Decentralized Intelligence Network (DIN)

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

Abstract: Decentralized Intelligence Network (DIN) addresses the significant challenges of data sovereignty and AI utilization caused by the fragmentation and siloing of data across providers and institutions. This comprehensive framework overcomes access barriers to scalable data sources previously hindered by silos by leveraging: 1) personal data stores as a prerequisite for data sovereignty; 2) a scalable federated learning protocol implemented on a public blockchain for decentralized AI training, where data remains with participants and only model parameter updates are shared; and 3) a scalable, trustless rewards mechanism to incentivize participation and ensure fair reward distribution. This framework ensures that no entity can prevent or control access to training on data offered by participants or determine financial benefits, as these processes operate on a public blockchain with an immutable record and without a third party. It supports effective AI training, allowing participants to maintain control over their data, benefit financially, and contribute to a decentralized, scalable ecosystem that leverages collective AI to develop beneficial algorithms.

Introduction

1.1 Systems Architecture: Overview

Originally designed as a decentralized network, the World Wide Web (Web 1.0) envisioned a digital landscape 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, leading to 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 [3]. In this fragmented digital environment, data remains siloed within centralized systems, limiting data sovereignty and hindering the full potential of AI.

This paper proposes a comprehensive framework to address these challenges by integrating federated learning (FL) and a trustless rewards mechanism. Three key elements are integral to the framework: personal data stores to ensure individual data ownership, a scalable federated learning (FL) protocol on a public blockchain for decentralized AI training and a trustless rewards system - that is also scalable - to incentivize participation and ensure fair reward distribution. This setup ensures that no single authority controls the FL process, preserving participant sovereignty over their data while fostering collaborative AI efforts.

Our framework's orchestration process revolves around three main components: aggregation, coordination, and rewards. We assert that as long as the latter two processes—coordination and rewards—are conducted without requiring a third party, we can sufficiently preserve the sovereignty of individuals' data stores. Aggregation can be managed by a Model Owner in partnership with a third party, as this does not impede participants' involvement in the FL process nor determine who has access to the protocols for learning on this data.

The *DIN* protocol is designed to facilitate a transition towards decentralized, sovereign data stores controlled by individuals. It acknowledges that institutional silos may continue to participate as single-identity entities, potentially leading to a period where these system architectures co-exist. This approach does not preclude institutions from contributing to the FL protocol, and the *DIN* protocol may act as a catalyst for this transition. By enhancing data access, privacy, and security, the *DIN* protocol promotes the standardization of data formats across systems, encouraging data monetization for both large and small players. Additionally, by not being limited by geographical constraints of institutional silos, the *DIN* protocol ensures a truly global reach and inclusivity.

Hence, we define that data sovereignty of the individual is maintained in this setup, provided that no authority may:

1. Resume access and management controls to determine access and control over the Participants' data itself.
2. Act as an authority to decide who does or does not have access to a Participant's data for FL.
3. Assume an authority role acting as a third-party broker to determine which Participant is rewarded for their contributions, and by how much.

Key participants in this system include:

- **Participants**: Individuals 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 individual data sovereignty.
- **Evaluators**: Network-staked entities responsible for decentralized auditing, ensuring transparency and fairness in evaluating participant contributions and distributing rewards.

The decentralized intelligence network (*DIN)* protocol employs smart contracts (SC) to manage key processes, including *intelligence* SC for coordinating and rewarding AI training and *token* SC for enabling Evaluators to assess participant contributions in a secure, proof-of-stake ecosystem. By leveraging these decentralized mechanisms, the framework encourages the adoption of scalable, sovereign data solutions that uphold individual rights and foster technological advancements, which may lead to new use cases and support the ongoing transition towards decentralized data ownership.

2. DIN Orchestration

2.1 Aggregation

While this paper acknowledges and discusses potential research directions for 'aggregator-less' and decentralized aggregation protocols that could be utilized in the future, our current approach remains acceptable. One such proposal, IPLS, collectively trains a model in a peer-to-peer fashion without the assistance of a server by using an IPFS-based protocol [4]. 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 [4]. However, this framework requires extensive expertise to handle various model types and compression techniques, making it difficult to train more complex algorithms.

Vincent et al. [2020] proposed "Blockchain-aided Federated Learning" (BC-FL), which replaces the need for a central server in the aggregation process by leveraging a public blockchain [5]. This approach considers that local model updates can be received by miners through a gossip protocol over the P2P network [5]. However, gossip-like protocols are notorious for diverging from the real value and failing to reach consensus [6].

