Decentralized Intelligence Network (DIN)

Abraham Nash
University of Oxford
abraham.nash@cs.ox.ac.uk

Abstract: Decentralized Intelligence Network (DIN) is a theoretical framework tackling AI challenges like data fragmentation and siloing. It enables efficient AI training on decentralized data stores, overcoming barriers to diverse data access by leveraging: 1) Decentralized data stores to maintain data ownership, ensuring data stays securely within Participants' chosen stores; 2) A scalable federated learning protocol for decentralized AI training, where only model parameter updates are shared, keeping data within these stores; 3) A trustless cryptographic rewards mechanism on a public blockchain to incentivize participation and ensure fair reward distribution via decentralized auditing. Aggregation is managed by decentralized Evaluators—participants who secure the network, validate models, and assess performance to ensure fair rewards distribution. This ensures anyone can access the data needed to train artificial intelligence (AI) without owning or storing a data silo. Coordination of the aggregation and rewards processes is managed on a public blockchain, ensuring no entity can control or prevent data access, nor insert themselves as intermediaries in the rewards process.

1. Introduction

The World Wide Web's evolution from its decentralized origins to today's landscape reflects a complex journey in digital architecture. Originally designed as a distributed network, Web 1.0 envisioned a digital space where data and resources could be shared across multiple nodes without central oversight [1]. However, the emergence of Web 2.0 marked a shift towards centralized platforms, bringing significant efficiency and scalability at the cost of user privacy and control over personal data [2]. While Web 3.0 aims to return to decentralized principles, progress has been gradual [2].

In today's digital landscape, the rapid advancement of artificial intelligence (AI) and the growing volume of data generated across various sectors have created a paradox: while more data than ever is available, much of it remains inaccessible due to fragmentation and siloing within centralized systems. Data is often the lifeblood of AI, yet valuable data remains underutilized due to these silos, where creators and data producers are not fairly compensated for their contributions. This situation limits both decentralized data ownership and the full potential of AI development.

Various styles of decentralized data stores have emerged to distribute data across independent, decentralized locations, offering a promising solution to data fragmentation and privacy challenges [3], [4]. These systems keep data in decentralized locations, avoiding centralized control or siloing. While they enhance data accessibility and ownership, they present a new challenge for AI development. Traditional AI approaches often require re-centralization for data aggregation by third parties, conflicting with the core principles of decentralization. The key challenge is to enable AI models to learn from diverse, decentralized data sources without requiring data to be moved or centralized.

This dichotomy presents two interrelated challenges: ensuring scalable access to data for AI development while preserving decentralized data ownership in an increasingly data-driven world. A key focus is finding better incentives for data contribution and fair value distribution, addressing how to motivate and reward data providers effectively. This paper aims to design and outline a decentralized intelligence network for AI development that tackles both challenges.

Federated Learning (FL) emerges as a promising solution in this context, enabling AI model training without requiring data centralization [5]. However, many current systems still operate within siloed structures that mirror centralized models. While these systems decentralize the training process, they often rely on frameworks that favor third-party controllers of siloed data or services in the real world. As a result, current FL implementations mainly serve the interests of single-entity providers by

focusing on data minimization and breach prevention, but they fail to fully leverage the potential of decentralized data stores or enable truly decentralized AI development across such networks.

DIN proposes a new approach to decentralized AI that ensures data ownership remains with participants, enabling learning within decentralized data networks—such as those used by small and medium-sized enterprises (SMEs), individual entrepreneurs, consumer networks, and industry-specific sectors (e.g., retail, logistics, agriculture, or energy). These networks often hold valuable, diverse data, but on their own, this data has limited potential for offering or monetizing without broader integration. *DIN* utilizes public blockchain and IPFS technologies with a decentralized Federated Learning (FL) architecture to enable scalable, decentralized AI. It adapts tools and workflows from existing FL frameworks (e.g., Bonawitz et al., 2019) [5] and integrates secure aggregation techniques, such as those used in TensorFlow (Abadi et al., 2016) [6] to facilitate decentralized learning. These adjustments are essential for overcoming the limitations of traditional, siloed clusters, ensuring AI models can be trained effectively across diverse, decentralized data stores.

By introducing new monetization models for decentralized data owners, *DIN* enables individuals, SMEs, and enterprises to retain ownership of their data while unlocking its economic potential. This framework fosters the emergence of decentralized economies, where data owners directly benefit from their contributions to AI development. *DIN* enhances access to owner-held, decentralized data, overcoming the limitations of siloed systems, and empowers AI ecosystems that promote innovation, fairness, and economic opportunity.

The remainder of this paper is structured as follows: **Section 2** outlines an exploration of the problem statement and the current limitations in AI and data management. **Section 3** provides an overview of the proposed *DIN* framework systems architecture while **Section 4** presents a theoretical implementation approach of the protocol. Finally, **Section 5 onward** offers its conclusion, outlining future research directions and the broader implications of the work.

2. Problem Statement

The current digital ecosystem faces several interconnected challenges:

1. **Data Ownership**: Individuals and organizations lack control over their data, often surrendering ownership and usage rights to centralized entities [7].
2. **Limited AI Utilization**: The fragmentation of data across providers and institutions hinders the development of comprehensive, widely beneficial AI models [8].
3. **Access Barriers**: Researchers and developers face significant obstacles in accessing diverse, large-scale datasets necessary for training advanced AI models [9].
4. **Incentive Misalignment**: Current data ecosystems often fail to adequately compensate data providers, discouraging participation in data-access initiatives [10].
5. **Centralization Risks**: Existing AI development paradigms concentrate power and benefits in the hands of a few large tech companies, raising concerns about monopolistic practices and potential misuse of AI technologies [11]. Centralized platforms often create a closed environment with full-stack lock-in and a walled garden, where a single entity decides on value attribution and distribution. This leads to minimal privacy protection and user control, leaving users with limited choices and bargaining power.
6. **Privacy and Security**: Centralized data storage and processing increase vulnerability to breaches and unauthorized access [12].
7. **AI Safety and Control**: The trend towards large, centralized models raises several concerns:
    - Increased risk of developing agent-like behaviors, complicating alignment and control [13].
    - Potential for creating surveillance-like environments due to extensive data access [14].
    - Disproportionate influence of a few entities on global information flow and decision-making [15], [16], [17].
    - Amplification of biases present in training data or introduced by a small group of developers [18].

Decentralized Intelligence Network (DIN) offers an innovative solution to the challenges surrounding data availability, AI development, and privacy in the current digital landscape. By utilizing decentralized data stores, federated learning (FL), public blockchain technology, and IPFS, the framework provides a secure, efficient, and scalable data ecosystem that upholds individual data ownership while driving innovation in AI.

2.1 Requirements

To address the challenges of decentralized, large-scale AI training while ensuring fair, decentralized rewards for participation in federated learning protocols, we propose a framework that upholds ownership and control of decentralized data stores. In this framework, data remains distributed across various decentralized stores, with no central authority exerting control.

Specifically, we define the following principles:

1. **Data Ownership:** Participants retain ownership and control over their decentralized data stores, ensuring no entity can manage or control their data.
2. **Decentralized AI:** Access to data for federated learning is determined by Participants, who can opt in to offer their data for AI development. No entity can deny AI developers access to data that Participants have chosen to contribute.
3. **Direct Rewards:** Reward distribution is transparent and decentralized, with no third-party intermediaries determining the rewards for Participants, ensuring fairness in how contributions are recognized and compensated.

DIN ensures decentralized control of FL orchestration processes, allowing participants to retain ownership of their data while keeping it securely within decentralized stores, except for model updates. It enables a transition to data stores that can be owned and monetized by a broader range of entities, while acknowledging that centralized learning will continue in the near term. By supporting widespread participation in the FL protocol, *DIN* creates new opportunities for scalable, decentralized AI development. The framework addresses key challenges in the digital landscape, promoting a fairer, more secure environment for AI development with inclusivity and open participation.

3. Background & Related Works

3.1 Orchestration

Federated Learning (FL) orchestration can be broken down into three primary components: 1) Aggregation, 2) Coordination, and 3) Rewards. Each of these elements is essential for the effective operation of FL, ensuring efficient and secure AI model training. This discussion specifically addresses FL orchestration within the context of decentralized solutions, emphasizing the importance of decentralized data stores, which are crucial for maintaining data ownership and privacy. For additional details, refer to the relevant references [3], [19], [20], [21]. In this framework, decentralized data stores offer the infrastructure needed for efficient data management, reducing costs and enhancing scalability, while enabling a flexible, decentralized approach to AI training.

3.2 Aggregation

3.2.1 Decentralized Aggregation Process

Aggregation is a core component of Federated Learning (FL), where local model updates from multiple participants are combined into a global model. Traditionally, this process relies on a central server to collect, process, and average updates. In contrast, *DIN* replaces the central server with Evaluators—decentralized nodes responsible for aggregating, validating, and evaluating model updates. By decentralizing these tasks, DIN enhances transparency and fairness in reward distribution while maintaining model integrity.

To scale the aggregation process, DIN allows Participants to conduct Federated Learning (FL) in multiple groups, which then have their model updates processed by designated aggregator groups. For example, in a group of a thousand participants, there might be ten subgroups of a hundred. Within each subgroup, ten Evaluators could be assigned in a 1:10 ratio. Each Evaluator, using their own computational resources, conducts the aggregation of the 100 models, sharing their results using IPFS to publish the outcomes. The smart contract then verifies that all Evaluators reached the same results.

This process is fully decentralized, with Evaluators randomly assigned to further ensure fairness and prevent collusion. The evaluation process is made secure through Sybil resistance, where more than 50% of Evaluators would need to collude to corrupt the aggregation, a highly unlikely scenario given the random assignment of Evaluators. This reduces the potential for malicious

attacks. To minimize on-chain costs, the process can be conducted off-chain using IPFS, with Evaluators cross-checking results among themselves. If discrepancies arise, they may participate on-chain for additional checks.

