Decentralized Intelligence Network (DIN)

Abraham Nash
abrahamnash@protonmail.com

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 implemented on a public blockchain 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. By eliminating centralized gatekeepers, *DIN* enables open access to and contribution toward AI training resources while maintaining data control. Participants benefit financially through a trustless peer-to-peer network and actively contribute to a decentralized, scalable ecosystem that harnesses their data to develop impactful AI algorithms.

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 the fuel of AI, yet valuable data remains underutilized due to these silos, where the 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 personal 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 re-centralized.

This dichotomy presents two interrelated challenges: 1) ensuring scalable access to training on data for AI development, and 2) preserving decentralized data ownership. In an increasingly data-driven world, it becomes crucial to establish better incentives for data contribution and fair value distribution—effectively addressing how to motivate and reward data providers through peer-to-peer mechanisms that bind decentralized participation. This paper aims to design and outline a decentralized intelligence network for AI development that addresses both challenges cohesively.

One promising approach to addressing these challenges is Federated Learning (FL),which enables AI model training without requiring data centralization [5]. However, many current FL systems still operate within siloed structures that reflect centralized models. While these systems decentralize the training process, they often rely on frameworks controlled by third-party entities managing siloed data or services. Consequently, such implementations primarily serve the interests of single-entity providers, focusing on data minimization and breach prevention rather than unlocking the full potential of decentralized data stores to enable truly peer-to-peer and decentralized AI development across broader 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 individuals, small and medium-sized enterprises (SMEs), 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* harnesses public blockchain, off-chain file storage (e.g., IPFS), a decentralized federated learning (FL) protocol, and privacy-preserving technologies to enable scalable, decentralized AI development through a trustless peer-peer process. *DIN* facilitates decentralized learning at scale, capable of managing hundreds of thousands to millions of active devices, with the potential to expand to billion*s* [5]. It empowers AI developers to adapt tools and workflows from established scalable FL protocols (e.g., Bonawitz et al., 2019) [5] as implemented in TensorFlow (Abadi et al., 2016) [6], effectively integrating them within a decentralized network to unlock greater opportunities for data accessibility and collaborative learning.

DIN facilitates peer-to-peer AI training and data monetization, addressing the limitations of siloed systems. By enabling effective AI model training across distributed data stores while safeguarding privacy, it fosters decentralized and circular data economies, empowering data owners to directly benefit from their contributions. This approach enhances data accessibility, drives innovation, and creates inclusive economic opportunities for development.

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].

DIN seeks to resolve the challenges of centralized data control, fragmented access, and misaligned incentives that hinder AI development, privacy, and equitable participation, while addressing concerns about security, bias, and the concentration of power in a few entities.

2.1 Requirements

DIN seeks to address the challenges of decentralized, large-scale AI training while ensuring fair, peer-to-peer rewards for participation in FL protocols, upholding 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 requirements:

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 implements a decentralized peer-to-peer orchestration process that includes three essential components: 1) Aggregation, 2) Coordination, and 3) Rewards. By decentralizing these processes, *DIN* ensures that Participants retain ownership of their data while securely contributing to federated learning. This framework enables widespread participation in the FL protocol, fostering scalable, decentralized AI development and opening new opportunities for inclusive, fair, and secure AI systems.

3. Background & Related Works

3.1 Orchestration

The orchestration of Federated Learning (FL) involves three key components: 1) Aggregation, 2) Coordination, and 3) Rewards, each playing a critical role in ensuring efficient and secure AI model training. Each of these elements is essential for the effective operation of FL, ensuring efficient and secure AI model training.This section focuses on FL orchestration in the context of decentralized solutions, with an emphasis on decentralized data stores (e.g. Personal Data Stores (PDS)). These stores are vital for maintaining both data ownership and privacy. For additional details, refer to relevant works [3], [19], [20], [21]. In this framework, decentralized data stores provide the necessary infrastructure for efficient data management, lowering costs and improving scalability, while enabling a more flexible, decentralized approach to AI training.

3.2 Aggregation

3.2.1 Decentralized Aggregation Process

Aggregation is a key component of Federated Learning (FL), where local model updates from multiple Participants are combined to form 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 decentralized Validators—nodes responsible for aggregating, validating, and evaluating model updates. This decentralization improves transparency and fairness in reward distribution while ensuring model integrity.

To scale the aggregation process, *DIN* enables Participants to engage in Federated Learning (FL) across multiple groups, with each group acting as a designated aggregator subgroup for processing model updates. For example, in a group of a thousand Participants, there might be ten subgroups of a hundred. Within each subgroup, ten Validators could be assigned in a 1:10 ratio. Each Validator, using their own computational resources, conducts the aggregation of the 100 models, sharing their results using IPFS to publish the outcomes. The smart contract (SC) then verifies that all Validators reached the same results.