Ramanan et al. [2020] proposed "BAFFLE," an aggregator-free FL protocol that eliminates the need for a central server during the FL process [7]. 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.

These methods face challenges in scalability and meeting the diverse requirements of training various algorithms. In the meantime, the use of third parties by the Model Owner (i.e., the entity seeking to access FL protocols to train algorithms on data) for the aggregation process does not interfere with the framework and provides a scalable solution that can be incorporated into the architecture. This approach does not compromise data sovereignty.

The aggregation process itself can be conducted within a trusted execution environment (TEE), which later serves as an aggregator to update the global model. Alternatively, as long as it is confirmed by consensus on a public blockchain, the Model Owner can perform the aggregation themselves, with on-chain verification before signaling the completion of FL rounds and issuing rewards.

Nevertheless, it is crucial to establish clear privacy-preserving techniques, such as differential privacy, in the update and aggregation processes to ensure the anonymity and privacy of Participants' data, regardless of whether it is sent to a TEE or not. Differential privacy, which involves adding random noise to data or model parameters, can prevent inference attacks. It ensures that, with high probability, N−1N-1N−1 colluding agents cannot infer information about the remaining agent when 3N≥3, as the noise masks individual contributions effectively [8], [9]. Overall, the framework is designed to be adaptable and open to updates.

2.2 Coordination

In the coordination process, storing FL protocols on a public blockchain enables an immutable ledger that transparently structures how participants' data is utilized while ensuring individual data remains sovereign to each Participant and is never exchanged. One of the main advantages of leveraging the blockchain for FL is its computational benefits, which enhance round delineation, model selection, and model aggregation in a decentralized manner [10]. Coordination on a public blockchain ensures that no single authority can control who has access to the data for FL, thereby preserving individual sovereignty [5].

In current FL applications, a central server often coordinates the aggregation of local model updates to form a global model. This centralized approach poses potential problems such as dishonest aggregation, accidental network failures, external attacks, and ensuring that all clients follow predefined FL protocols [11]. By contrast, a distributed consensus protocol enabled by blockchain provides transparency, fairness, and impartiality, building trust among Participants in the FL process [5]. Moreover, blockchain’s peer-to-peer (P2P) design offers inherent fault tolerance, improving the system's integrity.

Smart contracts (SC) can orchestrate multiple FL tasks simultaneously across different sets of devices [5]. Addressing the need for an incentive mechanism to encourage Participants to join these FL protocols is crucial, as it is an integral component of quantitative and evaluative inquiries in FL [12]. The proposed architecture utilizes a public blockchain to orchestrate a "trustless" process for coordination and rewards, meaning the process is conducted without relying on a third party [5], [11]. In contrast, a private blockchain relies on a trusted setup, where the orchestrator might collude with the Model Owner, potentially acting maliciously, such as unfairly favoring the rewards process. Additionally, traditional FL lacks incentives to encourage clients to follow the protocol honestly and provide reliable data—clients contribute their computing power without any rewards in return [11].

Zero-knowledge proofs (ZK-proofs) can further enhance security in this setup by allowing participants to prove the validity of their computations without revealing the underlying data, thus ensuring privacy and integrity in the aggregation process. This method helps in mitigating dishonest behaviors and ensuring compliance with FL protocols [13], [14].

A disadvantage of using blockchain in the FL process is that the network topology can affect the performance of the learning process [7]. However, in practical applications, this level of delay may be considered acceptable. Another key consideration is that a blockchain can be architected as a private chain with a central authority responsible for orchestrating FL protocols (similar to central servers) and selecting participating clients (e.g., hospitals in a network). Therefore, a public blockchain ledger is vital to the proposed framework to overcome the competitive interests of institutional stakeholders and the tendency towards re-centralization of data.

2.2.1 Decentralized Intelligence Network (*DIN*) Protocol

In this architecture, Participants opt into federated learning (FL) protocols as defined by the *intelligence* smart contract on a decentralized public blockchain infrastructure (such as layering solutions built upon layering solutions in the Ethereum ecosystem, or others based on the preference of Model Owners, Evaluators, and Participants). This process involves engaging in a system where the *DIN* protocol leverages a public blockchain to manage the coordination and rewards process for training machine learning models on data held in Participant-owned personal data stores.

Ownership here means that Participants can self-govern the management and access control of the data generated about them. Whilst the data remains within the Participant's control, communication can occur with SC on the public blockchain, coordinating the training on local data that never leaves their sovereign datastore, and sending model updates for aggregation during the FL process.