To ensure the integrity of the process, Evaluators are required to stake tokens, which are forfeited if they act maliciously, ensuring that the aggregation process remains trustworthy, secure, and fair.

3.2.2 Sybil Resistance and Trustworthiness

To ensure the integrity of the aggregation process, *DIN* incorporates a **staking mechanism** that incentivizes Evaluators to act honestly. Evaluators must stake tokens to participate in model aggregation, and if they misbehave (e.g., by submitting invalid evaluations), they forfeit their stake. This mechanism serves to deter malicious behavior and ensures that only reliable Evaluators contribute to the aggregation process.

In addition, *DIN* requires that a majority (greater than 50%) of Evaluators agree on the aggregated model scores. This threshold prevents a single rogue Evaluator from corrupting the aggregation, ensuring a fair and accurate model update. The network fee generated from this system helps support the operations of the Evaluators and incentivizes active participation, creating a positive feedback loop that strengthens the overall network.

3.2.3 Scalability, Efficiency, and Privacy

DIN's decentralized approach enhances scalability by organizing participants into smaller aggregator groups, where multiple Evaluators validate model updates concurrently. This structure is inspired by hierarchical aggregation methods for scalability (e.g., as described by Bonawitz et al., 2019), but with a key difference: the coordination of the process is managed on-chain through a public ledger, while the actual aggregation is performed by Evaluators on decentralized nodes using their own computing resources. This decentralization reduces reliance on centralized infrastructure, speeds up the aggregation process, and improves efficiency. At the same time, the system ensures transparency and security, as the process is validated and protected by Sybil resistance and token staking.

Additionally, *DIN* can incorporate privacy-preserving techniques, such as secure aggregation, to protect user data. While more advanced methods like differential privacy (McMahan et al., 2018) could further enhance privacy, DIN's existing framework ensures that colluding agents cannot infer information about other participants when $N \geq 3$, preserving privacy across the network. This combination of decentralization, secure aggregation, and privacy preservation strengthens the overall robustness and trustworthiness of the *DIN* framework.

Recent research has explored alternative decentralized aggregation methods aimed at eliminating the need for central servers, improving scalability, and enhancing privacy, all of which are key objectives of *DIN*. For instance:

- IPLS framework enables peer-to-peer model training without a central server, utilizing an IPFS-based protocol. It divides the model into partitions replicated across multiple agents, though it requires significant expertise for diverse model types and compression techniques, complicating training for more complex algorithms [22]. Unlike the centralized setting, where only the server is responsible for storing, updating, and broadcasting the model to the participating agents, IPLS splits the model into multiple partitions replicated on multiple agents [22].
- Vincent et al. (2020) proposed "Blockchain Assisted Federated Learning" (BC-FL), which replaces the need for a central server in the aggregation process by leveraging a public blockchain [23]. This approach considers that local model updates can be received by miners through a gossip protocol over the P2P network [23]. However, gossip-like protocols are notorious for diverging from the real value and failing to reach consensus [24].
- Ramanan et al. (2020) proposed "BAFFLE," an aggregator-free FL protocol that eliminates the need for a central server during the FL process [25]. However, this requires splitting and compressing machine learning models on the blockchain itself, posing significant challenges due to the complexity of model compression techniques and the extensive research needed to make this feasible.

Overall, *DIN* stands to benefit from exploring these innovative possibilities and adapting new technologies to effectively address the ongoing privacy and scalability concerns inherent in Federated Learning.

3.3 Coordination

Coordination in FL traditionally relies on a central authority to manage participant interactions and model updates. In their 2019 work, Bonawitz et al. demonstrated that centralized coordination can achieve both scalability and security, using an architecture consisting of Coordinators, Master Aggregators, and subgroups of Aggregators, capable of handling thousands of active devices and potentially scaling to billions [5].

However, centralized coordination poses several risks, including dishonest aggregation, network failures, external attacks, and reliance on potentially insecure third-party hardware used in aggregation processes. Additionally, ensuring protocol adherence within centralized systems can introduce vulnerabilities that compromise the integrity and security of the federated learning process [26]. To address these issues and maintain decentralized data ownership, *Decentralized Intelligence Network* (*DIN*) proposes using blockchain technology for coordination.

Blockchain offers several advantages for FL coordination:

1. Decentralization: Prevents any single authority from controlling data access, preserving ownership [27] .
2. Transparency: An immutable ledger records and verifies updates, enhancing trust among participants [21].
3. Fault tolerance: The peer-to-peer design improves system integrity [28], [29].
4. Computational benefits: Enhances round delineation, model selection, and model aggregation in a decentralized manner [30].

DIN adopts a decentralized federated learning (FL) approach, replacing centralized coordination with a public blockchain smart contract (SC) protocol [5]. This innovative structure maintains scalability while ensuring open access to FL protocols.

Participants are organized into smaller groups, each with dedicated Evaluators responsible for aggregating and validating model updates. By leveraging blockchain smart contracts, the coordination process remains transparent, secure, and decentralized, eliminating the need for centralized infrastructure.

The system builds upon the 'secure aggregation' principle, ensuring individual device updates remain uninspectable. Evaluators are randomly assigned to participant subgroups and run staked nodes, which provides Sybil resistance and incentivizes good behavior. Each Evaluator independently processes updates from at least k devices, mitigating the quadratic computational costs associated with large-scale networks [31], [5]. Evaluators produce intermediate aggregation results published on-chain, which are then averaged by the model owner to update the global model. Participants can verify aggregated scores and the final model directly on-chain, preventing malicious tampering and ensuring accuracy. While blockchain can introduce network delays [25], , the benefits of decentralization often outweigh this drawback. Crucially, *DIN* uses a public blockchain to prevent re-centralization and overcome institutional competitive interests, addressing limitations of both centralized approaches and private blockchain implementations [10].

By leveraging this decentralized framework, *DIN* can potentially handle large numbers of participants efficiently while keeping data distributed. This approach enables broader application of federated learning tools within decentralized data networks, promoting more open and collaborative machine learning ecosystems [5].

3.4 Rewards

The reward mechanism utilizes smart contracts (SCs) on a public blockchain to ensure fair compensation for computational contributions, eliminating the need for a third-party intermediary and allowing Participants to be rewarded directly. By implementing a decentralized reward system on a public blockchain using smart contracts (SCs), this approach allows Evaluators to assess Participants' work, verify their computational contributions, and complete the evaluations process transparently. Smart contracts (SCs) verify and allocate rewards based on precise computational evaluations, creating a trustless environment that incentivizes participation while preserving the integrity of the federated learning (FL) process. Smart contracts (SCs) verify and allocate rewards based on precise computational evaluations, creating a trustless environment that incentivizes participation while preserving the integrity of the federated learning (FL) process [26], [27]. In contrast, private blockchains often rely on a trusted setup, where the orchestrator is responsible for issuing rewards and may collude with the model owner or other stakeholders, potentially acting maliciously. This lack of transparency creates vulnerabilities, particularly in traditional federated learning (FL) systems, where there are limited incentives for clients to honestly follow the protocol and provide reliable data. Malicious participants can exploit the system to steal rewards or undermine the training process [32].

As a result, several prior works have emerged, such as 2CP by Cai et al. (2020) and Blockflow by Mugunthan et al. (2020), which outline procedures for measuring participants' contributions in a decentralized crowdsourcing protocol. 2CP employs Substra for step-by-step evaluation [30], [33], while Blockflow evaluates overall scores based on the median score reported for each model and the inverse of the maximum difference between reported and median scores [34]. For instance, BlockFlow (2020) demonstrated an average absolute difference of less than 0.67% between evaluators' scores across various limited numbers of agents (1, 25, 50, and 100) using income data. However, these frameworks are limited to small numbers of participants, as they were designed to mimic their real-world centralized counterparts. They do not address the scalability needed for larger participant pools, nor do they provide the necessary security guarantees for issuing rewards while maintaining decentralization and scalability [33], [30], [34]. Both BlockFlow (2020) and 2CP (2020) implemented a 1:1 ratio of evaluators to participants, with each participant evaluating every other participant's score [30, p. 2], [33]. Both of these frameworks assume all Participants must act as evaluators in the rewards process, which is not scalable as costs rise asymptotically with the number of Participants [30]. For example, with 100 Participants, all would need to download and evaluate the models of the other N - 1 Participants.

Unlike previous works such as BlockFlow (2020) and 2CP (2020), which do not fully address scalability in reward distribution, *DIN* is designed to ensure scalable and decentralized reward issuance. The proposed architecture leverages a public blockchain to enable a **trustless** process for reward distribution, eliminating the need for third-party intermediaries [27], [32]. Smart contracts (SC) handle key tasks, and can resolve disputes during model validation within Evaluator subgroups, coordinating protocol interactions, and ensuring smooth operation across the network.

DIN framework integrates two key contributions to enhance scalability and efficiency:

1. **Role Delineation**: The framework introduces a clear separation of roles in the evaluation process by delineating them into two distinct categories, thereby introducing a new entity to the process: Participant and Evaluator. In this setup, the Evaluator is specifically assigned the task of evaluation, while the Participant primarily acts as a decentralized data holder. This role separation allows for task specialization and ensures that not all Participants are required to participate in evaluations, facilitating scalability.
2. **Evaluator-to-Participant Ratio**: Inspired by BlockFlow's (2020) recommendations, the DIN framework integrates a ratio of Evaluators to Participants to perform evaluations. Evaluators are randomly selected ($Q \ll N$) to assess Participants' work within each subgroup FL aggregator group each round. For example, in an aggregator group with 100 Participants, 10 Evaluators might be assigned. This ratio is dynamically tied to the structure of the aggregator subgroup processes, adapting as the number of participants and the configuration of the FL system evolve. While a sufficiently large number of Evaluators is theoretically expected to improve accuracy and resist potential manipulation, the exact effectiveness of this ratio in ensuring accurate results and maintaining resilience against a majority of malicious agents ($M < N/2$) will need to be validated through empirical testing [30]. This integration supports scaling across increasing FL rounds, ensuring both robustness and efficiency [30].

