A Perspective on Decentralizing AI

Abhishek Singh[a], Charles Lu[a], Gauri Gupta[a], Ayush Chopra[a], Jonas Blanc[a], Tzofi Klinghoffer[a], Kushagra Tiwary[a], and Ramesh Raskar[a]

MIT Media Lab

Recent progress in AI has demonstrated its tremendous potential to solve problems at scale. However, the current AI paradigm is highly centralized and limited in domains where data and knowledge are distributed across organizations and geographies. This paper advocates for a self-organized approach to building and deploying AI in decentralized contexts, such as healthcare, climate science, and supply chain management. We identify five key technical challenges — (1) privacy, (2) verifiability, (3) incentives, (4) orchestration, and 5) crowdUX that need to be addressed to unlock the potential of AI in these domains. By overcoming these challenges, we can enable distrusted, disincentivized, and disinterested entities to collectively solve global problems while pursuing local objectives. This perspective aims to stimulate discussion and research towards a more decentralized, participatory, and resilient future of AI.

1. Introduction

Current progress in AI is led by large organizations that rely on the centralization of data, compute, and governance. However, as AI expands into real-world industries such as healthcare, finance, supply chain, and smart cities, the centralized approach faces several major challenges. Confidentiality and competition will hinder collaboration and trust between entities while the lack of incentives and privacy concerns in siloed organizations limits the availability of data and compute resources. Ultimately, this results in concentrating large-scale AI capabilities in the hands of just a few major AI companies. In this paper, we outline a more decentralized AI approach to promote collaboration between disparate entities through incentivization and orchestration of data and compute.

Motivation: To contextualize the problem, let's consider the story of Sarah from rural Texas, who has developed severe chest pain after recovering from a recent bout of COVID-19. She goes to her local clinic with all of her past data and has her chest X-ray examined, but her local doctor is unable to conclusively diagnose the condition. The promise of AI in healthcare lies in assisting patients like Sarah, who have relevant data but lack access to expert decision-making to diagnose her complex health condition. Can the doctor find a better diagnosis for some fixed budget, say $100, in a matter of seconds by sharing her medical data with a privacy-preserving decision-support service? Imagine that the exabytes of health data all around the world could be used to train an AI model to help Sarah and her doctor decide on the best diagnosis and treatment plan. One can argue that, with this extreme centralization of health data and compute, the majority of patients can get more informed and higher-quality care. However, this promise faces major obstacles in practice. Medical data today sits in isolated silos across smartphones, hospitals, wearables, and research labs. Patients are reluctant to share personal data with a central system they do not trust. This centralized utopia clashes with the decentralized realities of fragmented health data and misaligned incentives.

Recent Trends: Three recent trends in the machine learning (ML) community motivate the urgent need for adopting a more decentralized approach to AI:

- **Personal agents** — Recent advances in foundation models have sparked widespread interest in personal AI agents (assistants, co-pilots, etc.) capable of interpreting information and acting on our behalf. These agents will require a comprehensive understanding of the intent and preferences of each individual user through their personal data including their emails, finances, health data, and personal relationships. Scaling such a system to a population level necessitates orchestrating billions of personal and organizational AI agents. A decentralized framework is crucial to achieve this scale without creating a surveillance state.

- **AI-PC** — AI-embedded Personal Computers (1), characterized by integrated hardware accelerators (GPUs and NPUs), are experiencing rapid market growth (2, 3) due to the increasing demand for on-device AI capabilities. These systems facilitate a decentralized computational paradigm, enabling both inference and training of large-scale machine learning models locally. This edge computing approach offers benefits such as reduced latency, enhanced privacy, and improved offline functionality. However, the distributed nature of this ecosystem necessitates an orchestration layer to address challenges in synchronization and coordination if we want to utilize the collective potential of on-device resources.