This process is fully decentralized, with Validators randomly assigned to further ensure fairness and prevent collusion. The evaluation process is made secure through Sybil resistance, where greater than 50% of Validators would need to collude to corrupt the aggregation, a highly unlikely scenario given the random assignment of Validators. This reduces the potential for malicious attacks. To minimize on-chain costs, the process can be conducted off-chain using IPFS, with Validtors cross-checking results among themselves. If discrepancies arise, they may participate on-chain for additional checks.

To ensure the integrity of the process, Validators 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 Validators to act honestly. Validators 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 Validators contribute to the aggregation process.

In addition, *DIN* requires that a majority (>50%) of Validators agree on the aggregated model scores. This threshold prevents a single rogue Validator from corrupting the aggregation, ensuring a fair and accurate model update. The network fee generated from this system helps support the operations of the Validators 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 Validators 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 Validators 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 by utilizing an architecture consisting of Coordinators, Master Aggregators, and subgroups of Aggregators. This setup is capable of handling hundreds of thousands or even millions of active devices, with the potential to scale 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 Validators 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. Validators are randomly assigned to Participant subgroups and run staked nodes, which provides Sybil resistance and incentivizes good behavior. Each Validator independently processes updates from at least k devices, mitigating the quadratic computational costs associated with large-scale networks [31], [5]. Validators 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 Validators 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. Furthermore, 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 validator 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 evalutors 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 Validator 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 Validator. In this setup, the Validator 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. **Validator-to-Participant Ratio**: Inspired by BlockFlow's (2020) recommendations, the *DIN* framework integrates a ratio of Validators to Participants to perform evaluations. Validators 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 Validators 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 ability of Participants to reliably perform tasks and maintain connections around the clock.

In contrast, the *Decentralized Intelligence Network (DIN)* improves upon this model by clearly delineating the roles of those who evaluator from the Participants. In *DIN*, Validators are incentivized to provide reliable and dedicated services, taking on the responsibility of aggregating results and auditing rewards on behalf of Participants. By designating these dedicated Validators to handle such tasks, *DIN* ensures more reliable, scalable, and trustworthy operations within the network.

To effectively benchmark model updates and evaluate performance, DIN proposes that the Model Owner publish a test dataset. This dataset allows Validators 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 risks, secure evaluation mechanisms must be implemented, with Validators using Sybil resistance to ensure consistency in evaluating model updates prior to reward distribution. For example, Mugunthan (2020) in BlockFlow proposed scoring procedures that penalize extreme scores and use a median scale. These procedures, when applied between Validators, help address the 50% malicious threat model, as detailed in Section 6. We propose that the Model Owner upload an encrypted test dataset using their public/private keys to IPFS, enabling Validators to securely retrieve and use it for benchmarking. Validators with proof of stake can then signal to the Model Owner that they are ready to begin evaluation and retrieve decryption keys. Validators will apply contributivity scoring procedures, such as 2CP's Substra or BlockFlow's median scoring, to assess performance accurately [30], [33]. 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 Validators, 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, thus maintaining trust in the system. Furthermore, while this paper assumes a steady-state system with fixed numbers of Participants and Validators per aggregator subgroup per FL round, future research will need to focus on experimenting with the dynamic nature of networks. Looking ahead, further security may be offered through privacy-preserving methods, enabling Validators to use techniques like homomorphic encryption (HE) and Zero-Knowledge Proofs (ZKPs) to validate computations without revealing underlying test data for benchmarking [35], [36].

4 Proposed Solution: Systems Architecture and Overview

Decentralized Intelligence Network (DIN) presents a comprehensive framework for decentralized, AI-driven ecosystems that enable scalable data accessibility while preserving ownership and privacy. By leveraging distributed computing models across consumer hardware, edge computing resources, and decentralized storage solutions, *DIN* reimagines artificial intelligence development. Unlike traditional AI models that rely on centralized, siloed data infrastructures and massive computational resources, *DIN* inverts this paradigm. It prioritizes decentralization, privacy, and collaborative progress by designing smaller,

distributed models that run on consumer hardware, utilize on-device or edge computing capabilities, and seamlessly integrate with emerging sovereign data networks. This approach contrasts sharply with resource-intensive, centralized systems, democratizing access and shifting the computational landscape from concentrated power to distributed intelligence.