Model Owners, or entities seeking to train their models on Participants' data, use the *intelligence* smart contract to define the FL coordination across several training rounds. This system includes a network-based rewards mechanism, where rewards are issued by a smart contract on the public blockchain based on specific value-based measures, such as model contributivity scores. This ensures a fair and transparent process for all participants involved.

For scalability and to ensure computational efficiency and cost-effectiveness, an on-chain smart contract-based FL protocol coordinates with an off-chain decentralized distributed file storage system called the InterPlanetary File System (IPFS) [15]. This optimizes the cost of participation by providing a location to upload and download model updates during the learning process. For example, decentralized public blockchain infrastructures measure computational costs in terms of gas, which includes storage used and CPU instructions executed. This extends to layer two and other scaling solutions, which provide reduced or non-existent gas costs associated with executing protocols within these environments [16, p. 2]. This choice reflects our understanding that blockchains are ideal for recording transactions, while decentralized file storage systems offer a better environment for storing models and other data, thereby providing a complementary solution [15]. Combining an off-chain decentralized file storage service lowers the cost of participation and maximizes computational efficiency and storage. It is also assumed that clients' computational costs are relatively small compared to the value of their data, so each client is incentivized to train on their entire dataset in each iteration to maximize expected performance and reward [10].

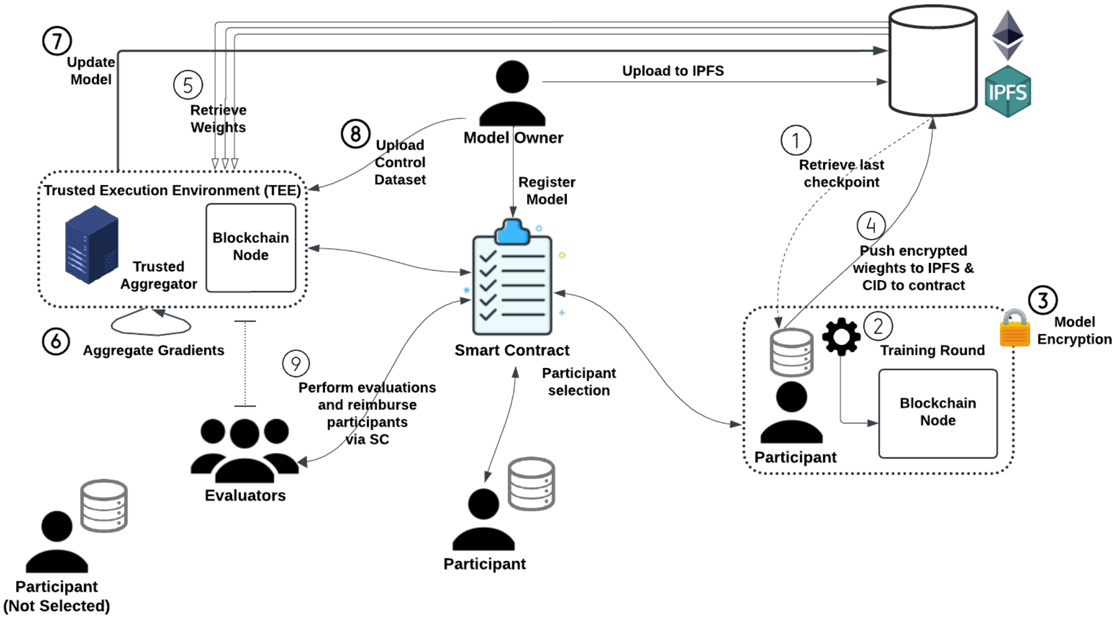

Figure 1. *Global overview of a training round. Adapted from Consensys Health [17].*

1. Model Owner: a. Deploys *intelligence* smart contract on blockchain b. Creates genesis model, uploads to IPFS, records its CID on the contract c. Deposits reward amount in smart contract 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 and upload their updated models to IPFS, recording CIDs on *intelligence* contract d. This completes one FL training round; Participants wait for the next round

