.1 FLAI-SuperDAO Governance Model

7.1.1 Purpose and Scope

The FLAI-SuperDAO serves as the central governance body for the FLAI ecosystem, overseeing global operations, policy updates, and the alignment of incentive mechanisms. Its primary goal is to ensure the efficient functioning and sustainable growth of the platform while maintaining fairness and inclusivity.

7.1.2 Membership and Voting Power

Membership in the SuperDAO is extended to FL Task Publishers and other platform stakeholders. Members participate in governance by staking FLAI tokens, which serve as proof of membership and the basis for determining voting power within the governance structure. The staking and voting processes are transparently managed through smart contracts to ensure fairness and accountability.

7.1.3 Decentralized Voting Mechanisms

Governance decisions within the SuperDAO are made through decentralized voting mechanisms, ensuring that every member's voice is heard.

Proposal Submission: Any member of the SuperDAO can propose platform-level updates or the initiation of new FL tasks. Proposals are submitted via smart contracts and made available for review by the community.

Voting Thresholds: Decisions are classified based on their impact:

- **Platform-Level Updates and FL Task Approvals:** Require a predefined supermajority (e.g., 66%) to ensure alignment across the community.
- **Operational Changes:** Require a lower majority (e.g., 51%) for efficient decision-making.

Approved proposals are automatically executed through smart contracts, ensuring transparency, immutability, and trust in the governance process.

7.1.4 Oversight of SubDAO Operations

The SuperDAO monitors and evaluates the performance of all SubDAOs. It sets thresholds for task-specific reward distributions and ensures that SubDAO operations align with platform-wide policies. Reporting mechanisms facilitate communication between SubDAOs and the SuperDAO, enabling streamlined coordination and accountability.

7.2 FLAI-SubDAO Governance Model

7.2.1 Purpose and Scope

FLAI-SubDAOs are decentralized entities created for task-specific governance. Each FL Task is managed by a dedicated SubDAO, which focuses on the execution of model training, validation, and the distribution of rewards to contributors. SubDAO governance is flexible, allowing members to make decisions tailored to their specific tasks while adhering to thresholds set by the SuperDAO.

7.2.2 Membership and SBT Allocation

Membership in a SubDAO is granted to FL Trainers participating in a specific FL Task. Trainers receive SubDAO SBTs, which are proportional to their contributions in training and validation cycles. These tokens dynamically evolve after each FL cycle, reflecting recent activity and ensuring fairness in governance and reward distribution.

7.2.3 Task-Specific Decentralized Voting

Governance decisions within SubDAOs are made collaboratively, with voting mechanisms tailored to the task at hand:

Model Validation Votes: SubDAO members use a peer-review system to validate local models submitted for training. Voting power is weighted based on SubDAO SBTs, ensuring that contributions are appropriately recognized.

Reward Distribution Votes: SubDAO members collectively decide on formulas for reward allocation, prioritizing fairness and incentivizing high-quality contributions. Reward thresholds are set within limits defined by the SuperDAO.

Pricing Votes: Pay-per-inference pricing for trained models is determined by SubDAO members through a weighted voting mechanism. This ensures fair pricing reflective of market demand and task-specific efforts.

Governance Updates: SubDAO members can propose changes to governance structures, such as adjustments to task parameters or revisions to training protocols. Significant changes require a higher voting threshold (e.g., 75%), while operational updates may pass with a simple majority.

7.2.4 Transparency and Reporting

To ensure accountability, all task-specific decisions and actions are recorded on a dedicated blockchain ledger for each SubDAO. This ensures a transparent and auditable history of governance activities. SubDAOs regularly report their lifecycle progress, including model status and incentive distributions, to the SuperDAO.

7.3 Alignment of SuperDAO and SubDAO Governance

The hierarchical yet decentralized relationship between the SuperDAO and SubDAOs ensures that platform-wide goals are met while allowing for task-specific autonomy. The governance model's dual-layer structure fosters a collaborative environment where stakeholders can contribute effectively, benefiting from decentralized decision-making and transparent operations.

8 Validation and Reward Structures

The validation and reward structures within the FLAI ecosystem are designed to ensure fairness, transparency, and incentivization of high-quality contributions. By employing robust validation mechanisms and dynamic reward distribution, FLAI fosters a collaborative environment where participants are recognized and rewarded based on meaningful contributions.

8.1 Validation Mechanism

Validation is a cornerstone of the FLAI federated learning (FL) pipeline, ensuring the reliability, accuracy, and effectiveness of both local and global models. FLAI employs a dual-layered validation mechanism encompassing Local Model Validation (LMV) and Global Model Validation (GMV).