These integrated aspects collectively address the challenges of scalability and task specialization in the federated learning process, enhancing the overall effectiveness of the *DIN* framework.

3.4.1 Ensuring Secure and Scalable Evaluation in DIN

In previous decentralized crowdsourcing protocols, such as 2CP and BlockFlow, participants were responsible for benchmarking each other's models using their own datasets by downloading, evaluating, and publishing scores themselves [30], [33]. However, this approach is not scalable, especially when considering network adaptability and the willingness and capability of participants to reliably maintain connections around the clock. In contrast, *DIN* improves upon this by clearly delineating the roles of Evaluators and Participants.

To effectively benchmark model updates and evaluate performance, *DIN* proposes that the Model Owner publish a test dataset. This dataset allows Evaluators to assess Participant models and enables the Model Owner to track progress throughout the training process, ensuring satisfaction with the results. Previously, participants used local datasets for this purpose.

To mitigate this risk, secure evaluation mechanisms must be implemented to ensure the test dataset remains concealed from Evaluators, preventing leakage to Participants who could unfairly train on it and manipulate their results. While Mugunthan (2020) in BlockFlow proposed scoring procedures that penalize extreme scores and use a median scale, these alone cannot

address all scenarios. We propose that the Model Owner upload an encrypted test dataset to IPFS for Evaluators to securely retrieve and use for benchmarking. Evaluators apply contributivity scoring procedures, such as 2CP's Substra or BlockFlow's median scoring, to assess performance accurately [30], [33]. To further enhance security and privacy, the auditing process enables Evaluators to use privacy-preserving computations like homomorphic encryption and Zero-Knowledge Proofs (ZK-proofs), allowing participants to validate their computations without revealing underlying data [35], [36]. These procedures are detailed in **Section 5.2, Decentralized Auditing Protocol.**

While DIN focuses on the architecture of the system, future experiments should explore how the network behaves with a larger ratio of Participants to Evaluators, as this may vary depending on the data type being trained on. Additionally, validating the protocol across heterogeneous data sources is crucial, with subgroups requiring stress testing to confirm their effectiveness and scalability. This decentralized approach, executed on a public blockchain consensus, prevents any single entity from manipulating the reward distribution, thereby maintaining trust in the system. Furthermore, while this paper assumes a steady-state system with fixed numbers of Participants and Evaluators per aggregator subgroup per FL round, future research will need to focus on experimenting with the dynamic nature of networks.

4 Proposed Solution: Systems Architecture and Overview

Decentralized Intelligence Network (DIN) offers a framework for decentralized, AI-driven ecosystems that enables scalable AI development while preserving ownership and privacy. Focused on smaller, distributed models running on consumer hardware, *DIN* prioritizes privacy-preserving approaches to AI.

Using smart contracts (SC), *DIN* coordinates AI training and rewards participation, while enabling Evaluators to assess contributions within a secure, proof-of-stake ecosystem. This decentralized structure ensures scalable training and fosters technological progress, all while maintaining control over data.

The framework aligns with the requirements detailed in **Section 2**, ensuring that no single authority controls the federated learning (FL) process. Only model updates, not raw data, are transferred out of decentralized data stores, preserving user privacy.

By integrating federated learning (FL) with a trustless rewards mechanism, this paper proposes a solution that enables collaborative, large-scale AI advancements, while ensuring data decentralization, privacy, and fair rewards for **on-device** and **edge computing** participation in FL protocols

A critical component of the frameworks approach is ensuring that FL protocols can effectively leverage data from numerous decentralized data stores while maintaining data ownership. As the number of decentralized data participants increase, FL protocols must scale accordingly, presenting new challenges in designing systems that can accommodate a larger and more diverse network of contributors.

Equally important is the implementation of a **scalable and decentralized reward system** that aligns with FL principles. This system acknowledges participants' contributions by recognizing both their data and computational resources, while ensuring transparency and fairness without centralized control.

By integrating federated learning (FL) with a trustless rewards mechanism, this paper proposes a solution that enables collaborative, large-scale AI advancements, while ensuring data decentralization, privacy, and fair rewards for on-device and edge computing participation in FL protocols.

The proposed framework consists of three key elements:

- 1) Decentralized data stores to ensure decentralized data ownership.
- A scalable federated learning (FL) protocol coordinated on a public blockchain for decentralized AI training, leveraging both on-device and edge computing resources.
- 3) A trustless rewards system to incentivize participation and ensure fair reward distribution.

DIN is designed to facilitate the transition to decentralized data stores, while acknowledging that institutional silos may continue to operate as single-identity entities. During this period of coexistence, these institutional architectures can still contribute to the federated learning (FL) protocol, utilizing their data for AI development. *DIN* can act as a catalyst for this transition, enabling institutions to participate while promoting decentralized data utilization through on-device or edge computing.

Decentralized data stores, in isolation, often lack the intrinsic value needed for large-scale utilization, as they are typically underappreciated or constrained by traditional business models dominated by centralized entities. These large-scale companies have the resources to acquire, aggregate, and monetize data at scale. ***DIN***, however, unlocks the latent value of decentralized data by creating new economic opportunities for its monetization. It fosters circular economies and enables decentralized data to be leveraged in ways that were previously only possible within centralized systems, opening up new avenues for innovation and collaboration.

By prioritizing models that can operate on consumer devices and other smaller scale computing resources, *DIN* aims to avoid a privacy and centralized-control dystopia where AI relies solely on centralized servers and siloed data. In such a scenario, server operators could monitor all actions and shape AI outputs according to their biases in ways participants cannot escape. Instead, *DIN*'s approach empowers individual users, allowing them to leverage AI capabilities while maintaining control over their data and reducing reliance on centralized infrastructure.

Key participants in this system include:

- **Participants:** Decentralized data owners who own and control their data stores, contributing data to the FL process while maintaining privacy and benefiting from collaborative AI training.
- **Model Owners:** Entities such as companies or researchers that utilize the FL protocols to enhance their models with decentralized data, without compromising data decentralization.
- **Evaluators:** Network-staked entities are responsible for decentralized aggregation, rewards evaluation, and auditing, ensuring secure aggregation processes, as well as transparency and fairness in evaluating participant contributions and distributing rewards.

This decentralization-integrative strategy contrasts with acceleration-reductionist approaches that emphasize ever-larger models and computing clusters. *DIN* prioritizes a vision of AI development that mitigates privacy risks and centralized control associated with large, server-based models. By leveraging consumer hardware, this approach aims to create AI systems that function more as practical tools with defined limitations, potentially offering significant advantages in terms of AI safety, control, and both individual and collective empowerment.

In summary, this paper presents a novel approach to addressing the challenges of decentralized data, AI development, and privacy in the current digital landscape. By leveraging decentralized data stores, federated learning, and blockchain technology, the proposed framework offers a path towards a more equitable, secure, and efficient data ecosystem that respects individual rights while fostering innovation in AI.

5. Methodology

5.1 *Decentralized Intelligence Network* (*DIN*) Protocol

Decentralized Intelligence Network's (*DIN*) protocol operationalizes the federated learning (FL) architecture outlined in **Section 4**. Built on a decentralized public blockchain infrastructure, the *DIN* protocol orchestrates the aggregation, coordination, and rewards process for training AI models using data stored in Participant-owned decentralized data stores. This approach ensures data decentralization while enabling scalable AI development.

Participants opt into federated learning (FL) protocols defined by smart contracts (SC) on a public blockchain, ensuring no entity or authority can block participation. This allows participants to operationalize and monetize their data stores, contributing to AI training while the protocol remains on an immutable, publicly accessible ledger. The blockchain coordinates the FL process and manages rewards, while raw data stays within the participant's datastore. Only model updates are shared during the FL process, preserving privacy and control.

To enhance scalability and computational efficiency, the *DIN* protocol incorporates an off-chain decentralized file storage system, such as the InterPlanetary File System (IPFS) [37]. This system provides a location for uploading and downloading model updates during the learning process, optimizing participation costs and complementing the blockchain's transaction recording capabilities.

This setup ensures a fair and transparent reward system while maintaining data decentralization and reducing reliance on centralized infrastructure. The following sections detail the specific methodologies and operational mechanisms of the *DIN* protocol, including the roles of key participants such as Model Owners, Participants, and Evaluators.