3. Aggregation: a. The Aggregator is operated by the Model Owner. b. Acting as a participant with the public blockchain, it fetches all the encrypted weights from decentralized storage as instructed by the Model Owner and verified on-chain. c. The Aggregator decrypts the weights within the safe realm of its encrypted memory and performs the aggregation. d. The TEE fetches encrypted model weights from IPFS using CIDs recorded on the blockchain, ensuring secure and verifiable processing. e. The aggregated results are confirmed on-chain before being revealed to the Model Owner. f. The Aggregator uploads the new model checkpoint to the shared storage and updates the Orchestrator smart contract with the new pointer. g. Multiple TEEs can be instantiated to accommodate a larger workload or introduce more decentralization and reliability.
4. Next Training Round: a. Participants see all CIDs of the previous round's model updates b. Download updates from IPFS and independently calculate mean aggregate (all Participants reach the same result) c. Start training this round from the aggregated global model
5. Model Aggregation Continuation: a. The Model Owner continues to aggregate asynchronous FL round updates. b. The Model Owner tests the global model update against their control dataset to determine when they are satisfied with the training. c. The decision to end or continue training is communicated to the smart contract either in advance or during training, depending on the availability of funds.
6. Post-Training: a. The Model Owner encrypts the control dataset and uploads it to the Trusted Execution Environment (TEE). b. The intelligent contract randomly assigns a standardized fraction of Evaluators per Participant (e.g., 1:10). c. Evaluators, assigned to a specific asynchronous FL round, benchmark all Participant models of that round inside the TEE for off-chain benchmarking (unless there is a disagreement, in which case benchmarking is conducted on-chain).
7. Evaluators: a. Anyone staking native token can be an Evaluator b. Evaluate Participants' models against the control dataset in a trusted execution environment (TEE) c. Submit evaluation consensus scores with ZK-proofs to *intelligence* contract (see **2.3.1 decentralized auditing protocol** for rewards)
8. *intelligence* Smart Contract: a. Calculates reward fraction for each Participant based on scores b. Distributes Model Owner's deposited reward accordingly, per recorded scores

Instead of relying on a single large federated learning (FL) round limited to a small set of Participants, our architecture extends the FL process over multiple asynchronous rounds. In each round, only a subset of the total Participants evaluate and update the global model. This approach enables high scalability by allowing large numbers of Participants to contribute over time, while also reducing the gas consumption on the blockchain per round. As demonstrated by Ramanan et al. in their BAFFLE system, this asynchronous FL protocol can achieve comparable convergence to classical synchronous FL without significant loss in model performance [7]. By incorporating principles of asynchronous rounds and subset evaluation, our architecture supports highly scalable federated learning involving large numbers of Participants in a decentralized manner, similar to the approach shown in BAFFLE [7].

Future work will consider computationally efficient multi-party computation (MPC) in place of trusted execution environments. Secure Aggregation, as described by Bonawitz et al. (2017), utilizes a multiparty computation (MPC) protocol based on Shamir's Secret Sharing scheme (Shamir, 1979). This method, which requires a large number of active devices for privacy guarantees, is currently computationally expensive [18], [19]. As the technology develops, it can be integrated into our architecture to enhance its capabilities. This does not detract from the current architecture presented in this paper, which seeks to address these challenges with a novel framework.

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.

2.3 Rewards Process

Our framework includes a reward mechanism to incentivize participation in the federated learning (FL) process. Participants receive rewards based on their contributions, calculated through a transparent and decentralized protocol. The reward distribution leverages smart contracts on a public blockchain, ensuring fairness and eliminating the need for a central authority.

A decentralized auditing protocol (*DIN*) ensures the integrity and fairness of the rewards process. Evaluators, randomly selected from the network, assess participant contributions using predefined metrics. To enhance security and privacy, the auditing process employs Zero-Knowledge Proofs (ZKPs) and Trusted Execution Environments (TEEs), ensuring that evaluation results are accurate and confidential. This decentralized approach that is executed on a public blockchain consensus prevents any single entity from manipulating the reward distribution, maintaining trust in the system.

In a federated learning (FL) process that issues rewards (e.g., cryptographic micropayments), an evaluation metric is required to assess the relative contributions of each Participant. Several prior works, such as 2CP and Blockflow, have outlined procedures for measuring Participant contributions. 2CP employs Substra to measure contributivity using a step-by-step evaluation [10], [20], while Blockflow evaluates Participants' overall scores based on the median score reported for their model and the inverse of the maximum difference between one's reported score and the median score for each model [21].

However, these frameworks are limited to a small number of Participants and do not address scalability or security guarantees [20], [10], [21]. These frameworks assume that all Participants act as Evaluators in the entire FL process due to the small number of Participants. For example, in an experiment with 100 Participants, all 100 would need to download and evaluate the N - 1 Participant models. This approach is not scalable, as the costs increase asymptotically with the growing number of Participants [10].