8.1.1 Local Model Validation

Local Model Validation (LMV) evaluates the performance of individual FL Trainers' models against task-specific requirements.

Validation Dataset: The task-specific dataset, provided by the FL Task Publisher, serves as the standard for independent validation. This dataset remains encrypted to maintain privacy and adhere to SMPC protocols.

Peer-Review Mechanism: FL Trainers conduct peer reviews of each other's models using the validation dataset. Peer-review outcomes are aggregated using weighted consensus mechanisms that account for the reputation and past contributions of reviewers. This approach ensures objectivity, minimizes biases, and promotes trust within the SubDAO.

8.1.2 Global Model Validation

Global Model Validation (GMV) evaluates the aggregated model created from local updates, ensuring its generalization capabilities and overall effectiveness.

Distributed Validation: FL Trainers validate the global model across their respective datasets, testing its performance on diverse data sources. This distributed approach guarantees robust evaluation across varying real-world conditions.

Task-Specific Metrics: The global model is assessed using predefined task-specific performance metrics provided by the FL Task Publisher. These metrics, combined with peer-validation results, form a comprehensive evaluation of the model's success.

8.2 Ranking Contributions

To promote accountability and reward meaningful participation, FLAI ranks FL Trainers based on their contributions during each FL cycle. Rankings are determined by combining LMV and GMV scores with other contribution metrics.

8.2.1 Ranking Criteria

Trainers are ranked using the following factors:

- **Validation Scores:** Local Model Validation (LMV) scores are derived from peer-review outcomes, reflecting the accuracy and robustness of individual models.
- **Global Model Validation (GMV) Impact:** Trainers' contributions to the global model's performance are evaluated using task-specific metrics and weighted for their significance.
- **Data Quality and Quantity:** Contributions are assessed based on the relevance and volume of training data provided during the FL cycle.
- **Model Performance:** Individual contributions to the global model's improvements are validated and weighted accordingly.

Composite Scoring: Rankings are calculated using a composite score:

$$\text{Composite Score} = \alpha(\text{LMV}) + \beta(\text{GMV}),$$

where α and β are weight coefficients summing to 1, reflecting the relative importance of LMV and GMV.

8.2.2 Impact on Rewards

Rankings directly influence the distribution of rewards. Trainers with higher composite scores receive:

- A larger share of pay-per-inference revenue.
- Increased governance influence through redistributed SubDAO SBTs.
- Additional benefits such as reduced inference costs or free usage of the global model.

8.3 Incentivizing High-Quality Contributions

FLAI employs multiple mechanisms to encourage participants to deliver high-quality work, recognizing both immediate contributions and sustained engagement.

8.3.1 Token-Based Rewards

Top-ranked contributors receive higher allocations of platform tokens, derived from pay-per-inference revenue. This ensures high-quality contributions are monetarily incentivized.

8.3.2 Governance Influence

High-ranking trainers gain increased governance influence within their SubDAOs through redistribution of SubDAO SBTs, enabling them to shape decisions and strategies.

8.3.3 Reduced Costs and Exclusive Benefits

Top contributors may enjoy reduced inference costs or even free usage of the trained model. This incentivizes excellence and promotes continued engagement.

8.4 Reward Distribution Mechanisms

The distribution of rewards is governed by transparent and decentralized mechanisms that align with FLAI's principles of fairness and incentivization.

8.4.1 Platform Token Distribution

Platform tokens are allocated to SubDAO contributors based on their rankings and validated contributions. This ensures equitable and transparent distribution of rewards.

8.4.2 SubDAO Governance Token Redistribution

SubDAO governance tokens are dynamically redistributed after each FL cycle. Higher-ranked contributors receive a larger share, while passive or minimally active participants see reduced allocations. This dynamic redistribution promotes active engagement.

8.4.3 Redistribution Dynamics

The reward system adapts to evolving contributions, ensuring that rewards are aligned with validated efforts. By incorporating LMV and GMV metrics, FLAI creates a meritocratic environment that recognizes and values high-quality work.

8.5 Transparency and Accountability

All validation outcomes, rankings, and reward distributions are recorded on the blockchain. This ensures transparency, auditability, and alignment with FLAI's commitment to responsible AI and decentralized governance.

9 Incentive Mechanisms

The FLAI ecosystem incorporates a sophisticated incentive mechanism to ensure sustained participation, fair rewards, and the alignment of individual contributions with the platform's broader goals. This system leverages tokenomics, a pay-per-inference revenue model, and dynamic governance token redistribution to create a self-sustaining and meritocratic environment.

9.1 Tokenomics Structure

The tokenomics structure of FLAI is designed to incentivize contributors while maintaining platform sustainability. It features two primary types of tokens: platform tokens and SubDAO-specific governance tokens.