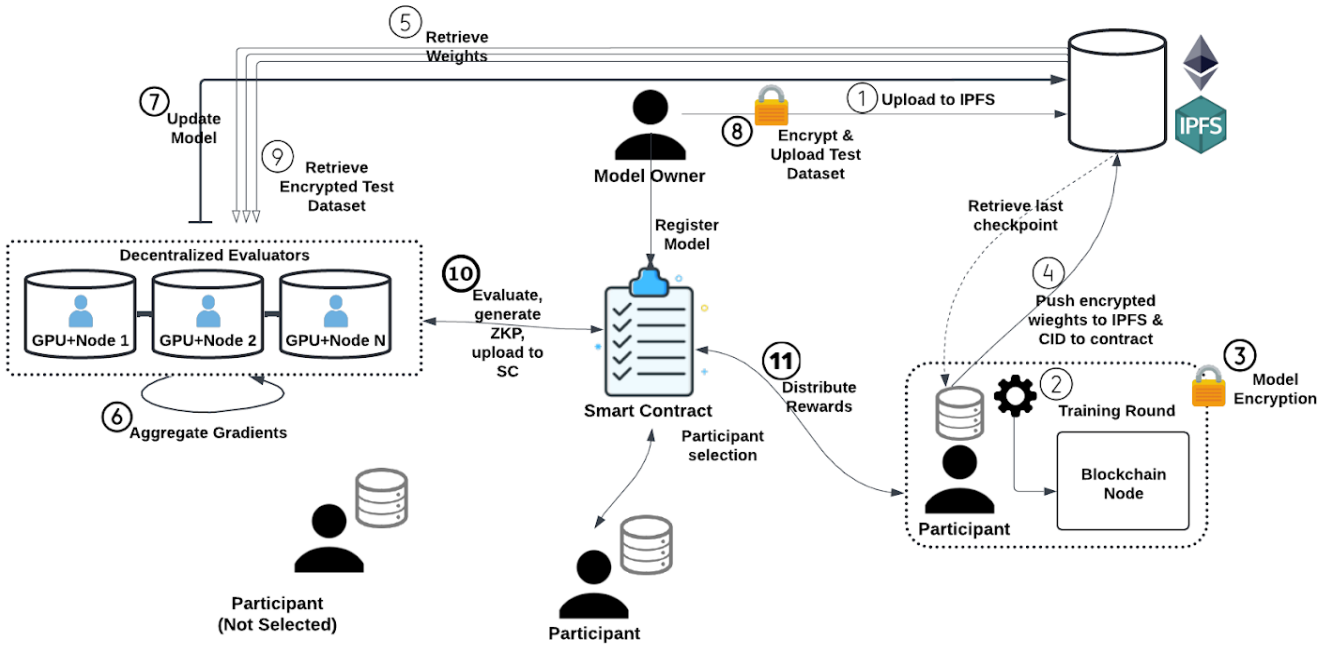

Figure 1. *Global overview of a training round.*

1. **Model Owner:** a. Deploys *intelligence* smart contracts (SC) on the blockchain. Although referred to as "*intelligence*," multiple contracts may work in unison on-chain, fulfilling different roles to enhance scalability and efficiency (e.g., *DIN* protocol, evaluator registry, evaluator staking, decentralized aggregation management, staking for evaluators, reward distribution, etc.). b. Creates genesis model, uploads to IPFS, records its CID on the contract. c. Deposits reward amount in smart contract (SC) to be allocated to Participants after FL rounds.
2. **Upon Model Owner's transaction confirmation:** a. Participants can see the genesis model CID and download it from IPFS. b. Using their own data stores, Participants run training iterations on model. c. Participants encrypt their models using secure aggregation protocol (e.g. Bonawitz et al. 2019) [5]. d. Participants upload their encrypted updated models to IPFS, recording CIDs on *intelligence SC*. e. This completes one FL training round; Participants wait for the next round.
3. a. **Decentralized Evaluators**: *DIN* utilizes **Evaluators** as decentralized nodes, each randomly selected and allocated into aggregator subgroups for scalable model aggregation. These Evaluators validate and aggregate model updates independently using their own GPU hardware, eliminating the need for a centralized aggregator server. The smart contract (SC) manages the overall coordination, ensuring that only validated aggregation results are accepted and final. b. **Secure Processing**: Evaluators fetch encrypted model weights from decentralized storage (e.g., IPFS) via **CIDs** recorded on the blockchain, ensuring secure processing. Each Evaluator aggregates their portion of the model using their own hardware, such as decentralized GPUs, and independently validates updates based on the agreed-upon protocol. c. **Scalability through Subgroups**: Scalability is achieved by decentralizing the aggregation process across multiple **Evaluator subgroups**, similar to the approach described in **Bonawitz et al. (2019)** [5], [31], where each subgroup is tasked with a subgroup of the aggregation of participants' model updates, thus enabling parallelization of

the aggregation process. Multiple Evaluators are assigned to each group to handle larger workloads while minimizing centralized dependencies, improving efficiency, and increasing the overall scalability of the system. d. **Security and Sybil Resistance**: Security is maintained through **Sybil resistance** and **majority consensus**. Each **aggregator subgroup** must reach agreement on the aggregated model updates. Evaluators within a subgroup must validate that the model updates, when summed, match the expected total. If the results do not match, a dispute is triggered. This ensures that only valid, accurate model updates are accepted. The consensus process requires that greater than 50% of the Evaluators in each subgroup agree on the final aggregated result, preventing malicious or fraudulent actions from influencing the outcome. e. **Dispute Resolution**: If there is a disagreement among Evaluators (i.e., they do not reach the same aggregate resulti i.e., off-chain on IPFS), an **on-chain dispute resolution** is triggered. Evaluators who fail to align with the majority consensus are **slashed**, losing their staked tokens and their ability to participate in future aggregation rounds, thus maintaining the integrity of the process. f. **Finalizing the Aggregated Model**: Once the results are confirmed on-chain, the aggregated global model is uploaded to shared storage. The **Model Owner** sums the individual subgroups' results to form the new global model. However, the final model must be consistent with the sum recorded by the on-chain **smart contract**, which tracks the aggregation across all subgroups. Participants can verify on-chain that the newly published global model matches the smart contract's sum of prior rounds, ensuring integrity and preventing any malicious actions by the Model Owner. This provides full transparency and ensures that the final aggregated model is both accurate and tamper-proof. g. **Multiple Aggregator Instances**: To further enhance **decentralization** and **resilience**, multiple instances of Evaluators and secure aggregation environments can be instantiated, enabling distributed computation, fault tolerance, and the ability to handle larger workloads across the network.

4. **Next Training Round:** a. A new global model is published by the Model Owner for the next training round. b. **Optional:** If occurring asynchronously, Participants can check all CIDs of the previous round's model updates in their aggregator subgroup. b. Download updates from IPFS and independently calculate the mean aggregate for their subgroup (all participants in a subgroup reach the same result). c. Each subgroup performs the average of their own subgroup's global model and then averages other aggregator groups' averages as published on IPFS located on-chain to reach global model published by Model Owner.
5. **Model Aggregation Continuation:** a. Evaluators continues to aggregate FL round updates, averaging their updates as rounds progress. b. The Model Owner can continue to test the average global model update against their test dataset to determine when they are satisfied with the training. c. The decision to end or continue training is communicated to the SCs either in advance or during training, depending on the Model Owner's availability of funds. d. The Model Owner signals the final round, after which one additional round occurs to evaluate Participants' rewards before the final global model is revealed to the Model Owner.
6. **Post-Training:** 6. a. The Model Owner encrypts the test dataset using Homomorphic Encryption (ensuring independent verifiability) and generates evaluation keys for Evaluators, then uploads both to IPFS with verification parameters stored in the smart contract. b. The *intelligence* SC utilizes the existing Evaluator-Participant assignments from the aggregation phase (maintaining the standardized 1:10 ratio) according to the Model Owner's needs, ensuring continuity of the established subgroups for evaluation [30]. c. Evaluators (with verified stake as confiemd on-chain), who are assigned to specific subgroup FL aggregation rounds for scalability, perform encrypted evaluations of all Participant models within their subgroups using the homomorphically encrypted test dataset, generating ZK-proofs to verify correct evaluation execution, proper dataset usage, and adherence to evaluation metrics - if disputes arise from conflicting results, the evaluation automatically moves to on-chain verification with additional oversight.
7. **Evaluators:** a. Anyone staking native token can be an Evaluator. b. Evaluate Participants' models against the encrypted test dataset using HE operations. c. Submit evaluation consensus scores with ZK-proofs to *intelligence* SC (see **2.3.1 Decentralized Auditing Protocol** for rewards). Evaluators receive fees for their aggregation and evaluation services to offset the computational cost and incentivise participation.
8. **Distribute Rewards:** a. *Intelligence* SC calculates reward fraction for each participant based on objective scores (e.g., as Shapley Values, Substra Scoring, Median Scoring, and other open-preference scoring methods); so long as maintains integrity of the network [30], [33], [38], [39], [40]. b. Distributes Model Owner's deposited reward accordingly, per recorded scores.

In the related works section, we briefly reference the protocol by Bonawitz et al. (2019), which employs synchronous rounds with subsets of devices for scalable federated learning. Their Secure Aggregation method ensures privacy by encrypting device updates, and intermediate results are aggregated by dedicated actors to manage computational costs. This framework builds on these principles, enhancing scalability and privacy while addressing decentralized participation. By integrating subgroup

aggregation and subset evaluation, we extend Bonawitz et al.'s approach to support decentralized networks and broader applications [41], [42].

To incentivize participation in this scalable and decentralized FL process, we propose integrating a scalable, "trustless" rewards mechanism—one that does not require a third party for transactions. This mechanism is discussed in the following section.

5.2 Decentralized Auditing Protocol

Delineating the roles of Participant and Evaluator in the protocol raises concerns about the potential misuse of the test dataset by Evaluators in federated learning (FL) scenarios.In previous examples, each participant evaluated the model updates of every other participant using the data stores they employed to train their own models [30], [33]. However, once we distinguish between Participant and Evaluator and adjust the protocol to scale and generalize to other data types, a new issue emerges. Evaluators might download and illicitly share the test dataset published by the Model Owner with participants in one or more aggregator subgroups during FL rounds, particularly when benchmarking participants' contributions after the Model Owner signals the final round of training. This risk is heightened in asynchronous FL processes, designed to maximize network flexibility in handling unstable participant connections, potentially leading to harmful activities such as model poisoning or unfair compensation during the training process.