The innovation of *DIN* lies in its **peer-to-peer network orchestration**, which fundamentally decentralizes the entire AI development process. By disaggregating the core components of AI orchestration—**aggregation, coordination, and rewards**—into a decentralized framework, DIN enables truly peer-to-peer processes that challenge traditional hierarchical models of technological development. This approach not only democratizes AI development but also introduces a more resilient, flexible, and privacy-preserving method of collaborative intelligence creation.

The proposed framework consists of three key elements:

1. **Decentralized data stores ensure data ownership** while enabling the leverage of decentralized storage and integration with sovereign data networks.
2. 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's architecture is fundamentally structured around three core components: **decentralized aggregation**, **coordination**, and **rewards**. This peer-to-peer network orchestration disaggregates traditional centralized AI development models, creating a distributed ecosystem that fundamentally reimagines AI collaboration.

- **Aggregation**: The aggregation process in *DIN* enables distributed data collection with critical design principles. Participant nodes retain local data sovereignty, with only model updates shared across the network. Federated learning techniques preserve data privacy, allowing nodes to contribute computational insights without exposing sensitive information. This approach ensures that raw data remains localized while enabling collaborative model development.
- **Coordination**: Coordination occurs through sophisticated mechanisms that eliminate centralized control. Smart contract protocols define interaction rules, while transparent governance mechanisms and proof-of-stake validation ensure network integrity. Dynamic node selection and consensus algorithms validate model updates, creating a robust, adaptive collaborative environment without relying on a single authoritative entity.
- **Rewards**: The reward mechanism is designed to incentivize meaningful participation through a transparent and fair system. Participants receive compensation proportional to their computational and data contributions. Blockchain-based distribution ensures accuracy, with evaluation occurring through distributed consensus. Both computational resources and data quality are equally valued, preventing manipulation and promoting fair engagement.

Key Participants:

- **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.
- **Validators:** Network-staked entities 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.

DIN's architecture facilitates a transition to decentralized data storage and identity solutions, allowing institutional systems to contribute to federated learning without exclusion. This decentralization-integrative strategy contrasts with acceleration-reductionist approaches that emphasize ever-larger models and computing clusters, reducing privacy risks and centralized control. DIN envisions a future where AI systems are decentralized, empowering individuals and organizations by

shifting control away from centralized entities. This approach enables new opportunities for data utilization and AI development while ensuring individual autonomy and fostering innovation.

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 Validators.