9.1.1 Platform Tokens

Platform tokens serve as the foundational currency of the ecosystem. These tokens are utilized for:

- **Pay-per-Inference:** Payments made by users or external entities for utilizing trained models.
- **Rewards and Incentives:** Distributed to contributors based on their performance and contributions during an FL cycle.
- **Platform Treasury:** A portion of the token revenue is allocated to the platform treasury for maintenance, updates, and future development.

9.1.2 SubDAO Tokens

SubDAO-specific governance tokens are soulbound and represent the decentralized governance mechanism at the task level. These tokens are dynamically allocated to individuals based on their contributions, ensuring that active participants are recognized and rewarded. As soulbound tokens, they cannot be traded, reinforcing their role as a reflection of individual effort and engagement within the SubDAO. The number of SubDAO tokens held by an individual directly influences their governance voting power, enabling them to participate in decisions regarding task-specific parameters, pricing, and reward distribution. Additionally, the quantity of SubDAO tokens determines the proportion of revenue they receive from pay-per-inference or pay-per-query mechanisms, further incentivizing trainers and contributors to maintain high-quality participation and alignment with SubDAO goals.

9.2 Pay-Per-Inference Revenue Model

The pay-per-inference revenue model is central to FLAI's economic framework. It ensures that contributors are directly rewarded for the usage of trained models while maintaining platform sustainability.

9.2.1 Revenue Distribution

Revenue from inference usage is distributed as follows:

- **Platform Treasury:** A fixed percentage (e.g., 30%) of inference payments is allocated to the treasury for operational and developmental expenses.
- **SubDAO Contributors:** The remaining revenue is distributed among SubDAO members using a weighted distribution model. Contributors with higher rankings and validated contributions receive a larger share of the revenue. We must emphasize that this revenue distribution triggers after a certain period, as a distribution after each inference may not be feasible due to transaction costs.

9.2.2 Pricing Model

The pricing model is designed to balance accessibility and incentivization:

- **External Third Parties:** Charged a premium rate (e.g., $10x$ per inference) to utilize the model.
- **Model Requestors:** Charged a moderate rate (e.g., $3x$ per inference) for task-specific usage.
- **SubDAO Members:** Enjoy reduced or zero-cost inference usage (e.g., 0–x per inference) based on their ranking and reward allocation within the SubDAO.

9.3 Dynamic Redistribution of Governance Tokens

Governance token redistribution ensures that power within SubDAOs aligns with active and high-quality participation. This mechanism is executed at the end of each FL cycle.

9.3.1 End-of-Cycle Redistribution

At the conclusion of each FL cycle, SubDAO governance tokens are reallocated based on:

- **Peer-Reviewed Contributions:** Quality and quantity of local model submissions, as validated by peer review.
- **Ranking Scores:** Contributions to the local and global model validation processes, reflected in LMV and GMV rankings.

9.3.2 Lifecycle Redistribution

Governance tokens are dynamically redistributed after each cycle, ensuring that governance power remains tied to active participation. Redistribution metrics include:

- **Local Model Accuracy Improvement:** Measured improvement in local models, as determined during validation.
- **Global Model Contribution:** Impact on the aggregated global model's performance, validated through distributed testing.

Fairness and Sustainability: This dynamic redistribution mechanism promotes sustained engagement by rewarding consistent contributors and discouraging passive participation. It also ensures that governance power evolves in tandem with the ecosystem's needs and challenges.

9.4 Transparency and Accountability

The incentive mechanisms within FLAI are governed by transparent processes recorded on the blockchain. All token distributions, rankings, and validations are auditable, reinforcing trust in the system and aligning with FLAI's commitment to decentralized and responsible governance.

10 Security and Privacy

Security and privacy are foundational to the FLAI ecosystem, especially given its focus on sensitive domains like healthcare and fitness. The architecture and protocols employed are designed to protect participant data and ensure secure collaborative learning while maintaining transparency and accountability.

10.1 Importance of Security and Privacy

Federated learning (FL) inherently involves multiple stakeholders collaborating on model training without centralizing raw data. In domains such as healthcare and fitness, where data sensitivity is critical, ensuring robust security and privacy is essential. Breaches in confidentiality can lead to severe consequences, including legal liabilities and loss of trust. FLAI addresses these challenges by incorporating state-of-the-art cryptographic protocols and decentralized validation mechanisms.

10.1.1 Confidentiality in Collaborative Learning

FL enables model training and inference across decentralized datasets. However, ensuring that sensitive information remains private while facilitating collaborative computation is paramount. The FLAI platform achieves this through privacy-preserving techniques that protect data throughout its lifecycle—from training to inference.