To mitigate these risks, implementing secure evaluation mechanisms where the test dataset remains concealed from the Evaluators is essential. Evaluators can prove to the system they correctly evaluated against the test dataset without accessing it, mitigating risks of misuse or leakage. Evaluators can be provided with high-quality, well-distributed, and highly representative test datasets by the Model Owner. Evaluators can use this as a benchmark to evaluate each Participant's models as shown in **Figure 1**. The step-by-step protocol elaborates on the processes of Evaluators' involvement in the **decentralized auditing protocol** within the rewards process, as illustrated in **Figure 1**, as follows:

1. Model Owner preparation: a. Implements Homomorphic Encryption (HE) for the test dataset. b. Generates evaluation keys and verification parameters for Evaluators. c. Uploads encrypted test dataset to IPFS and records location CID on the *intelligence* SC.
2. Within decentralized Evaluator nodes: a. Evaluators compute performance metrics (such as accuracy, precision, and recall) on models using the encrypted test dataset and benchmark these metrics using objective scoring methods (e.g., Shapley Values of Distribution, Substra, Median Scoring, etc) [30], [33], [38], [39]. b. Evaluators perform computations on their own GPU hardware within their assigned aggregator groups. c. Evaluators generate Zero-Knowledge Proofs integrated with HE operations to prove evaluations were performed exactly as specified by the on-chain smart contract.
3. Privacy-Preserving Evaluation Process: a. Evaluators use HE operations to evaluate models on the encrypted test dataset. b. Evaluation processes run independently within each aggregator group.
4. Evaluators submit ZKPs and encrypted evaluations to blockchain *intelligence* SC.
5. *Intelligence* SC verifies ZKPs using a consensus mechanism (e.g., majority agreement).
6. Based on verified scores, *intelligence* SC calculates and distributes rewards transparently **(as seen in Figure 1)**.
7. All privacy-preserved transactions are recorded on the blockchain for an immutable audit trail.
8. Privacy-preserving techniques (HE operations) along with ZKPs provide multiple layers of security, where HE conceals data and ZKPs verify correctness without revealing information.
9. Protocol protects against insider threats through encrypted evaluation and exporting only ZKPs.
10. Final Global Model Update: a. Model Owner signals end of training process upon satisfaction with model performance. b. Final Global Model update revealed to Model Owner after completion of rewards process.

DIN introduces a flexible architecture and a comprehensive model that enables Owners to experiment with and implement various contributivity scoring methodologies tailored to their specific needs. This system empowers Evaluators to perform detailed off-chain assessments of Participants' contributions, which are subsequently confirmed and securely recorded on-chain, ensuring transparency, accuracy, and immutability.

This protocol ensures secure and reliable model evaluations through a fully decentralized process, utilizing privacy-preserving techniques. The evaluations are conducted in a manner that prevents interference or manipulation, as outlined in the threat model

(see Section 6). The protocol aligns with the incentives of Model Owners, who, despite covering the costs of network fees paid to Evaluators, benefit from robust data contributions and trustworthy evaluation processes that are essential for model training and improvement. These processes are transparently priced using objective, pre-defined metrics.

Importantly, the protocol preserves data decentralization for Participants—no central authority controls access to their data, which remains stored in its original location. This ensures that Model Owners, seeking data to train their AI models, are not restricted by third-party paywalls or limited to data that has been selectively acquired by centralized entities (often incomplete or biased). Instead, they have access to a broader and more diverse set of data, without relying on intermediaries that might impose restrictions or distortions. Furthermore, rewards for Participants are determined in a decentralized manner by a public blockchain smart contract, based on auditable and transparent criteria. This eliminates the need for a central authority to decide compensation, mitigating risks such as dishonest aggregation or external attacks. The protocol thus ensures scalability while addressing the challenges of centralized systems, as demonstrated in Bonawitz et al. (2019), by leveraging the immutable nature of the blockchain and decentralized validation[5].

This decentralized auditing protocol maintains Participants' autonomy while enabling secure, reliable, and incentive-aligned model evaluations. It addresses the challenges of decentralized participation within a novel framework, enabling wider application of these tools and workflows within decentralized networks.

6. Threat Model

The papers threat model addresses potential risks in the federated learning (FL) process, ensuring robust security and privacy. The protocol is resilient to up to 50% malicious participants, leveraging public/private key cryptography and a proof-of-stake consensus mechanism. By using immutable storage on IPFS we ensure data integrity. Additionally, the use of Zero-Knowledge Proofs (ZKPs) and privacy-preserving techniques such as homomorphic encryption (HE) mitigates risks associated with model evaluation and reward distribution. This comprehensive approach ensures the security and reliability of the FL process, maintaining trustlessness and data decentralization.

Firstly, in an experiment with N agents, it is resistant up to $M \in [0, N/2)$ agents neglecting to follow the protocol for the experiment to maintain its integrity [30]. For example, public/private key cryptography and a proof-of-stake consensus protocol secure the Ethereum blockchain. Currently, there are no feasible attacks on the Ethereum Network, without controlling 50% of the computational power of the entire Ethereum network and such an attack has never been successful on the Ethereum mainnet [43].

Secondly, as a public blockchain is public and anonymous, clients could enroll multiple times in an experiment and thus have a disproportionate participation. However, through decentralized identity verification, verifiable credentialing, or manual processes, agents can ensure that each other agent controls only one account [19], [20], [44].

Third, IPFS is immutable, meaning agents cannot change their model after submitting the cryptographic hash to the smart contract [37]. Like in BlockFlow, the *DIN* protocol requires each agent to report if it can load strictly more than N/2 models, and have strictly more than N/2 agents report the same for their model. The *DIN* threat model guarantees that there are strictly more than N/2 honest Participants. Additionally, as long as N/2 or more Evaluators who receive these models for evaluation are honest, which the *DIN* protocol guarantees, the system remains resistant to N/2 attacks. Since IPFS allows anyone to share any content, one or more honest parties would share the model with all other Participants if they are unable to retrieve a model directly from the source (e.g., due to firewall restrictions). Therefore, each Participant would still be able to obtain all necessary models [30], [37].

Fourth, there are several possible attacks on the contribution scoring procedure itself. Malicious models are those with weights that do not reflect a truthful dataset, such as models trained on randomly generated data or inverted output features. Naively averaging such models into a global model would likely harm the shared objective. The *DIN* protocol can choose contribution-scoring procedures that penalize those who submit malicious models. For instance, BlockFlow (2020) uses a contributivity score system where lower scores result in less cryptocurrency received [30], [37]. In this system, any agent with an evaluation more than 0.5 away from the median score receives an overall score of 0 and no share of the cryptocurrency pool [30],

[37]. This penalizes attempts to fabricate scores, as the protocol limits a Participant's overall score to the evaluation furthest from the median [30], [37].

Fifth, Participants can collude during the training process to submit better models by secretly sharing raw data or models among M<N2 colluding Participants [30], [37]. The *DIN* protocol rewards Participants who contribute strong models, and it is acceptable for multiple Participants to submit identical models. Such collusion is not considered an attack, as it is similar to having many Participants with strong datasets [30], [37]. For attacks by Evaluators in the evaluation process, the I smart contract can use encryption and a commit-then-reveal protocol (e.g., Secret Sharing MPC, Elliptic Curve Diffie-Hellman keys, etc.) to prevent Evaluators from copying others' scores without collusion [45]. If a minority subset of malicious Evaluators reports perfect 1.0 scores for certain models and 0.0 scores for all others (e.g., models from honest agents), the median score is guaranteed to be between the minimum and maximum scores reported by the honest agents, as long as there are strictly fewer than half malicious Evaluators [30], [37]. Evaluators are incentivized to stake an NFT (non-fungible token) to gain the right to evaluate participant models in the rewards process within a proof-of-stake (PoS) ecosystem. This staking mechanism involves the use of a native NFT token standard. The system operates as a self-assessed value framework, incorporating Harberger taxation, proceeds of which fund public good systems. Evaluators found acting maliciously are slashed from the network, losing some or all of their stake, thus maintaining network security and incentivizing honest work.

Sixth, in this papers threat model, it is crucial that the test dataset provided by the Model Owner remains encrypted to prevent its misuse. If the test dataset were accessible to colluding Participants, Model Owners, Evaluators, or other entities, they could exploit it to skew the reward distribution. For example, colluding parties could use the test dataset to strategically improve their model performance or manipulate evaluation outcomes to gain undeserved rewards. Encrypting the test dataset ensures that it cannot be revealed or utilized by these entities to unfairly influence the results. To enhance security further, dual protection strategies can be employed. For instance, the preferred scoring method, such as median scoring used by BlockFlow (2020), can be integrated into the protocol [30]. In this approach, any score deviating significantly from the median—beyond a specified threshold—can be penalized. BlockFlow's method maps any score differing by more than 0.5 from the model's median to a score of 0, with an a priori score set at 0.5 [30]. This mechanism encourages evaluators to provide honest assessments by penalizing scores that deviate substantially from the median. This method helps mitigate the risk of anomalous scores due to collusion and maintains fairness in the reward distribution process. Overall, encrypting the test dataset and employing robust scoring mechanisms collectively safeguard the integrity of the evaluation process and prevent potential manipulation by malicious actors.

Seventh, Evaluators could compromise fairness by selectively sharing test data with participants. To prevent this, the model owner encrypts test data and verifies it on-chain, with Evaluators gaining access only after completing training and depositing rewards. *DIN* can employ two approaches for privacy and verification, preferentially using Homomorphic Encryption (HE) with Zero-Knowledge Proofs (ZKPs). HE enables computation on encrypted data, while ZKPs verify computation correctness without revealing data. This method proves more efficient for individual Evaluators and smaller datasets, with trust established through cryptographic proofs and smart contracts validating encrypted evaluations. Costs are managed through dynamic training fees. Multi-Party Computation (MPC) serves as an alternative, splitting data across multiple Evaluators for collaborative computation without full dataset exposure. While MPC effectively distributes trust across Evaluators with results verified post-collaboration, it demands more computational resources than the HE and ZKPs approach. Security is maintained through encryption, access controls, security audits, and smart contract verification [46].

7. DIN Applications

Decentralized Intelligence Network (*DIN*) offers a scalable and versatile framework for learning from decentralized data stores, supported by a reward system designed to boost participation. This paper lays the groundwork for future research on decentralized services, aiming to leverage sovereign data stores for innovative algorithm development.

- **Healthcare:** In healthcare, patients store their health data in self-sovereign decentralized data stores, allowing them to retain full control over access and sharing of their data. Medical researchers and healthcare providers can access the federated learning (FL) protocol on-chain to train AI models, using this data to enhance diagnostics and treatment plans, all while ensuring that the raw data is never exposed. This model enables patients to be financially rewarded for contributing their data to medical research, with the option to use these rewards to offset insurance premiums, making healthcare more accessible and aligned with patient-driven incentives.