Our approach delineates the roles of Participant and Evaluator as separate entities. This separation accommodates diverse data scenarios and recognizes that not all Participants may be willing or capable of participating in the evaluation process. To ensure generalizability, the Model Owner publishes a control dataset to a Trusted Execution Environment (TEE) once the training metrics from asynchronous FL rounds meet the specified criteria. Evaluators are then notified via the intelligence smart contract (SC) to assess Participants' performance using this control dataset in the TEE. They apply contributivity scoring procedures, such as 2CP's Substra or Blockflow's median scoring, to evaluate performance.

Evaluators are randomly selected (Q ≪ N) to evaluate Participants' work in each asynchronous FL round, enabling scalability. Both BlockFlow [2021] and 2CP explored a 1:1 ratio score allocation of Evaluators to Participants, where each Participant evaluates every other Participant's score [10]. For example, in BlockFlow (2021), experiments recorded the average median agent F1 scores when varying the number of Evaluators for 1, 25, 50, and 100 agents. They found that the average absolute difference between the Evaluators' scores at each level of participation was <0.67% on their datasets (income data) [10].

One key difference in the *DIN* protocol, which advances BlockFlow's work when considered in its entirety, is the definition of a fraction of the total number of Participants to act as Evaluators within a given asynchronous FL round. This approach accommodates scaling over an increasing number of FL rounds. For example, within one asynchronous round, there might be 100 Participants and 10 Evaluators assigned. A sufficiently large number of Evaluators, with high probability, leads to accurate results and resistance to M<N2 malicious agents [10].

Therefore, future experiments in implementing the *DIN* protocol should evaluate whether this difference in score allocation holds when a larger ratio of Participants to Evaluators is used, which may depend on the data type being trained upon. Additionally, validating the protocol for heterogeneous data sources is crucial. While Participants can also be potential Evaluators, this separation enhances integrity and applicability across different data types.

This separation accommodates diverse data scenarios, enabling our adaptable evaluation protocol's effectiveness across data types. The Model Owner issues a control dataset for Evaluators to assess Participants using suitable contributivity scoring systems (e.g., 2CP's Substra, Blockflow's median scoring), ensuring fair, objective evaluations and process integrity. This paper assumes a steady-state system with constant Participant and Evaluator numbers per asynchronous FL round, though addressing the dynamic network nature is crucial for future work.

2.3.1 Decentralized Auditing Protocol

Delineating the roles of Participant and Evaluator in the protocol raises concerns about the potential misuse of the control dataset by Evaluators in federated learning (FL) scenarios. In previous examples, each Participant evaluated every other Participant using their data and an objective scoring metric [10], [20]. 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 control dataset published by the Model Owner with Participants in one or more asynchronous FL rounds, potentially leading to harmful activities such as model poisoning or unfair compensation during the model 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 control dataset without accessing it, mitigating risks of misuse or leakage. Evaluators can be provided with high-quality, well-distributed, and highly representative control 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 selects trusted third-party Trusted Execution Environments (TEEs) for model evaluation.
2. Model Owner distributes encrypted control dataset to TEEs.
3. Within TEEs: a. Evaluators compute performance metrics (accuracy, precision, recall) on models using a control dataset. b. Evaluators utilize existing remote attestation mechanisms to provide proof that the execution is performed within the TEE and that the environment is exactly as specified, ensuring the execution is as requested without revealing any data. c. Evaluators generate Zero-Knowledge Proofs (ZKPs) for each metric, proving correct computation without revealing data.
4. Evaluators submit ZKPs and encrypted evaluations to blockchain *intelligence* smart contracts.
5. Smart contract verifies ZKPs using a consensus mechanism (e.g., majority agreement).
6. Based on verified scores, smart contract calculates and distributes rewards transparently.
7. All transactions are recorded on the blockchain for an immutable audit trail.
8. TEEs and ZKPs provide dual security - TEEs isolate data, and ZKPs prove correctness without exposure.
9. Protocol protects against insider threats by computing within TEEs and exporting only ZKPs.