10.2 Secure Multi-Party Computation (SMPC) for Privacy Guarantees

Secure Multi-Party Computation (SMPC) is the cornerstone of FLAI's privacy-preserving framework. This advanced cryptographic technique ensures that sensitive data is never exposed, even during collaborative operations.

10.2.1 Privacy in Model Training

Local model updates, such as gradients, are computed and encrypted using SMPC protocols before being shared. This ensures:

- Sensitive data never leaves the local devices or institutions.
- Encrypted gradients contribute to the global model update without exposing individual contributions.

10.2.2 Privacy in Inference Requests

Inference processes are also secured with SMPC:

- Users encrypt their input data before submitting it for inference.
- The trained model processes encrypted inputs, ensuring that neither the model operators nor other participants gain access to user data.

This privacy-preserving inference mechanism guarantees confidentiality at all stages, reinforcing trust in the system.

10.3 Mitigation of Data Leakage and Tampering Risks

FLAI implements robust measures to mitigate the risks of data leakage and tampering, which are inherent in federated systems.

10.3.1 Gradient Leakage Prevention

In traditional FL, gradients shared during training can inadvertently leak sensitive information. To address this:

- SMPC ensures gradients are encrypted and shared securely among participants.
- This protocol prevents any single party from reconstructing the raw data from gradient information.

10.3.2 Decentralized Validation and Aggregation

Decentralized mechanisms reduce the risks associated with centralization:

- **Local Model Validation:** Peer reviews within SubDAOs validate local models, ensuring transparency and reducing single points of failure.
- **Secure Aggregation:** Global model aggregation is conducted using SMPC, maintaining the confidentiality of individual contributions while achieving robust model updates.

10.4 Ensuring Trust through Transparency

The combination of SMPC and decentralized validation ensures that FLAI's security and privacy measures remain auditable and trustworthy. All validation and aggregation operations are recorded on the blockchain, creating an immutable ledger of activities. This enables:

- Full traceability of model updates and validations.
- Accountability for all participants, fostering a culture of responsible collaboration.

10.5 Addressing Core Risks in Federated Learning

FL systems face inherent risks, such as gradient leakage and tampering. FLAI's architecture is specifically designed to mitigate these vulnerabilities:

- Secure protocols ensure that gradients and updates are never exposed to unauthorized parties.
- Decentralized validation mechanisms reduce reliance on central entities, preventing systemic vulnerabilities.

By combining SMPC, decentralized validation, and transparent governance, FLAI establishes itself as a secure and privacy-respecting platform. These measures enable stakeholders to collaborate confidently, knowing that their sensitive information is protected throughout the federated learning lifecycle.

11 Use Cases

FLAI's architecture and features enable transformative applications across various domains, leveraging federated learning's inherent strengths in privacy, scalability, and collaboration. This section explores key use cases, illustrating the platform's potential to drive innovation while ensuring data confidentiality.

11.1 Healthcare Data Sharing

Healthcare systems generate vast amounts of sensitive data that hold the potential to improve patient outcomes and streamline operations. However, privacy concerns and regulatory requirements often hinder data sharing. FLAI's privacy-preserving federated learning framework overcomes these challenges, enabling collaborative model development without compromising patient confidentiality.

11.1.1 Pharmaceutical Industry Applications

Pharmaceutical companies can harness the power of federated learning to develop advanced predictive models from personal health records (PHR) data provided by individuals, all while adhering to stringent privacy standards. Key applications include:

Market Segmentation and Sizing Models: These models categorize patient populations based on specific clinical attributes, such as genetic markers or disease progression stages. By analyzing federated datasets, pharmaceutical companies can estimate the size of potential markets for new drugs, informing product development and marketing strategies.

Treatment Response Prediction Models: Federated learning allows the creation of models that predict which subsets of patients are most likely to respond positively to specific treatments. These models utilize data on past treatment outcomes, patient demographics, and clinical characteristics, enabling precision medicine approaches that enhance therapeutic efficacy.

Health Economics and Outcomes Research (HEOR) Models: HEOR models evaluate the clinical and economic impacts of treatments by considering metrics such as quality-adjusted life years (QALYs) and healthcare costs. With federated learning, such models can incorporate data from multiple institutions without centralizing sensitive information, supporting cost-effective healthcare delivery and policy decisions.

11.2 Supply Chain Optimization

Efficient supply chains are vital for manufacturing, retail, and pharmaceuticals. Federated learning optimizes operations by leveraging insights from decentralized data sources while preserving data privacy.