- **DeFinance:** Financial data is stored in decentralized data stores, ensuring that users maintain control over their transaction data. Financial institutions and service providers can leverage the FL protocol on-chain to offer personalized financial advice and develop innovative financial products based on aggregated, anonymized insights. By participating in this ecosystem, users benefit from a transparent and incentive-aligned financial system. They can also earn rewards for sharing their data in this way, further incentivizing participation and enhancing the integrity of financial systems.

- **EdTech:** Educational institutions store academic records, learning progress, and other relevant data in decentralized data stores. These data repositories allow educational institutions to use the FL protocol on-chain to tailor learning experiences, offer personalized support, and improve educational outcomes, all without ever needing to access the raw data itself. Schools can participate in this decentralized system by allowing their data to contribute to educational research, with the potential to earn rewards that can help offset educational costs and reinvest in their institution's infrastructure.

- **Smart Cities:** Residents' data related to energy consumption, transportation patterns, and other metrics are stored in decentralized data stores across smart cities. City planners and utility providers can access the FL protocol on-chain to optimize urban services and infrastructure, improving city planning without compromising the privacy of individuals' raw data. In this model, residents can receive rewards for contributing their data to enhance the sustainability and efficiency of the urban environment. These rewards can be used to support various living costs, thus improving the overall quality of life for the broader community.

- **Smart Agriculture:** In the agricultural sector, data on crop yields, soil conditions, and weather patterns are stored in decentralized data stores managed by farmers and agricultural organizations. Researchers and agricultural companies can use the FL protocol on-chain to develop better farming practices, new technologies, and optimize crop yields. Farmers maintain control over their data and can earn rewards for their contributions, fostering innovation and sustainable agricultural practices. These rewards can be reinvested into areas like crop insurance or local ecosystem initiatives, supporting the continued growth and sustainability of the agricultural sector.

These use cases emphasize the use of decentralized data management and federated learning protocols to ensure privacy while allowing industries to leverage valuable insights for enhancing their services.

8. Tokenomics, Governance, and Public Goods

This section elaborates on the protocol designed to incentivize and manage participation within a *Decentralized Intelligence Network (DIN)*. It integrates economic and social dimensions into modern systems architecture, emphasizing tangible incentives and broader systems design—an approach aligned with early internet pioneers and recent literature [47].

The protocol adopts a standard Proof of Stake (PoS) mechanism, utilizing a native ERC-20 token to ensure sybil resistance and secure the network, with malicious actors subject to slashing. Evaluators are granted permissions to aggregate and evaluate contributions within the network, based on their confirmed stake. In return, they earn network fees, which can be paid in stablecoins or the local currency of the employed network, aligning incentives and ensuring flexibility in compensation.

Model Owners may be required to stake a percentage of the native token (e.g., 5% of the total predicted cost of AI training) in order to gain access rights to the network. This staking requirement further enhances the utility of the token within the ecosystem. The token distribution follows established patterns, allocating portions to founders, the foundation, and other stakeholders, in a manner similar to Ethereum's distribution model.

Alternatively, the protocol can incorporate a novel public goods funding mechanism that not only secures the network but also integrates seamlessly with existing public goods ecosystems. It leverages NFT staking, unique evaluation mechanisms, and principles of Partial Common Ownership (PCO) to foster a circular economy for the development and enhancement of global AI models. While the staking mechanism is central to the protocol, it does not necessarily require a native token or coin, though the potential for such integration could be explored.

NFT Proof of Stake (PoS) Mechanism for Evaluators (Optional): This component explores the novel application of combining innovative evaluation mechanisms and staking methods with Harberger taxation and PCO principles. It focuses on

using NFT staking to secure the network and aims to establish standard, open-source implementations of Partial Common Ownership (PCO) of Ethereum ERC721 NFTs [48], [49]. By integrating these methods with Harberger taxation, this approach not only strengthens network security but also seeks to contribute revenue to public goods ecosystems, potentially enabling self-funding development of the *DIN* and other adjacent public goods ecosystems [49]. Core components of the staking mechanism are detailed:

- **Network Fees**
  - The Model Owner, who trains the algorithm and pays Participants for the Federated Learning (FL) process on decentralized data stores, is assumed to pay this fee as part of the process.
  - **The fee distribution from rewards to participants and evaluators is dynamic and remains an open question.** It could be either an added tax on the reward or a distribution model, such as allocating 97% of the reward to participants and 3% to evaluators.
  - This fee is separate from and in addition to any blockchain-specific gas costs, and is a part of the estimated costs of the rewards process.
  - The exact calculation and distribution method for this reward is an open question for experimentation.
- **Fee and Reward Currency**
  - Fees and rewards are primarily paid in a stablecoin (e.g., USDC, etc) however new stablecoin assets prevent value depreciation (e.g., RAI [50]) that is not pegged to centralized stablecoin assets are worth exploring.
  - This approach helps mitigate risks associated with inflationary measures or other external factors affecting centralized stablecoins, to fairly reward Participants.
  - The use of native tokens in lieu of stablecoins remains an open question for further exploration.
- **Evaluator Staking and NFTs**
  - Evaluators must stake an NFT to participate in evaluation processes i.e., to earn network fees.
  - These NFTs represent the Evaluator's stake and reputation in the network.
  - NFT values are self-assessed and based on the chosen stablecoin to ensure stability.
- **NFT Valuation and Taxation**
  - NFT values are subject to **Harberger taxation:**
    - Owners periodically self-assess their property and pay tax on its value.
    - Others are able to purchase the property from the owner at the taxed price at any time, forcing a sale [51].
  - Harberger taxation is priced in the fees paid to Evaluators (i.e., stablecoin, native token,etc) and is charged periodically based on the value of the owner's NFT asset.
  - Values can be adjusted either:
    a) Dynamically based on performance, or
    b) At set periods, after which they become open to auction (PCO mechanism).
- **Evaluator Incentive Structure**
  - As Evaluators perform more work, they:
    a) Receive more rewards from fees.
    b) Can assess their NFT stake at a higher value, as the profits from fees exceed the amount taxed.
  - This structure incentivizes high-quality evaluations and active participation [51].
- **Partial Common Ownership (PCO)**
  - Implements a mechanism where NFTs can be put up for auction after certain periods or at all times.
  - Helps maintain fair valuation and prevents monopolistic behavior; setting non-speculative asset pricing which reflects work done in the network.

This protocol aims to create a balanced, fair, and efficient system for decentralized machine learning model evaluation and improvement. It is also a novel proposal for the implementation of a public goods funding mechanism. By leveraging economic incentives and novel ownership structures, the protocol aligns the interests of all participants towards the common goal of advancing AI capabilities, while simultaneously contributing to the funding of public goods. It addresses potential challenges and areas for further refinement, ensuring a sustainable and equitable ecosystem for all involved. Alternatively, it considers leveraging existing ERC standards or exploring other traditional staking protocols—such as those used with a native coins—that do not aim to become part of a public goods ecosystem to meet the wider protocol requirements [49].

Public Goods & Governance in *DIN*: Projects like Gitcoin funding vision for community-driven proposals and public goods funding highlight the increasing focus on supporting shared resources and communal benefits [52], [53]. The proceeds from the taxation mechanism within our protocol are **allocated towards funding *DINs* open-source public goods infrastructure like or broader ecosystems**. This could involve supporting the network's own public goods or contributing to initiatives such as Gitcoin grants. **These approaches align with principles embraced by communities such as RadicalxChange (RxC), the Plurality Book, Ethereum blockchain ecosystems, and the Kernel Community. They also reflect the values of RDI Berkeley in DeAI, which emphasize openness, responsibility, and a democratized AI economy.** By integrating transparent, community-driven mechanisms and decentralized models, these approaches promote equitable participation and resource distribution [51], [54], [55], [56], [57]. Their work underscores the need for **ongoing experimentation and a willingness to explore new ideas**, crucial for developing transparent systems that benefit the public.

DIN is an organizational network and public goods software by design, though its applications extend beyond the realm of public goods. It emphasizes leveraging decentralization and may explore governance mechanisms to keep engaged, incorporating models such as Gov4Git (non-coin-based voting) and quadratic voting tools to engage contributors [58]. The concepts of decentraliztion are… as it delves into decentralized governance, commons-based peer production, and digital communities with shared values that operate independently of traditional structures. Network societies explore the potential for decentralized models to reshape governance and resource distribution in novel ways, and may also contain relevance to experimental network societies [59].

DIN may include **DPPs** (*DIN* Proposal Protocols) for drawing attention to proposals for improving the network. These proposals will be voted upon by contributors who are allotted non-coin voting credits, employing tools akin to those or including Gov4Git [58]. A flexible, inclusive rollout driven by community input is essential to mitigate wealth concentration within the crypto ecosystems. Circulating financial value within ecosystems that benefit the public can stimulate economically advantageous societies. This approach, coupled with a commitment to continuous innovation, is vital for advancing these concepts in dynamic and impactful ways.

9. Miscellaneous & Concerns

Smaller Models: Smaller, more efficient models are essential for improving performance, particularly in decentralized networks where participants may have limited computational resources. By optimizing the size and complexity of models, the system can enhance inclusivity, enabling more participants to engage without requiring expensive hardware or substantial bandwidth. This approach ensures faster training and inference, allowing participants with constrained resources to contribute effectively and access results in a timely manner.

Cost of Advanced Privacy Techniques: While privacy-enhancing techniques like Zero-Knowledge Proofs (ZK-proofs), Homomorphic Encryption (HE), and Multi-Party Computation (MPC) are crucial for protecting sensitive data during training, they are also resource-intensive and can lead to network lag. Although network fees can help offset the costs of these methods, DIN aims to optimize its protocols to reduce both fees and latency. By refining algorithms and improving efficiency, DIN strives to make advanced privacy techniques more practical and scalable without sacrificing security or performance.