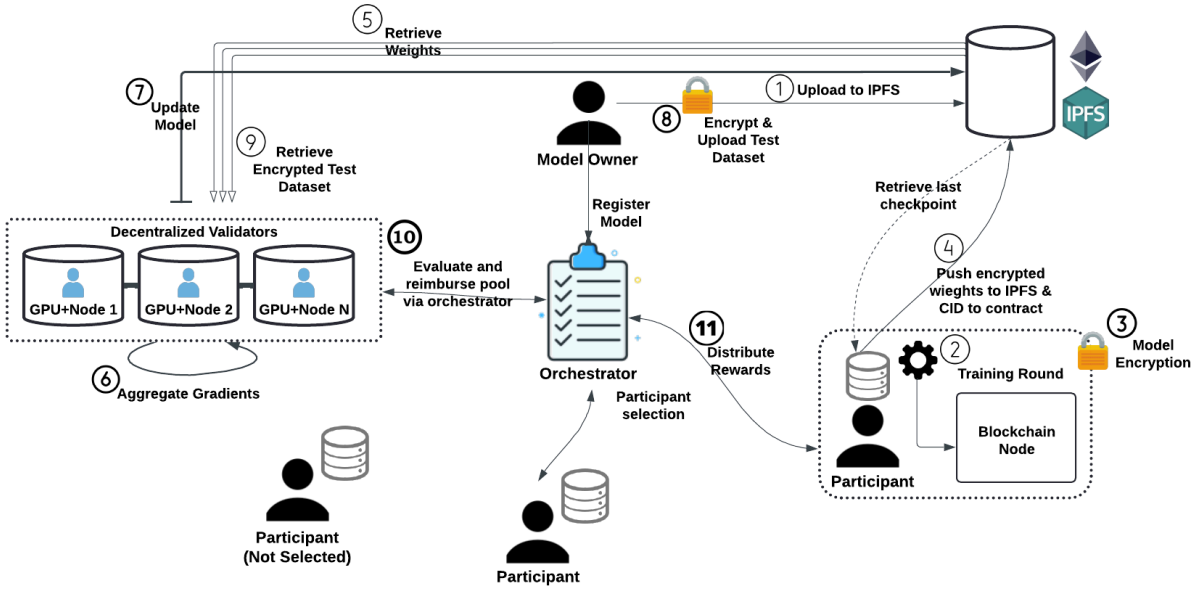

Figure 1. *Global overview of a training round.*

1. **Model Owner:** a. Deploys *intelligence* smart contracts (SC) on the blockchain (i.e. Orchestrator). Although the Orchestrator is referred to as "*intelligence*," multiple contracts may work in unison on-chain, fulfilling different roles to enhance scalability and efficiency (e.g., *DIN* protocol, Validator registry, Validator staking, decentralized aggregation management, 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 models. c. Participants encrypt their models using secure aggregation protocol (e.g. Bonawitz et al. 2019, differential privacy, etc) [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** Validators: *DIN* utilizes Validators as decentralized nodes, each randomly selected and allocated into aggregator subgroups for scalable model aggregation. These Validators 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**: Validators fetch encrypted model weights from decentralized storage (e.g., IPFS) via **CIDs** recorded on the blockchain, ensuring secure processing. Each Validators 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 Validators 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 Validators 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. Validators 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 Validators 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 Validators (i.e., if they do not reach the same aggregate result off-chain on IPFS), an on-chain dispute resolution process is triggered. Validators who fail to align with the majority consensus are slashed, losing their staked tokens and their ability to participate in future aggregation rounds, thereby 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 guarantees that the final aggregated model is both accurate and tamper-proof. g. **Multiple Aggregator Instances**: To further enhance decentralization and resilience, multiple instances of Validators and secure aggregation environments are 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. Participants download updates from IPFS and independently calculate the mean aggregate for their subgroup (ensuring all Participants in a subgroup reach the same result). Optional: If occurring asynchronously, Participants can check all CIDs of the previous round's model updates in their aggregator subgroup. c. Each subgroup performs the average of their own global model and then averages other aggregator groups' averages as published on IPFS (located on-chain) to reach the global model published by the Model Owner.
5. **Model Aggregation Continuation**: a. Validators continue to aggregate FL round updates, averaging their updates as rounds progress. b. The Model Owner can continue testing 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 smart contracts either in advance or during training, depending on the Model Owner's available funds. d. The Model Owner signals the final round, after which one additional round occurs. Validators receive aggregated model updates

and re-signal to the smart contract and Model Owner that the final round has been completed. e. No further rounds are permitted at this stage, as signaled on-chain (visible and transparent). f. Validators are then ready to evaluate Participants' rewards once the final global model is revealed to the Model Owner.

6. **Post-Training**: a. In the final round, Validators receive Participants' scores. b. The Model Owner then encrypts the test dataset using their public/private keys and uploads both to IPFS with verification parameters stored in the smart contract. c. The *intelligence* smart contract utilizes the existing Validators-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. d. Validators signal receipt of the encrypted test dataset and are then provided the decryption key by the Model Owner. e. Validators (with verified stake as confirmed on-chain), who are assigned to specific subgroup FL aggregation rounds for scalability, perform their evaluations of all Participant models within their subgroups on the test dataset. f. Sybil resistance is maintained as Validators submit their evaluations to the smart contract within acceptable ranges (i.e., scoring metrics ensure gross misvaluations or deviations of >50% are penalized). g. Additionally, correct evaluation execution, proper dataset usage off-chain, and adherence to evaluation metrics are ensured. h. If disputes arise from conflicting results, the evaluation automatically moves to on-chain verification with additional oversight. i. Furthermore, randomness in group selection and organization in asynchronous FL processes can further protect against malicious sharing of the test dataset to those still training sufficiently. J. **Optional:** Exploration of benchmarking conducted with HE & ZK-proof circuits to maintain tight security.
7. **Validators**: a. Anyone who stakes the protocols native token can be a Validator. b. Validators evaluate Participants' models against the encrypted test dataset. c. Validators submit evaluation consensus scores to the *intelligence* smart contract (see 2.3.1 Decentralized Auditing Protocol for rewards). d. Validators receive fees for their aggregation, interacting with the coordination of the FL process and evaluation services, which offset the computational cost and incentivize participation.
8. **Distribute Rewards:** a. The intelligence smart contract calculates reward fractions for each Participant based on objective scores (e.g., Shapley Values, Substra Scoring, Median Scoring, and other open-preference scoring methods), ensuring the integrity of the network [30], [33], [38], [39], [40]. b. The Model Owner's deposited rewards are distributed accordingly, based on 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 Validators in the protocol raises concerns about the potential misuse of the test dataset by Validators 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 Validators and adjust the protocol to scale and generalize to other data types, a new issue emerges. Validators 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 Validators is essential. Validators can prove to the system that they correctly evaluated against the test dataset without accessing it, mitigating the risks of misuse or leakage. The Model Owner can provide high-quality, well-distributed, and highly representative test datasets for Validators to use as a benchmark to evaluate each Participant's models, as shown in **Figure 1**. The step-by-step protocol elaborates on the processes of Validators' involvement in the decentralized auditing protocol within the rewards process, as illustrated in **Figure 1**, as follows:

1. **Model Owner preparation**: a. Encrypts with public/private keys for the test dataset. b. Generates evaluation keys and verification parameters for Validators. c. Uploads encrypted test dataset to IPFS and records location CID on the *intelligence* SC.
2. **Within decentralized** Validators **nodes:** a. Validators 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. Validators perform computations on their own GPU hardware within their assigned aggregator groups.
3. c. Sybil resistance ensures that scores remain reliable, with a >50% threshold ensuring that the evaluation scores do not deviate too far from the expected results (i.e., the scores may not differ by more than 50%, which helps to mitigate malicious behavior).
4. d. Validators (with verified stake as confirmed on-chain) assigned to specific subgroup federated learning (FL) aggregation rounds for scalability perform their evaluations of all Participant models within their subgroups using the encrypted test dataset. Sybil resistance holds as Validators submit their evaluations to the smart contract (SC) within acceptable ranges (i.e., scoring metrics ensure that gross misvaluations or deviations of >50% are penalized). Validators are required to execute the evaluations correctly, ensure proper off-chain dataset usage, and adhere to evaluation metrics. If disputes arise from conflicting results, the evaluation automatically moves to on-chain verification with additional oversight. Furthermore, randomness in group selection and organization in asynchronous FL processes can further protect against malicious sharing of the test dataset to those still training sufficiently [43], [44].
5. **Reward Distribution: a)** Based on verified scores, *intelligence* SC calculates and distributes rewards transparently **(as seen in Figure 1)**. b) All transactions are recorded on the blockchain for an immutable audit trail.
6. **Global Model Update & Next Round:** a. The Model Owner signals the end of the training process upon satisfaction with the model's performance. b. The final global model update is revealed to the Model Owner after the completion of the rewards process, and the next round begins.

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 Validators 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 Validators, 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 paper's 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, sybil resistance offered by Validators 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 [45].

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], [46].

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 Validators 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 Validators 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 Validators from copying others' scores without collusion [47]. If a minority subset of malicious Validators 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 Validators [30], [37]. Validators are incentivized to stake a token to gain the right to evaluate Participant models in the rewards process within a proof-of-stake (PoS) ecosystem. Validators 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 paper's threat model, it is crucial that the test dataset provided by the Model Owner remains encrypted to prevent misuse. If the test dataset were accessible to colluding Participants, Model Owners, Validators, or other entities, they could exploit it to manipulate the reward distribution. For example, colluding parties could use the test dataset to strategically improve their model performance or influence evaluation outcomes to gain undeserved rewards. Encrypting the test dataset ensures that it cannot be revealed or used by these entities to unfairly affect 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 that deviates 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 Validators to provide honest assessments by penalizing scores that deviate substantially from the median, helping to mitigate the risk of anomalous scores due to collusion and maintaining fairness in the reward distribution process. Overall, encrypting the test dataset and employing robust scoring mechanisms together safeguard the integrity of the evaluation process and prevent potential manipulation by malicious actors.

Seventh, Validators could compromise fairness by selectively sharing test data with Participants. To prevent this, the Model Owner encrypts the test data and verifies it on-chain. Validators only gain access to the data after completing training and depositing rewards. Validators (with verified stakes, as confirmed on-chain), who are assigned to specific subgroup federated learning (FL) aggregation rounds for scalability, perform their evaluations of all Participant models within their subgroups. In this process, sybil resistance ensures that Validators submit their evaluations to the smart contract (SC) within acceptable ranges. Specifically, scoring metrics ensure that gross misvaluations or deviations of more than 50% are penalized. Correct evaluation execution, proper off-chain dataset usage, and adherence to evaluation metrics are all enforced. If disputes arise from conflicting results, the evaluation automatically moves to on-chain verification with additional oversight. Furthermore, the randomness in group selection and organization within asynchronous FL processes helps prevent malicious sharing of the test dataset with those still training sufficiently [43], [44]. Costs are managed through dynamic training fees [48].