- **From Monolithic to Polylithic models** — The emergence of compound systems (4) and multi-agent approaches (5, 6) to machine learning models signals a paradigm shift. We are moving away from si
integrated systems of multiple components that coordinate with the help of M
increasing complexity of tasks, where no single organization can be expected to possess all the necessary components

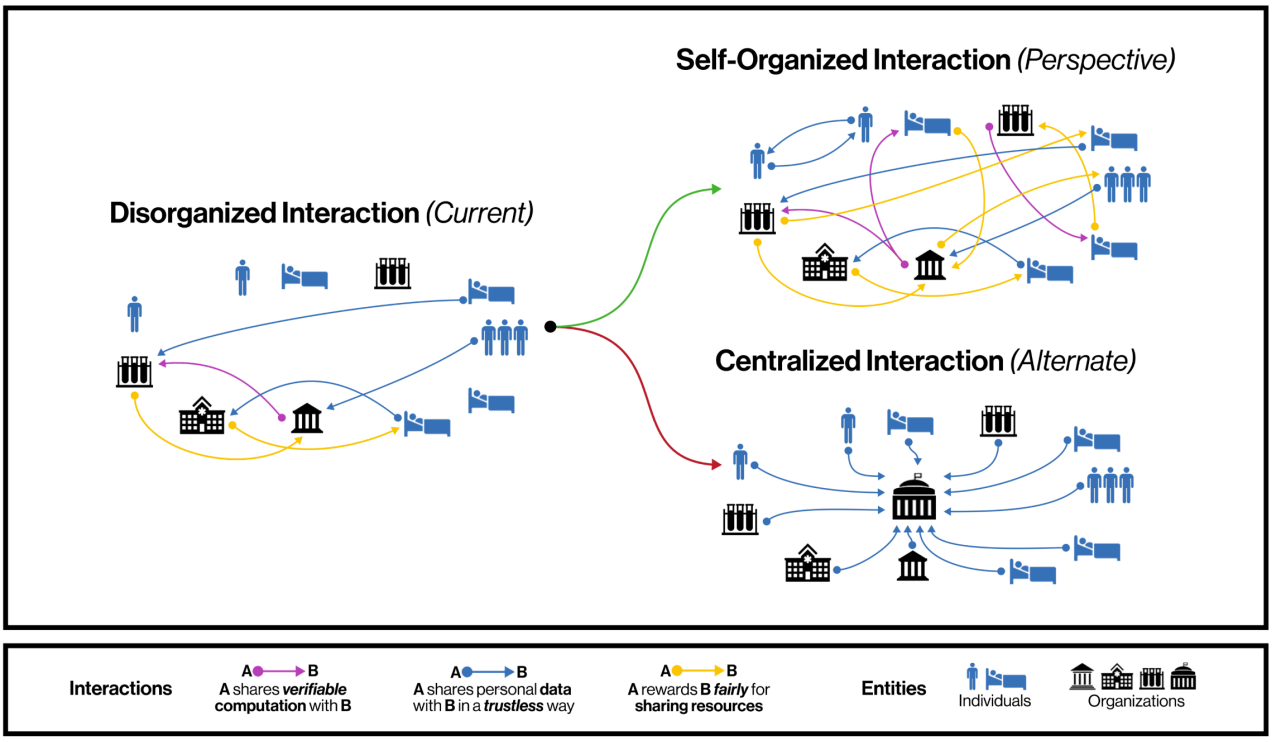

Fig. 1. Missed opportunities in today's AI. We posit that *self-organization* can increase the inter-connectedness of siloed entities in the current disorganized ecosystem where only a few entities can participate and interact. While advances in federated learning and open-source software have shown the benefits of decentralization, significant progress is needed to enable verifiable sharing of computation, incentivize data sharing, and reward entities fairly and equitably for sharing their resources. Addressing these challenges will improve the collaboration among entities, enabling new frontiers in AI that keep humans healthier, our planet cleaner, and our financial system more secure.

and tools to solve complex problems. Consequently, this shift introduces new challenges in synchronizing efforts across multiple entities.

Problems with the Centralized AI Paradigm: While today's AI depends upon centralized data and computation, society is much more decentralized. Forcing these fragmented stakeholders to become centralized in a top-down manner will likely result in forced adoption but marginalization of minor players or outliers, such as patients with rare or stigmatized diseases.