11.2.1 Collaborative Demand Forecasting

Organizations can jointly train models to predict demand patterns using sales data, inventory levels, and external factors such as seasonality. Federated learning enhances forecasting accuracy without compromising proprietary data security.

11.2.2 Logistics and Route Optimization

FLAI supports collaborative model development for optimizing logistics operations, including route planning. Sharing insights from local datasets helps reduce transportation costs, improve efficiency, and lower environmental impact.

11.3 Financial Fraud Detection

The financial sector requires adaptive fraud detection mechanisms to counter evolving threats. Centralized approaches are often constrained by privacy regulations. FLAI offers a decentralized, secure alternative for collaboration among financial institutions.

11.3.1 Anomaly Detection Models

Federated learning enables the development of models to detect anomalous transactions by analyzing patterns across multiple institutions. This approach strengthens detection capabilities without exposing sensitive data.

11.3.2 Real-Time Fraud Prevention

FLAI facilitates real-time fraud prevention systems that monitor transactions for suspicious activities. Leveraging decentralized data ensures adaptability to emerging threats while maintaining privacy compliance.

11.4 Broader Impacts Across Industries

FLAI extends beyond healthcare, supply chain management, and finance, with applications in energy, retail, and education. It enhances efficiency, personalizes services, and supports innovation. Its flexible architecture adapts to diverse challenges while ensuring privacy and security.

FLAI enables secure, collaborative learning across industries, demonstrating its ability to address complex problems and advance privacy-preserving AI.

References

[1] B. McMahan, E. Moore, D. Ramage, S. Hampson, and B. A. y. Arcas, "Communication-Efficient Learning of Deep Networks from Decentralized Data," in *Proceedings of the 20th International Conference on Artificial Intelligence and Statistics*, Fort Lauderdale, FL, USA, Apr. 2017.

[2] W. Wei, L. Liu, M. Loper, K. H. Chow, M. E. Gursoy, S. Truex, and Y. Wu, "A Framework for Evaluating Gradient Leakage Attacks in Federated Learning," Apr. 2020, arXiv:2004.10397.

[3] U. Majeed, L. U. Khan, A. Yousafzai, Z. Han, B. J. Park, and C. S. Hong, "ST-BFL: A Structured Transparency Empowered Cross-Silo Federated Learning on the Blockchain Framework," *IEEE Access*, vol. 9, pp. 155 634–155 650, Nov. 2021.

[4] D. Ramage and S. Mazzocchi, "Federated Analytics: Collaborative Data Science without Data Collection," May 2020, Accessed: Dec. 25, 2024. [Online]. Available: https://research.google/blog/federated-analytics-collaborative-data-science-without-data-collection/

[5] S. R. Pandey, M. N. H. Nguyen, T. N. Dang, N. H. Tran, K. Thar, Z. Han, and C. S. Hong, "Edge-Assisted Democratized Learning Toward Federated Analytics," *IEEE Internet of Things Journal*, vol. 9, no. 1, pp. 572–588, Jan. 2022.

[6] 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*, Cloudcroft, New Mexico, USA, Sep. 2001, pp. 13–22.

[7] K. Bonawitz, H. Eichner, W. Grieskamp, D. Huba, A. Ingerman, V. Ivanov, C. M. Kiddon, J. Konečný, S. Mazzocchi, H. B. McMahan, T. Van Overveldt, D. Petrou, D. Ramage, and J. Roselander, "Towards Federated Learning at Scale: System Design," in *Proceedings of the 2nd Conference on Systems and Machine Learning (SysML)*, Stanford, CA, USA, Apr. 2019.

[8] P. Kairouz, H. B. McMahan, B. Avent, A. Bellet, M. Bennis, A. N. Bhagoji, K. Bonawitz, Z. Charles, G. Cormode, R. Cummings *et al.*, "Advances and Open Problems in Federated Learning," Dec. 2019, arXiv:1912.04977.

[9] Q. Yang, Y. Liu, T. Chen, and Y. Tong, "Federated Machine Learning: Opportunities and Challenges," *IEEE Transactions on Neural Networks and Learning Systems*, vol. 30, no. 2, pp. 502–516, 2019.

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

[11] J. C. Benaloh, "Secret Sharing Homomorphisms: Keeping Shares of a Secret Secret," in *Conference on the Theory and Application of Cryptographic Techniques*, Berlin, Heidelberg, Aug. 1986, pp. 251–260.

[12] I. Damgård, V. Pastro, N. Smart, and S. Zakarias, "Multiparty Computation from Somewhat Homomorphic Encryption," in *Annual Cryptology Conference (CRYPTO)*, Berlin, Heidelberg, Aug. 2012, pp. 643–662.