7. DIN Applications

Decentralized Intelligence Network (DIN) offers a scalable framework for decentralized data storage and federated learning, supported by an incentivized reward system. This enables industries to utilize decentralized data stores while maintaining privacy and control. The following use cases exemplify this approach:

- **Decentralized Healthcare (DeHealth):** Patients store their health data in decentralized, secure data stores, controlling who can access and share it. Using federated learning (FL), AI models are trained on this data to improve diagnostics and treatments while preserving privacy. Patients are rewarded directly with tokens for their participation without intermediaries taking a cut, enabling new funding streams for covering their insurance payments via decentralized healthcare insurance.
- **Decentralized Finance (DeFi):** Users retain full control over their financial data in decentralized stores. Financial institutions utilize FL to personalize services and enhance transparency. Through tokenized incentives, users are rewarded for contributing data, driving a more inclusive and decentralized financial ecosystem.
- **Decentralized Physical Infrastructure Networks (DePIN):** In DePIN applications, individuals or organizations contribute physical infrastructure (like IoT devices, sensors, or computing resources) to a decentralized network. Participants are rewarded with tokens for contributing resources and data, while federated learning enables AI models to enhance infrastructure management (e.g., smart grids, renewable energy systems). In agriculture, AI developers can create predictive tools for farmers to forecast weather events and optimize crop yields. Farmers can use the rewards

from their data contributions to purchase crop insurance, protecting against environmental risks, all while maintaining data privacy.

- **Decentralized Smart Cities:** Residents control their data on energy usage, transportation patterns, and environmental metrics within decentralized data stores. City planners use federated learning to optimize urban services such as traffic management and energy distribution. Residents earn tokens for data contributions, which can reduce living costs or fund community-driven sustainability projects.
- **Decentralized Education Technology (DeEdTech)**: In DeEdTech, decentralized networks use federated learning to personalize educational content and assessments while preserving privacy. Learners and educators contribute data and resources, earning token rewards for participation. This model incentivizes continuous learning, supports the creation of tailored learning tools, and can fund educational initiatives, ensuring broader access to quality education.
- **Decentralized Social Media and Content Creation:** Content creators retain control over their data on decentralized platforms, using federated learning to personalize recommendations and boost engagement. They are rewarded with tokens, enabling them to monetize content and reinvest rewards into further content creation.

By supporting data monetization while preserving privacy, *DIN* creates new economic models with tokenized circular economies, benefiting both decentralized and traditional institutions across sectors like finance, healthtech, and education.

8. Tokenomics, Governance, & Public Goods

This section outlines a protocol designed to incentivize and manage participation within a *Decentralized Intelligence Network (DIN*). It integrates both economic and social elements into modern system architecture, emphasizing tangible incentives and a broader systems approach, drawing inspiration from early internet pioneers and recent literature [49].

8.1 Tokenomics and Network Participation

DIN protocol operates as a Proof of Stake (PoS) system, implementing a native ERC-20 token that ensures both sybil resistance and network security. At its core, the protocol employs a comprehensive system of slashing penalties to deter and punish malicious behavior. Validators play a crucial role in the network, being responsible for aggregating and assessing network contributions. To participate, these Validators must meet minimum staking requirements, which helps ensure the fair distribution of rewards.

Network integrity is maintained through stringent slashing mechanisms. The consequences of violations are clearly defined:

1. Validators face immediate slashing for incorrect model aggregation scores or deviant evaluation reports.
2. Delegators to a slashed Validators incur a % reduction in their stake
3. Slashed Validators are permanently removed from the active set and must create a new Validators to participate again

The protocol maintains chain agnosticism to ensure maximum flexibility and enable cross-chain integration. This approach preserves the option to invite external Validators or potentially launch a dedicated chain in the future, with treasury funds available for subsequent developments. However, the establishment of a dedicated "Layer AI" protocol may prove to be a more efficient risk strategy, allowing focused development on AI capabilities while scaling across Layer 2 solutions and beyond.

Validators can **generate revenue through the following services:**

- Aggregation services
- Compute provision
- Evaluation services
- Network fees in native chain currency (ETH on networks like Optimism, Arbitrum, etc)

The introduction of AI Validators and increased fees to support aggregation and compute services may raise Layer 2 costs but enables a powerful blockchain and AI protocol that sits on top of Layer 2s. This economic model ensures Validators are properly incentivized while maintaining the network's security and efficiency.

Participants staking in the network earn through three primary mechanisms:

1. The protocol's native currency inflation
2. A share of transaction fees
3. Delegation rewards from Validators who charge a commission

The system implements a Delegated Proof of Stake (DPoS) model that supports in-protocol delegation. This approach allows Doctelligence token holders to stake their tokens with Validator without the necessity of running their own Validator nodes, thereby encouraging broader network participation.

Our token economy will employ a carefully designed inflation and reward structure. The network mints new tokens as rewards, creating inflation to incentivize staking. Following a model similar to Ethereum 2.0, the inflation rate will decrease over time, ensuring a sustainable token economy. Rewards are distributed proportionally based on stake amounts, while burn mechanisms funded by transaction fees help maintain a balanced supply that supports growth. The system offers flexibility by removing minimum staking requirements for delegators, though Validators must meet minimum thresholds. Rewards can be auto-compounded to optimize returns.