- **Privacy Risks and Collaboration friction** — Data misuse by large companies and recent cybersecurity breaches have exposed the vulnerability of centralized repositories holding vast amounts of sensitive health information. Notable incidents include attacks on Change Healthcare (7) and 23andMe (8), a popular DNA sequencing company. The latter resulted in the leak of genetic data belonging to approximately 7 million individuals, underscoring the risks associated with a single entity storing large volumes of personally identifiable health data. This not only puts existing centralized data lakes at privacy risk but also creates friction in collaboration, preventing individuals and organizations from exchanging wisdom and insights.
- **Governance Pitfalls** — Large companies like OpenAI and Google's Gemini have struggled recently with governance decisions that satisfy all stakeholders (9, 10). It puts an unreasonable burden on a small group of individuals to deploy AI services for the rest of the world. Excessive consolidation of data, models, talent, and decision-making (steering of model's outputs) can be fragile to the ecosystem.
- **Compensation Conflicts** — Recent lawsuits against major AI companies highlight the problem of a single entity extracting value from content creators and data producers without their consideration or consent for their data contributors, leading to disputes over intellectual property rights and compensation (11–13).
- **Innovation Friction** — Centralized corporate networks often lock users into their platforms to reduce churn and prevent competition (14). However, such practices stifle innovation and concentrate power in the hands of service providers, creating barriers to entry, and limiting the overall growth and accessibility of the AI ecosystem.

2. What is Decentralized AI?

In real-world scenarios, assets required for developing and deploying AI are inherently decentralized and distributed across countless individuals and organizations. However, the prevailing paradigm for building ML systems today requires centralized

accessibility and control over these assets. Figure 1 illustrates the contrast between different approaches to building AI systems. From our perspective, decentralized AI enables collaboration between entities with complementary assets, such as data and computation, without requiring any central oversight of the overall system. Now we discuss the motivation for the decentralization of the key assets.

Decentralized Data: One of the significant bottlenecks in AI advancement is access to high-quality, diverse training data. Despite the vast troves of data generated through digitization, much of it remains siloed within the confines of individual organizations, such as financial institutions, hospitals, and personal devices. This fragmentation is often due to valid privacy concerns and the lack of incentive to process, list, and share data. Consider again the case of Sarah. Hundreds of patients worldwide might have similar diagnostic data and treatment outcomes that could inform her care. However, the inaccessibility of this data means the collective knowledge remains untapped by Sarah's doctor. Decentralized AI protocols offer a framework for unlocking these datasets at each stage of the machine learning pipeline — from research and development to training and inference. With the right set of tools for data sharing and aggregation, decentralized AI can break down the silos that currently limit the flow of knowledge and analysis from information and data.

Decentralized Computation: Training large-scale deep learning models requires substantial computing resources, which are often concentrated within a few well-funded organizations. This limitation hinders the ability of the broader research community to fully explore and innovate in the field. Decentralized AI offers a solution by democratizing access to computational power. By harnessing the collective resources of a large network of devices with limited individual capacity, such as smartphones, laptops, and edge devices, researchers can effectively distribute and parallelize computations. This approach enables the undertaking of large-scale computations that would otherwise be infeasible or cost-prohibitive. However, realizing this vision of decentralized computation must overcome open challenges such as incentivizing device owners to contribute their computational resources on a shared network and asynchronously orchestrate a heterogeneous network of devices with varying connectivity and availability.

Decentralized Coordination: Decentralized AI extends beyond distributed data and computation to enable decentralized interactions. This aspect is crucial to prevent reliance on a few central organizations for coordinating collaboration. We propose that Decentralized AI can create an overlay network, similar to how the web operates on top of the internet. This network would facilitate self-organized coordination between data and compute owners, incorporating appropriate incentive structures, strong privacy measures, and verifiable processes. Such a system ensures that collaboration and innovation can occur without centralized control, fostering a more open and equitable AI ecosystem.