The *DIN* protocol can utilize any contributivity scoring procedure for Evaluators to perform their off-chain evaluations of Participants' contributions. The specific procedure depends on the context of the learning task being conducted. This evaluation process is triggered when the Model Owner is satisfied with the global model's performance metrics (e.g., F1 score, accuracy, etc.). Evaluators are randomly assigned to the asynchronous Federated Learning (FL) participant pools at a specific ratio (e.g., one Evaluator for every ten Participants). They perform their off-chain evaluations of each Participant's model using the control dataset published by the Model Owner, encrypt their score, and report their encrypted scores with a ZKP to the *intelligence* smart contract. Each Evaluator first reports to the smart contract the set of Participants whose models were successfully validated (i.e., within an acceptable bound specified by the Model Owner). Participants who fail this test are eliminated in that particular FL round. Once all the scores are received, each Evaluator provides the decryption key to provably reveal their score to the *intelligence* smart contract.

This protocol ensures secure and reliable model evaluations by incorporating third-party Trusted Execution Environments (TEEs) selected by the Model Owner and safeguarded by Zero-Knowledge Proofs (ZKPs) and blockchain technology. It aligns with the Model Owner's incentives, who, despite bearing the cost, benefit from robust data contributions and trustworthy evaluation processes necessary for successful model training and improvement. Crucially, the protocol preserves data sovereignty for Participants - no central authority determines access to their data, which never leaves its original storage. Rewards are also determined in a decentralized manner by a public blockchain smart contract based on pre-defined, auditable, and transparent metrics, eliminating the need for a central authority to decide compensation. This decentralized auditing protocol maintains Participants' autonomy while enabling secure, reliable, and incentive-aligned model evaluations.

It's worth noting that while fully homomorphic encryption, currently computationally expensive, may present a potential avenue for updating this protocol in the future, its current limitations shouldn't detract from the efficacy of the proposed architecture.

3. Threat Model

Our 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, our use of Zero-Knowledge Proofs (ZKPs) and Trusted Execution Environments (TEEs) mitigates risks associated with model evaluation and reward distribution. This comprehensive approach ensures the security and reliability of the FL process, maintaining participant trust and data sovereignty.

Firstly, in an experiment with N agents, it is resistant up to M∈[0, N/2) agents neglecting to follow the protocol for the experiment to maintain its integrity [10]. 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 [22].

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 [23], [24], [25].

Third, IPFS is immutable, meaning agents cannot change their model after submitting the cryptographic hash to the smart contract [15]. 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 [10], [15].

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 [2021] uses a contributivity score system where lower scores result in less cryptocurrency received [10], [15]. 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. This penalizes attempts to fabricate scores, as the protocol limits a Participant's overall score to the evaluation furthest from the median [10], [15].

Fifth, Participants can collude during the training process to submit better models by secretly sharing raw data or models among M<N2 colluding Participants [10], [15]. 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 [10], [15]. For attacks by Evaluators in the evaluation process, the intelligence smart contract uses encryption and a commit-then-reveal protocol (e.g., using Elliptic Curve Diffie-Hellman keys) to prevent Evaluators from copying others' scores without collusion [26]. 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 [10], [15]. Evaluators are incentivized to stake a native token to gain the right to evaluate Participant models in the rewards process within a proof-of-stake (PoS) ecosystem. 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, both the aggregation process involving trusted third-party computing environments and the utilization of Trusted Execution Environments (TEEs) with Zero-Knowledge Proofs (ZKPs) introduce distinct threat models. Concerns with aggregation hardware include potential data interception and manipulation, insider threats at third-party providers, hardware vulnerabilities such as side-channel attacks, and compliance issues with data protection regulations [27], [28]. TEEs, while isolating sensitive computations, face risks from hardware exploits, software vulnerabilities, and third-party trust issues. Additionally, implementations of ZKPs must be carefully managed to avoid cryptographic flaws that could undermine their effectiveness [29]. To counteract these threats, robust encryption, rigorous access controls, regular security audits, and compliance assurance are employed [29]. These measures ensure that data remains confidential and integral, reducing the dependency on trust by making processes transparent and verifiable through smart contracts on the blockchain. This strategy enhances security and stabilizes residual risks within a robust, transparent operational framework.

4. DIN Applications

The decentralized intelligence network (*DIN*) protocol offers a scalable and versatile framework for learning from sovereign, individually owned 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.

Key use cases include:

- **Healthcare**: Patients store their health data in self-sovereign data stores, controlling access and sharing securely. Medical researchers and healthcare providers can access the FL protocol on-chain to train AI models on this data, improving diagnostics and treatment plans without ever seeing the raw data. Patients can be financially rewarded for contributing to medical research, and they can use these rewards to help cover insurance premiums, thereby lowering the barrier to providing accessible healthcare.