Open-Source Models: Open-source transparency fosters collaboration and accountability, but it also brings the risk of manipulation or overfitting when malicious actors gain access to critical datasets or model parameters. To mitigate these risks, DIN incorporates safeguards, such as restricting access to sensitive test datasets or using techniques like differential privacy. These precautions ensure that open-source models remain robust, transparent, and free from exploitation, while maintaining high levels of trust and integrity in the system.

Network Latency: One of the inherent challenges of decentralized networks is the potential for network latency, which can arise from the need for coordination among distributed nodes. This delay can negatively impact the timeliness of model training and evaluation. To minimize latency, DIN implements strategies like hierarchical aggregation and localized evaluation within smaller subgroups. These approaches reduce the distance data must travel and improve processing speeds, especially for participants in regions with slower internet connections, ensuring smoother operations across the network.

Poisoning Attacks: Poisoning attacks—where malicious actors inject false data or misleading models into the system—can severely undermine the integrity of decentralized training processes. To protect against these threats, DIN employs robust scoring mechanisms, such as blockflow-based median scoring, which helps identify and neutralize the effects of outliers or malicious inputs. By using decentralized validation methods and anomaly detection, DIN ensures that contributions are evaluated fairly and accurately, reducing the likelihood of successful poisoning attacks.

50% Attacks and Proof-of-Stake Security: DIN's Proof-of-Stake (PoS) mechanism provides resistance to 50%+ attacks, ensuring the network's security. Malicious actors are financially incentivized to act honestly, as any attempt to compromise the system could result in the loss of their staked tokens through slashing. While PoS offers a strong foundation for securing the network, continuous monitoring and upgrades are necessary to address emerging threats and vulnerabilities. Ongoing research into PoS and network security will ensure DIN's resilience as the ecosystem grows and evolves.

Steady-State Evaluator/Participant Ratios: This paper assumes a steady-state system with fixed numbers of Participants and Evaluators per aggregator subgroup for each Federated Learning (FL) round. However, as the decentralized network evolves, it will be important to consider the dynamic nature of these interactions. Future research should explore how fluctuations in the number of participants and evaluators, as well as changing network conditions, impact system performance. Adapting evaluator-participant ratios in response to these dynamics will be crucial for optimizing efficiency, minimizing bottlenecks, and ensuring scalability as the network grows.

10. Conclusion & Future Works

Decentralized Intelligence Network (DIN) is a theoretical framework designed to address challenges in AI development and deployment, particularly focusing on data fragmentation and siloing issues. Its core objective is to enable scalable AI through decentralized data stores while facilitating effective AI utilization within such decentralized networks. DIN represents a significant advancement in integrating key themes of:

- Decentralized Data
- Public blockchain
- Decentralized federated learning (FL)
- Off-chain file storage (e.g., IPFS)
- Decentralized Reward Protocols

By introducing a decentralized FL protocol within a decentralized data architecture, DIN enables Participants to retain ownership and control over their data while receiving rewards for its use. This scalable framework addresses the limitations of siloed data, benefiting both participants and data users, and includes a robust, decentralized auditing system for equitable reward distribution, without third party - maintaining our requirements.

Potential Benefits:

- **Enhanced AI Performance:** Access to more diverse data can lead to more robust and capable AI systems.
- **Improved Data Utilization:** Allows for more effective use of existing data sources that may currently be underutilized due to fragmentation or siloing.
- **Preserved Privacy and Control:** Maintains decentralized data stores while still enabling collaborative AI development.
- **Scalable Solutions:** Provides a framework for AI systems to grow and adapt as more data sources become available.
- **Future of an open, responsible AI economy**: AI agents automate tasks, giving humans more time to be human. The value produced by the AI economy lifts the standard of living for everyone, with safe applications of AI enabling scientific discovery and real-world sector applications, leading to a post-scarcity society.

DIN can potentially change how AI is developed and deployed, especially in scenarios where data privacy, decentralization of data, and diverse data access are crucial factors. It's important to note that *DIN* is a systems architecture for a network and does not address other subsections of Decentralized AI (DecAI). Institutional leverage of data whilst preserving interests (move beyond private setups, preventing need for collaboration, enabling wider monetization strategies whilst preserving privacy). New

economic models for tokenized systems with circular economies, with specific use case applications cross-sector inc. but not limited to finance, smart cities, healthtech, education, and more. Both decentralized and traditional institutions may benefit from this technology.

Future Works: While there are challenges associated with implementation, technological advancements provide a strong foundation for ongoing development. Future enhancements to DIN may involve:

- Expanding interactions with decentralized data stores
- Integrating more advanced, computationally efficient privacy-preserving techniques
- Addressing implementation complexities
- Optimizing performance trade-offs
- Improving scalability issues

These advancements will be crucial in continuing to evolve decentralized FL frameworks effectively.

Call To Action: *DIN* encourages researchers, practitioners, and stakeholders to engage with this framework to promote data ownership and decentralization. Collaborative efforts can lead to scalable, decentralization data solutions that advance technology while respecting individual data rights.

By working together, we can overcome the challenges associated with decentralized intelligence networks and create a future where AI development is both powerful and respectful of individual privacy and data ownership.

11. Acknowledgments

Special thanks to Paritosh Ramanan, Rui Zhao, Harry Cai, Peng "Dana" Zhang, and Jesse Wright for their invaluable discussions on many of these ideas. Specifically, their contributions include scalable FL architectures (Paritosh), scalable decentralized auditing protocol (Paritosh, Harry), decentralizaed architectures, and decentralized identity management (Dana). Special thanks to Rui and Jesse, who provided significant insights across various aspects of the framework. Their insights and contributions have significantly shaped the development of this framework. Additionally, these works have been selected for presentation as a speaker at the **Summit on Responsible Decentralized Intelligence - Future of Decentralization and AI**, hosted by **Berkeley RDI** on **August 6, 2024**, at the **Verizon Center, Cornell Tech Campus, Roosevelt Island, NYC**. This summit offers an exciting opportunity to share and further refine these ideas with a broader audience.

References

[1] "The birth of the Web | CERN." Accessed: Jun. 22, 2024. [Online]. Available: https://home.cern/science/computing/birth-web

[2] A. K. Goel, R. Bakshi, and K. K. Agrawal, "Web 3.0 and Decentralized Applications," *Materials Proceedings*, vol. 10, no. 1, Art. no. 1, 2022, doi: 10.3390/materproc2022010008.

[3] M. Van Kleek and K. OHara, "The Future of Social Is Personal: The Potential of the Personal Data Store," in *Social Collective Intelligence: Combining the Powers of Humans and Machines to Build a Smarter Society*, D. Miorandi, V. Maltese, M. Rovatsos, A. Nijholt, and J. Stewart, Eds., in Computational Social Sciences. , Cham: Springer International Publishing, 2014, pp. 125–158. doi: 10.1007/978-3-319-08681-1_7.

[4] R. Zhao *et al.*, "Libertas: Privacy-Preserving Computation for Decentralised Personal Data Stores," Sep. 28, 2023, *arXiv*: arXiv:2309.16365. doi: 10.48550/arXiv.2309.16365.

[5] K. Bonawitz *et al.*, "Towards Federated Learning at Scale: System Design," Mar. 22, 2019, *arXiv*: arXiv:1902.01046. Accessed: Jul. 29, 2024. [Online]. Available: http://arxiv.org/abs/1902.01046

[6] M. Abadi *et al.*, "TensorFlow: Large-Scale Machine Learning on Heterogeneous Distributed Systems," Mar. 16, 2016, *arXiv*: arXiv:1603.04467. doi: 10.48550/arXiv.1603.04467.

[7] N. Naik and P. Jenkins, "Self-Sovereign Identity Specifications: Govern Your Identity Through Your Digital Wallet using Blockchain Technology," *2020 8th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud)*, pp. 90–95, Aug. 2020, doi: 10.1109/MobileCloud48802.2020.00021.

[8] F. Nargesian, A. Asudeh, and H. V. Jagadish, "Responsible Data Integration: Next-generation Challenges," *Proceedings of the 2022 International Conference on Management of Data*, pp. 2458–2464, Jun. 2022, doi: 10.1145/3514221.3522567.

[9] M. Altendeitering, J. Pampus, F. Larrinaga, J. Legaristi, and F. Howar, "Data sovereignty for AI pipelines: lessons learned from an industrial project at Mondragon corporation," *Proceedings of the 1st International Conference on AI Engineering:*