Potential of decentralized AI: We posit that decentralized AI will enable advancements in the following ways:

- **AI over siloed data** — Fragmented industries with multiple stakeholders, such as healthcare and climate science, are poised to benefit from a decentralized AI ecosystem. In healthcare, sharing data across organizations is a big concern. Existing AI development pathways have favored easily accessible web data, leaving valuable but siloed data largely untapped. Decentralized AI offers a solution by incentivizing collaboration and preserving data privacy, potentially leading to breakthroughs in disease diagnosis and treatment personalization. Similarly, in climate science, data is dispersed across sensors, smart homes, vehicles, and cities. Sharing this data currently faces problems of regulations and trade secrets (across geographies) and hence requires global collaboration to analyze emission patterns, forecast future scenarios, and implement mitigation strategies.

- **Collaborative and Responsible AI** — Responsible AI development requires multiple entities to ensure safety and auditability throughout the lifecycle of AI systems. The current centralized paradigm makes it challenging to audit the practices of large tech companies or organizations. In contrast, a decentralized ecosystem will promote greater plurality and transparency. By distributing responsibilities and control across multiple entities, decentralized AI reduces the risk of catastrophic failures stemming from a single compromised component. A network of checkpoints and safeguards provides better coverage than a single, monolithic system that must account for all possible contingencies and failures. This distributed approach allows for more robust and dynamic safety measures. Decentralized AI aims to enable greater transparency and verifiability without compromising intellectual property. Organizations can validate their systems and demonstrate compliance with safety standards while protecting proprietary algorithms and trade secrets.

- **Incentivized and Participatory AI** — A decentralized AI ecosystem can lead to a more equitable distribution of technological benefits. The participatory and permissionless nature of these systems allows individuals from diverse demographics to benefit from and contribute to such a system. A key component of Decentralized AI is an algorithmic incentive system that rewards participation based on the quality of data or wisdom shared by each node. This mechanism can foster increased local and global collaborations as more entities are incentivized to participate while safeguarding against exploitation.

- **Improved accessibility of resources** — Decentralized AI can accelerate the development of advanced algorithms and systems by making large swaths of data and computational resources available to individuals and organizations outside big tech companies. Researchers can tap into vast datasets and aggregated statistics, enabling large-scale experiments and hypothesis generation previously only possible for big organizations. By lowering barriers to entry, decentralized AI can significantly reduce friction in innovation for smaller players similar to how the internet and web have facilitated individual participation in various fields.