- **Finance**: Individuals store their financial transaction data in decentralized data stores. Financial institutions can access the FL protocol on-chain to provide personalized financial advice and develop new financial products based on aggregated insights. Users remain in control of their data and can receive rewards for their participation, fostering a transparent and incentive-aligned financial ecosystem.

- **Education**: Students store their academic records and learning progress in self-sovereign data stores. Educational institutions can access the FL protocol on-chain to tailor learning experiences and provide personalized support without accessing the raw data. Students can receive incentives for allowing their data to contribute to educational research and improvements, funding some of their education costs.

- **Smart Cities:** Residents store data related to their energy consumption, transportation patterns, and other smart city metrics in self-sovereign data stores. City planners and utility providers can access the FL protocol on-chain to optimize city services and infrastructure without accessing the raw data. Individuals receive rewards for allowing their data to promote sustainable and efficient urban living, and they can use these rewards to contribute toward various living costs, thereby improving their quality of life.

- **Agriculture:** Farmers store data on crop yields, soil conditions, and weather patterns in decentralized data stores. Agricultural researchers and companies can access the FL protocol on-chain to develop better farming practices and technologies. Farmers retain control over their data and receive rewards for their contributions, fostering innovation and sustainable agriculture. Additionally, farmers can use the rewards they receive to contribute to crop insurance, benefiting from monetizing the data they collect and reinvesting it into their local ecosystems.

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.

5. Public Goods, Governance, and Tokenomics

While it may seem unconventional in a technical paper, this work underscores the importance of considering social aspects and tangible incentives in market design for modern system architectures. Both early internet pioneers and recent literature emphasize this necessity.

Key social themes include:

- **Public Goods Initiatives**: Such as Gitcoin funding and Optimism's vision for community-driven proposals and funding of public goods ecosystems [30], [31], [32].

- **Governance Concepts**: Including Gov4Git (non-coin-based voting), quadratic voting, and delegate mechanisms, to engage contributors [33], [34], [35].

- **Non-speculative Tokenomics Design:** for example, utilizing Harberger taxation and partial-common ownership in the evaluation process [36].

These works align culturally with the Plurality for the Future of Collaborative Technology and Democracy, the Ethereum blockchain ecosystems, and their extensions [35], [37]. However, given the open nature and license of these intended works, and depending on people's preferences, the material and content can be forked and taken in the direction preferred by those communities and individuals.

A flexible and inclusive rollout, driven by community input, can help serve the public good and mitigate wealth concentration in the crypto ecosystem. We acknowledge the importance of circulating financial value within ecosystems that benefit the public, allowing market-driven value to act as a catalyst for economically beneficial societies. Embracing ongoing experimentation and a willingness to explore new ideas is crucial for advancing these concepts in dynamic and innovative ways.

6. Future Works

Decentralized Intelligence Network (*DIN)* integrates the latest themes of data sovereignty, public blockchain, decentralized federated learning (FL), off-chain file storage (e.g., IPFS), and reward protocols. It introduces a decentralized FL protocol within a sovereign architecture, allowing individuals to own and control their data while being rewarded for sharing it. This scalable framework overcomes the limitations of siloed data, benefiting both participants and data users. The protocol includes a scalable, decentralized auditing system for fair reward distribution.

Despite implementation challenges, technological advancements offer a promising foundation for further development. We encourage researchers, practitioners, and stakeholders to engage with this framework to promote data ownership and individual sovereignty. Collaborative efforts can lead to scalable, sovereign data solutions that advance technology and respect individual rights.

Future enhancements may include fully homomorphic encryption and expanded interactions with sovereign data stores, ensuring continued innovation and effectiveness. Additionally, the development of non-speculative token designs, and, enabling the DIN protocol to become a core public goods infrastructure.

7. 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 asynchronous FL architectures (Paritosh), scalable decentralized auditing protocol (Paritosh, Harry), sovereign architectures, and decentralized identity management (Dana). And 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.

References

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

[2] R. W. Gehl, "Distributed Centralization: Web 2.0 as a Portal into Users' Lives," *Lateral*, no. ateral 1, 2012, doi: 10.25158/L1.1.4.

[3] 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.

[4] 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.

[5] C. Ma *et al.*, "When federated learning meets blockchain: A new distributed learning paradigm," *arXiv preprint arXiv:2009.09338*, 2020.

[6] 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.

[7] 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.

[8] V. Bindschaedler, S. Rane, A. E. Brito, V. Rao, and E. Uzun, “Achieving differential privacy in secure multiparty data aggregation protocols on star networks,” in *Proceedings of the Seventh ACM on Conference on Data and Application Security and Privacy*, 2017, pp. 115–125.