Software Engineering for AI, pp. 193–204, May 2022, doi: 10.1145/3522664.3528593.
[10] J. Passerat-Palmbach, T. Farnan, R. Miller, M. S. Gross, H. L. Flannery, and B. Gleim, "A blockchain-orchestrated federated learning architecture for healthcare consortia," *arXiv preprint arXiv:1910.12603*, 2019.
[11] N. Naik and P. Jenkins, "Is Self-Sovereign Identity Really Sovereign?," *2022 IEEE International Symposium on Systems Engineering (ISSE)*, pp. 1–7, Oct. 2022, doi: 10.1109/ISSE54508.2022.10005404.
[12] J. Ernstberger *et al.*, "SoK: Data Sovereignty," *2023 IEEE 8th European Symposium on Security and Privacy (EuroS&P)*, pp. 122–143, Jul. 2023, doi: 10.1109/EuroSP57164.2023.00017.
[13] R. V. Yampolskiy and M. S. Spellchecker, "Artificial Intelligence Safety and Cybersecurity: a Timeline of AI Failures," Oct. 25, 2016, *arXiv*: arXiv:1610.07997. doi: 10.48550/arXiv.1610.07997.
[14] M. Brundage *et al.*, "The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation," Feb. 20, 2018, *arXiv*: arXiv:1802.07228. doi: 10.48550/arXiv.1802.07228.
[15] C. Draper and N. Gillibrand, "The Potential for Jurisdictional Challenges to AI or LLM Training Datasets," presented at the AI4AJ@ICAIL, 2023. Accessed: Jul. 28, 2024. [Online]. Available: https://www.semanticscholar.org/paper/The-Potential-for-Jurisdictional-Challenges-to-AI-Draper-Gillibrand/048c126ac8097546f005c2d55132ffe17d3c08d5
[16] R. Blumenthal, "Is Copyright Law the New Turing Test?," *SIGCAS Comput. Soc.*, vol. 52, no. 3, pp. 10–11, Dec. 2023, doi: 10.1145/3656033.3656036.
[17] "[2404.12590] The Files are in the Computer: On Copyright, Memorization, and Generative AI." Accessed: Jul. 28, 2024. [Online]. Available: https://arxiv.org/abs/2404.12590
[18] E. M. Bender, T. Gebru, A. McMillan-Major, and S. Shmitchell, "On the Dangers of Stochastic Parrots: Can Language Models Be Too Big? 🦜," *Proceedings of the 2021 ACM Conference on Fairness, Accountability, and Transparency*, pp. 610–623, Mar. 2021, doi: 10.1145/3442188.3445922.
[19] "Decentralized Identifiers (DIDs) v1.0." Accessed: Mar. 19, 2024. [Online]. Available: https://www.w3.org/TR/did-core/
[20] C. Brunner, U. Gallersdörfer, F. Knirsch, D. Engel, and F. Matthes, "DID and VC:Untangling Decentralized Identifiers and Verifiable Credentials for the Web of Trust," in *Proceedings of the 2020 3rd International Conference on Blockchain Technology and Applications*, in ICBTA '20. New York, NY, USA: Association for Computing Machinery, Mar. 2021, pp. 61–66. doi: 10.1145/3446983.3446992.
[21] P. Zhang and T.-T. Kuo, "The Feasibility and Significance of Employing Blockchain-Based Identity Solutions in Health Care," in *Blockchain Technology and Innovations in Business Processes*, S. Patnaik, T.-S. Wang, T. Shen, and S. K. Panigrahi, Eds., Singapore: Springer, 2021, pp. 189–208. doi: 10.1007/978-981-33-6470-7_11.
[22] C. Pappas, D. Chatzopoulos, S. Lalis, and M. Vavalis, "Ipls: A framework for decentralized federated learning," in *2021 IFIP Networking Conference (IFIP Networking)*, IEEE, 2021, pp. 1–6.
[23] Y. Wang, J. Zhou, G. Feng, X. Niu, and S. Qin, "Blockchain Assisted Federated Learning for Enabling Network Edge Intelligence," *Netwrk. Mag. of Global Internetwkg.*, vol. 37, no. 1, pp. 96–102, Jan. 2023, doi: 10.1109/MNET.115.2200014.
[24] L. Kiffer, A. Salman, D. Levin, A. Mislove, and C. Nita-Rotaru, "Under the hood of the ethereum gossip protocol," in *International Conference on Financial Cryptography and Data Security*, Springer, 2021, pp. 437–456.
[25] P. Ramanan and K. Nakayama, "Baffle: Blockchain based aggregator free federated learning," in *2020 IEEE International Conference on Blockchain (Blockchain)*, IEEE, 2020, pp. 72–81.
[26] S. Kit Lo, Q. Lu, C. Wang, H.-Y. Paik, and L. Zhu, "A Systematic Literature Review on Federated Machine Learning: From A Software Engineering Perspective," Jul. 2020. Accessed: Apr. 19, 2022. [Online]. Available: https://ui.adsabs.harvard.edu/abs/2020arXiv200711354K
[27] C. Ma *et al.*, "When federated learning meets blockchain: A new distributed learning paradigm," *arXiv preprint arXiv:2009.09338*, 2020.
[28] "Ethereum whitepaper - whitepaper.io." Accessed: Apr. 19, 2022. [Online]. Available: https://whitepaper.io/document/5/ethereum-whitepaper
[29] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System".
[30] V. Mugunthan, R. Rahman, and L. Kagal, "Blockflow: An accountable and privacy-preserving solution for federated learning," *arXiv preprint arXiv:2007.03856*, 2020.
[31] K. Bonawitz *et al.*, "Practical Secure Aggregation for Privacy-Preserving Machine Learning," in *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, Dallas Texas USA: ACM, Oct. 2017, pp. 1175–1191. doi: 10.1145/3133956.3133982.
[32] Z. Wang and Q. Hu, "Blockchain-based Federated Learning: A Comprehensive Survey," *arXiv preprint arXiv:2110.02182*, 2021.
[33] H. Cai, D. Rueckert, and J. Passerat-Palmbach, "2cp: Decentralized protocols to transparently evaluate contributivity in blockchain federated learning environments," *arXiv preprint arXiv:2011.07516*, 2020.
[34] "distributed-learning-contributivity/README.md at master · LabeliaLabs/distributed-learning-contributivity · GitHub." Accessed: Apr. 19, 2022. [Online]. Available: https://github.com/LabeliaLabs/distributed-learning-contributivity/blob/master/README.md
[35] Y. Zhou, Z. Wei, S. Ma, and H. Tang, "Overview of Zero-Knowledge Proof and Its Applications in Blockchain," in *Blockchain Technology and Application*, Y. Sun, L. Cai, W. Wang, X. Song, and Z. Lu, Eds., Singapore: Springer Nature, 2022, pp. 60–82. doi: 10.1007/978-981-19-8877-6_5.

[36] “Zero-knowledge proofs,” ethereum.org. Accessed: Jun. 22, 2024. [Online]. Available: https://ethereum.org/en/zero-knowledge-proofs/
[37] J. Benet, “Ipfs-content addressed, versioned, p2p file system,” *arXiv preprint arXiv:1407.3561*, 2014.
[38] R. Jia *et al.*, “Towards Efficient Data Valuation Based on the Shapley Value,” Mar. 03, 2023, *arXiv*: arXiv:1902.10275. doi: 10.48550/arXiv.1902.10275.
[39] R. Jia *et al.*, “Efficient Task-Specific Data Valuation for Nearest Neighbor Algorithms,” Mar. 29, 2020, *arXiv*: arXiv:1908.08619. doi: 10.48550/arXiv.1908.08619.
[40] R. Jia *et al.*, “Scalability vs. Utility: Do We Have to Sacrifice One for the Other in Data Importance Quantification?,” Nov. 16, 2019, *arXiv*: arXiv:1911.07128. doi: 10.48550/arXiv.1911.07128.
[41] “Secret Sharing Sharing For Highly Scalable Secure Aggregation,” ar5iv. Accessed: Jun. 22, 2024. [Online]. Available: https://ar5iv.labs.arxiv.org/html/2201.00864
[42] D. Pereira, P. R. Reis, and F. Borges, “Secure Aggregation Protocol Based on DC-Nets and Secret Sharing for Decentralized Federated Learning,” *Sensors*, vol. 24, no. 4, Art. no. 4, Jan. 2024, doi: 10.3390/s24041299.
[43] 51 Attack. Accessed: Apr. 19, 2022. [Online]. Available: https://www.coindesk.com/tag/51-attack/
[44] P. Zhang, J. White, D. C. Schmidt, G. Lenz, and S. T. Rosenbloom, “FHIRChain: applying blockchain to securely and scalably share clinical data,” *Computational and structural biotechnology journal*, vol. 16, pp. 267–278, 2018.
[45] R. Haakegaard and J. Lang, “The elliptic curve diffie-hellman (ecdh),” *Online at https://koclab. cs. ucsb. edu/teaching/ecc/project/2015Projects/Haakegaard+ Lang. pdf*, 2015.
[46] “Enterprise Ethereum Alliance Off-Chain Trusted Compute Specification v1.1.” Accessed: Jun. 22, 2024. [Online]. Available: https://entethalliance.github.io/trusted-computing/spec.html
[47] *pluralitybook/plurality*. (Jun. 22, 2024). Jupyter Notebook. Plurality: The Future of Collaborative Diversity and Democracy. Accessed: Jun. 22, 2024. [Online]. Available: https://github.com/pluralitybook/plurality
[48] “Partial Common Ownership,” RadicalxChange. Accessed: Jun. 22, 2024. [Online]. Available: https://www.radicalxchange.org/wiki/partial-common-ownership/
[49] *721labs/partial-common-ownership*. (Apr. 06, 2024). TypeScript. 721 Labs. Accessed: Aug. 29, 2024. [Online]. Available: https://github.com/721labs/partial-common-ownership
[50] “Reflexer,” Reflexer. Accessed: Aug. 29, 2024. [Online]. Available: https://www.reflexer.finance
[51] “Radical Markets: Uprooting Capitalism and Democracy for a Just Society,” Princeton Alumni Weekly. Accessed: Aug. 29, 2024. [Online]. Available: https://paw.princeton.edu/new-books/radical-markets-uprooting-capitalism-and-democracy-just-society
[52] Optimism, “Retroactive Public Goods Funding,” Optimism PBC Blog. Accessed: Mar. 02, 2024. [Online]. Available: https://medium.com/ethereum-optimism/retroactive-public-goods-funding-33c9b7d00f0c
[53] “Gitcoin | Fund What Matters To Your Community.” Accessed: Jun. 22, 2024. [Online]. Available: https://www.gitcoin.co/
[54] “RadicalxChange.” Accessed: Oct. 29, 2023. [Online]. Available: https://www.radicalxchange.org/
[55] “Home,” ethereum.org. Accessed: Jul. 01, 2024. [Online]. Available: https://ethereum.org/en/
[56] “Start | Kernel.” Accessed: Jul. 28, 2024. [Online]. Available: https://www.kernel.community/en/start/
[57] “Center for Responsible, Decentralized Intelligence at Berkeley.” Accessed: Aug. 29, 2024. [Online]. Available: https://rdi.berkeley.edu/
[58] *gov4git/gov4git*. (Jun. 18, 2024). Go. Gov4Git Foundation. Accessed: Jun. 22, 2024. [Online]. Available: https://github.com/gov4git/gov4git
[59] “Build network societies, not network states,” Combinations. Accessed: Nov. 14, 2024. [Online]. Available: https://www.combinationsmag.com/build-network-societies-not-network-states/