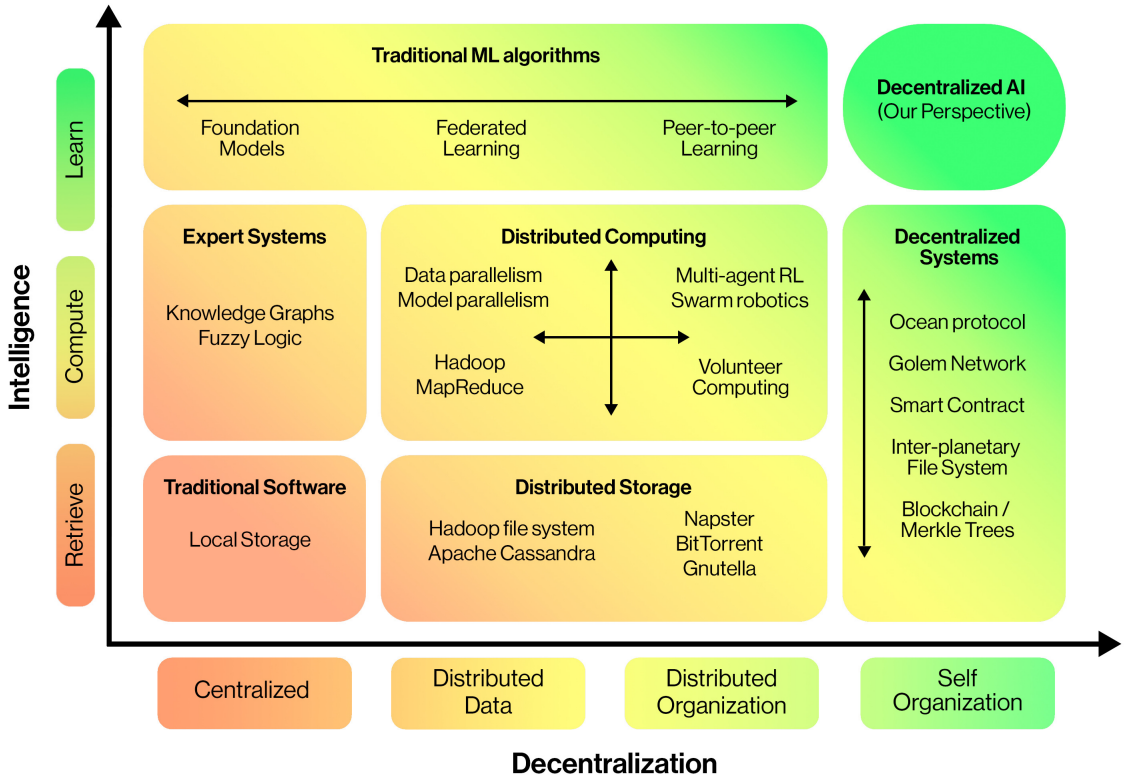

Fig. 2. Landscape of existing paradigms and the path towards self-organized AI. ML algorithms like foundation models excel in AI capabilities but remain centralized. Decentralized systems, like blockchains and volunteer computing, distribute storage and computation but lack intelligence. We argue that combining the benefits of the two capabilities can have an outsized impact. We call upon the AI community to focus on the open challenges in the upper-right quadrant, where decentralized architectures and self-organizing principles can give rise to a new generation of AI systems that are both highly capable and aligned with the values of a decentralized ecosystem.

Inspiration for Decentralized AI: While these technologies offer valuable insights and lay the groundwork for decentralized AI, they are insufficient on their own to address the unique challenges specific to decentralized AI.

- **Federated Learning (FL)** — enables training ML models on decentralized data. However, FL is limited by centralized orchestration, coupling between data and computation ownership, and focusing on model training. To fully realize Decentralized AI, we must extend decentralization to the entire ML lifecycle, decouple data and computation ownership, and address challenges such as incentives, verifiability, and fair attribution. Recent peer-to-peer FL approaches (15) remove centralized orchestration but still focus on collaboratively training neural networks. We consider a broader scope, including synthetic data sharing (16), collaborative inference (17), and more.

- **Web3** — Web3 aims to advance a more decentralized web ecosystem using blockchains. However, blockchains do not address several problems relevant to Decentralized AI (discussed in Sec 4) and have mostly focused on monetary aspects such as cryptocurrency. Nevertheless, several cryptographic approaches used in Web3, such as distributed consensus, zero-knowledge proofs, homomorphic encryption, and multi-party computations, will be important in solving challenges specific to Decentralized AI. Several promising directions have been proposed at the intersection of Web3 and AI (see (18) and Fig2).

- **Distributed AI** — Ideas from the area of distributed computing have been applied to scale deep learning workloads across data centers efficiently. Popular examples include research in data (19), model (20) and pipeline parallelism (21) and companies like AWS, together AI, Databricks, Snowflake etc. These approaches scale well in trusted, well-synchronized, homogeneous, and high-performing compute clusters. In contrast, decentralized AI operates in a regime of trustless, asynchronous, heterogeneous, and low-performing computing devices. Changes in the context introduce unique challenges (see Sec 4).

- **Volunteer computing** — Projects like Folding@home and SETI@home have successfully distributed large-scale computing tasks across geographically distributed machines. However, these systems lack sophisticated verifiability and incentive measures, relying on simple rules like competition credits. Privacy is not a significant challenge, as sensitive

data is not involved in scientific computing workloads. In contrast, Decentralized AI faces unique challenges due to the dynamic and private nature of data (discussed in Sec 4).