[9] H. Jiang, Y. Gao, S. M. Sarwar, L. GarzaPerez, and M. Robin, “Differential Privacy in Privacy-Preserving Big Data and Learning: Challenge and Opportunity,” in *Silicon Valley Cybersecurity Conference*, S.-Y. Chang, L. Bathen, F. Di Troia, T. H. Austin, and A. J. Nelson, Eds., Cham: Springer International Publishing, 2022, pp. 33–44. doi: 10.1007/978-3-030-96057-5_3.

[10] V. Mugunthan, R. Rahman, and L. Kagal, “Blockflow: An accountable and privacy-preserving solution for federated learning,” *arXiv preprint arXiv:2007.03856*, 2020.

[11] Z. Wang and Q. Hu, “Blockchain-based Federated Learning: A Comprehensive Survey,” *arXiv preprint arXiv:2110.02182*, 2021.

[12] 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

[13] “Zero-knowledge proofs,” ethereum.org. Accessed: Jun. 22, 2024. [Online]. Available: https://ethereum.org/en/zero-knowledge-proofs/

[14] 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.

[15] J. Benet, “Ipfs-content addressed, versioned, p2p file system,” *arXiv preprint arXiv:1407.3561*, 2014.

[16] “Layer 2,” ethereum.org. Accessed: Jun. 22, 2024. [Online]. Available: https://ethereum.org/en/layer-2/

[17] 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.

[18] “Secret Sharing Sharing For Highly Scalable Secure Aggregation,” ar5iv. Accessed: Jun. 22, 2024. [Online]. Available: https://ar5iv.labs.arxiv.org/html/2201.00864

[19] 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.

[20] 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.

[21] “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

[22] 51 Attack. Accessed: Apr. 19, 2022. [Online]. Available: https://www.coindesk.com/tag/51-attack/

[23] “Decentralized Identifiers (DIDs) v1.0.” Accessed: Mar. 19, 2024. [Online]. Available: https://www.w3.org/TR/did-core/

[24] 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.

[25] 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.

[26] 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.

[27] “PPFL: Privacy-preserving Federated Learning with Trusted Execution Environments,” ar5iv. Accessed: Jun. 22, 2024. [Online]. Available: https://ar5iv.labs.arxiv.org/html/2104.14380

[28] T. Geppert, S. Deml, D. Sturzenegger, and N. Ebert, “Trusted Execution Environments: Applications and Organizational Challenges,” *Front. Comput. Sci.*, vol. 4, Jul. 2022, doi: 10.3389/fcomp.2022.930741.

[29] “Enterprise Ethereum Alliance Off-Chain Trusted Compute Specification v1.1.” Accessed: Jun. 22, 2024. [Online]. Available: https://entethalliance.github.io/trusted-computing/spec.html

[30] Optimism, “Retroactive Public Goods Funding,” Optimism PBC Blog. Accessed: Mar. 02, 2024. [Online]. Available: https://medium.com/ethereum-optimism/retroactive-public-goods-funding-33c9b7d00f0c

[31] E. G. Weyl, P. Ohlhaver, and V. Buterin, “Decentralized Society: Finding Web3’s Soul,” May 2022, Accessed: Jun. 22, 2024. [Online]. Available: https://www.microsoft.com/en-us/research/publication/decentralized-society-finding-web3s-soul/

[32] “Gitcoin | Fund What Matters To Your Community.” Accessed: Jun. 22, 2024. [Online]. Available: https://www.gitcoin.co/

[33] “gov4git/gov4git.” Gov4Git Foundation, Jun. 18, 2024. Accessed: Jun. 22, 2024. [Online]. Available: https://github.com/gov4git/gov4git

[34] “RadicalxChange.” Accessed: Oct. 29, 2023. [Online]. Available: https://www.radicalxchange.org/

[35] “pluralitybook/plurality.” Plurality: The Future of Collaborative Diversity and Democracy, Jun. 22, 2024. Accessed: Jun. 22, 2024. [Online]. Available: https://github.com/pluralitybook/plurality

[36] “Partial Common Ownership,” RadicalxChange. Accessed: Jun. 22, 2024. [Online]. Available: https://www.radicalxchange.org/wiki/partial-common-ownership/

[37] “Home,” ethereum.org. Accessed: Jul. 01, 2024. [Online]. Available: https://ethereum.org/en/