8.2 Decentralized Governance

The governance model of *DIN* is designed to evolve through continuous feedback and community-driven improvement. DIN Proposal Protocols (DPPs) allow developers and community members to submit proposals that address potential network upgrades, changes, or new features.

Proposals are voted upon by contributors using non-coin-based voting credits, ensuring broad and inclusive participation in decision-making. Proposals related to economic parameters or core protocol changes are subject to community voting, ensuring that the direction of the network is determined by its stakeholders.

This flexible governance model enables the network to adapt over time, fostering innovation and continuous improvement. It also aims to mitigate the risks of wealth concentration, ensuring that governance decisions align with the principles of inclusivity, experimentation, and decentralization. As the ecosystem grows, *DIN* will continue experimenting with new models of governance, ensuring that the network remains dynamic, inclusive, and responsive to the needs of the community [51]. A flexible, inclusive rollout driven by community input is essential to mitigate wealth concentration within the DeAI ecosystems.

While token holders do not directly determine voting rights in most cases within the *DIN* protocol, the token may still play a role in network governance, particularly for key decisions that affect the economic model or significant changes to the network that could impact major contributors and Participants. In such cases, token holders can engage in network proposals and decisions through alternative, non-coin-based voting mechanisms. This approach ensures that governance remains inclusive, with decisions made through community consensus rather than centralized authority.

Doctelligence operates as a fully decentralized network, where developers can submit DIN Proposal Protocols (DPPs) for infrastructure upgrades. Only those proposals that impact economic parameters are subject to community voting, ensuring the governance process is both focused and efficient. Other decentralized DPPs aimed at improving network infrastructure can be implemented by developers without the need for a vote, thereby preserving decentralized autonomy and fostering continuous innovation.

8.3 Public Goods Funding

DIN's protocol is designed to allocate a portion of network fees to fund open-source public goods infrastructure, supporting both the network's internal needs and broader initiatives like Gitcoin grants [49], [50]. Votes requiring community approval will use non-coin-based voting, with token allocations based on participant types (e.g., Validators, Model Owners, Participants) through quadratic funding mechanisms, similar to GovGit [51]. This approach aligns with the values of communities like RadicalxChange (RxC), Ethereum, and its layers solutions like Optimism thereby promoting inclusive participation and resource distribution. [52], [53], [54], [55], [56].

Network societies - different to network states - further explore the potential for decentralized models to reshape governance and resource distribution in novel ways, and may also contain relevance to experimental network societies [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. Circulating financial value within ecosystems that benefit the public can stimulate economically advantageous societies.

9. Miscellaneous & Concerns

- **50% Attacks and Proof-of-Stake Security**
    - PoS mechanism resists 50%+ attacks by financially incentivizing honest behavior through token slashing.
    - A critical mass of Validators is needed to ensure random assignment, providing robust Sybil resistance in aggregation and auditing processes for rewards.
    - Ongoing monitoring and upgrades are required to ensure resilience against emerging threats.
- **Open Source & Smaller Models**
    - Smaller, more efficient models may not offer the same accuracy as larger models but help improve scalability.
    - AI model needs to remain open-source as they are downloaded by Participants, then privacy-preserving techniques are applied by the Participant, ensuring that user data remains secure during inference.
    - Essential for Participants with limited resources, ensuring faster training and inference.
    - A practical solution to foster broader participation, despite potential trade-offs in performance.
- **Asynchronous FL Orchestration**
    - **Decoupled Processing Architecture**
        - Implement a robust asynchronous communication framework that allows Participants to engage in training processes independently of global synchronization constraints.
        - Develop a flexible event-driven system that can handle staggered model updates, Participant availability, and computational heterogeneity.
    - **Adaptive Synchronization Mechanisms**
        - Design a dynamic synchronization protocol that can accommodate varying Participant computing capabilities and network conditions.
        - Utilize advanced queuing and event management techniques to manage model updates, aggregation, and reward distribution without blocking entire network operations.
    - **Fault-Tolerant Update Propagation**
        - Develop resilient on-chain/off-chain communication channels that can handle partial or intermittent Participant connections.
        - Implement intelligent retry and recovery mechanisms to ensure continuity of the learning process even when individual nodes experience temporary disconnections.
    - **Modular Coordination Layer**
        - Create a flexible protocol that abstracts the complexities of asynchronous coordination, allowing for:
            - Dynamic Participant onboarding and offboarding
            - Non-blocking model update submissions
            - Intelligent aggregation scheduling

        - Flexible reward distribution based on contribution quality and timing
    - **Performance and Resource Optimization**
        - Implement intelligent backpressure and load-balancing mechanisms to prevent network congestion and ensure efficient resource utilization.
        - Develop adaptive timeout and retry strategies that can dynamically adjust to network and computational constraints.
- **Network Latency**
    - Latency is a challenge in decentralized networks due to coordination among distributed nodes
    - Strategies like hierarchical aggregation and localized evaluation can minimize latency and improve processing speeds, especially in regions with slower internet.
- **Poisoning Attacks**
    - Malicious actors injecting false data can undermine decentralized training processes.
    - *DIN* uses scoring mechanisms (e.g., blockflow-based median scoring) and anomaly detection to identify and neutralize malicious contributions.
    - Safeguards, such as access restrictions and differential privacy, help protect against misuse while maintaining model integrity.
- **Steady-State Validator/Participant Ratios**
    - Assumes fixed numbers of Participants and Validators per aggregator subgroup.
    - Future research needed on the dynamic nature of these ratios
    - Adapting ratios will be key for optimizing efficiency, minimizing bottlenecks, and ensuring scalability.
- **Future of Integrating More Costly Advanced Privacy Techniques**
    - Techniques like Zero-Knowledge Proofs (ZK), Homomorphic Encryption (HE), and Multi-Party Computation (MPC) can increase computational overhead.
    - Network fees help offset some costs, but optimizing privacy techniques for scalability without compromising performance is critical.
    - HE + ZKPs still in early stages for ML and requires modifications to base code of existing frameworks (e.g zama & ezkl[43], [44])
    - Hardware is still developing to efficiently support these techniques, and infrastructure upgrades are anticipated to achieve scalability.

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)
- Privacy-Preserving Techniques (e.g. HE)
- 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 involvement—maintaining our requirements. It enables Model Owners to transact and train their AI on Participants' decentralized data stores peer-to-peer, without intermediaries.

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

- Decentralized networks are evolving to empower users with secure storage and control of their personal data, even on constrained devices such as smartphones, tablets, and IoT systems, as well as smaller computing setups like SME servers or edge clusters.
- Integrating more computationally efficient privacy-preserving methods, such as fully homomorphic encryption (HE) and zero-knowledge proofs (ZKPs), and the associated hardware, to enhance security and usability.
- Ongoing efforts focus on reducing barriers to adoption, including creating user-friendly workflows and minimizing deployment challenges.
- Expand protocol support for training smaller-scale models and testing environments, enhancing the number of AI models and decentralized systems that can operate effectively within the network.

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] “Zama - Fully Homomorphic Encryption.” Accessed: Nov. 25, 2024. [Online]. Available: https://www.zama.ai/
[44] “EZKL.” Accessed: Nov. 25, 2024. [Online]. Available: https://ezkl.xyz/
[45] 51 Attack. Accessed: Apr. 19, 2022. [Online]. Available: https://www.coindesk.com/tag/51-attack/
[46] 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.
[47] 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.
[48] “Enterprise Ethereum Alliance Off-Chain Trusted Compute Specification v1.1.” Accessed: Jun. 22, 2024. [Online]. Available: https://entethalliance.github.io/trusted-computing/spec.html
[49] Optimism, “Retroactive Public Goods Funding,” Optimism PBC Blog. Accessed: Mar. 02, 2024. [Online]. Available: https://medium.com/ethereum-optimism/retroactive-public-goods-funding-33c9b7d00f0c
[50] “Gitcoin | Fund What Matters To Your Community.” Accessed: Jun. 22, 2024. [Online]. Available: https://www.gitcoin.co/
[51] *gov4git/gov4git*. (Jun. 18, 2024). Go. Gov4Git Foundation. Accessed: Jun. 22, 2024. [Online]. Available: https://github.com/gov4git/gov4git
[52] “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
[53] “RadicalxChange.” Accessed: Oct. 29, 2023. [Online]. Available: https://www.radicalxchange.org/
[54] “Home,” ethereum.org. Accessed: Jul. 01, 2024. [Online]. Available: https://ethereum.org/en/
[55] “Start | Kernel.” Accessed: Jul. 28, 2024. [Online]. Available: https://www.kernel.community/en/start/
[56] “Center for Responsible, Decentralized Intelligence at Berkeley.” Accessed: Aug. 29, 2024. [Online]. Available: https://rdi.berkeley.edu/
[57] “Build network societies, not network states,” Combinations. Accessed: Nov. 14, 2024. [Online]. Available: https://www.combinationsmag.com/build-network-societies-not-network-states/