- **Open-Source Software (OSS) and Open-access** — Recent advancements in ML research have been fueled by open-source code and models. Platforms like arXiv, GitHub, EleutherAI, and HuggingFace have enabled millions of distributed collaborations, allowing more individuals to participate than any corporation can afford to hire. However, translating the potential of AI requires going beyond the existing open-source paradigm. While OSS has revolutionized software development by making source code accessible and collaborative, machine learning requires collaboration over additional assets, such as datasets, computation, and network infrastructure. Not all of these assets can be made available openly available to the public due to privacy, higher costs etc.

3. Pillars of Decentralized AI

Centralized systems have a few powerful entities in a rigid hierarchy, while decentralized systems have many diverse entities with limited individual resources. Decentralized systems must self-organize to use their collective intelligence effectively. While self-organization in AI has typically been used for distributed coordination at the level of neurons (22) and reinforcement learning (RL) agents (23). We aim to translate the idea of distributed coordination to higher-level entities such as individuals and organizations. Bringing self-organization at this level brings new challenges as each entity now has its own complex motivations and constraints. Returning to Sarah's case, her current health predicament motivates sharing data and spending money to receive care. Yet, privacy considerations mean that she does not want to reveal all of her medical records to an online marketplace. Consider a startup with a proprietary algorithm on this marketplace, motivated to earn by helping to diagnose patients like Sarah. However, releasing the full algorithm to run locally on Sarah's local device could undermine their business advantage. Distributed coordination at the scale of individuals and AI algorithms has unique challenges that need new kinds of interactions. These self-organized interactions are depicted in Fig 1. In this scenario, the entity requiring assets can request them *autonomously* without relying on a central orchestrator to manage access permissions. This exemplifies the concept of self-organization. However, it's important to note that third parties still play a valuable role within this ecosystem. We believe that existing industries and emerging startups could contribute significantly to improving access to relevant resources and services within a Decentralized AI ecosystem.

We believe the path for self-organization should be similar to the development of the internet infrastructure, where standards and protocols exist at several layers ranging from the physical layer to the application layer. Such protocols have enabled any individual to start a website and serve content. While the Internet ecosystem is helped by larger companies, the ecosystem does not fundamentally depend upon these companies. As long as an entity or organization follows agreed-upon standards and protocols, they can participate in this autonomous ecosystem. Considering the challenges of decentralization, five key problems need to be addressed — privacy, verifiability, incentives, orchestration, and Decentralized UI/UX. In our perspective, as shown in Fig. 3, these are the five key pieces that need to come together to enable self-organization between decentralized entities. All these components are deeply intertwined, and interesting challenges exist at their intersection. Next, we describe these components in more detail.

A: Privacy is critical for increasing participation and collaboration over siloed datasets. While centralized, impartial, and trusted brokers can mitigate these concerns, the ultimate aspiration of Decentralized AI systems is to transition towards a *breachless* future where privacy is not only assured but also provable and even if the adversary get access to information, it is sufficiently privatized that the attacker does not learn any new information.

B: Verifiability is an important requirement for decentralized systems that are permissionless and private. Verifiable mechanisms provide protection from and robustness to malicious actors. The problem is particularly challenging with privacy because giving anonymity allows malicious actors to poison the system without any accountability. We believe the algorithms and collaboration need to transition from a trusted and permissioned system to a *trustless* system where legitimate contribution can be proved by contributors and verified by other participants.

C: Incentives can be viewed as a way to significantly enhance the participation of contributors. The primary objective of decentralization is to foster collaboration among entities with distinct assets and objectives. Consequently, motivating contributors to engage and participate in the decentralized system is paramount. Thus, incentive mechanisms must be developed that not only encourage user involvement but also ensure fairness, transparency, and value attribution. Today, large AI companies use a broker-like system to purchase data from other consumer companies or data brokers to train machine learning models. We envision a *brokerless* system that enables coordination between buyers and suppliers to exchange data frictionlessly.

D: Orchestration is essential for enabling coordination between many entities with different assets and objectives. A key dilemma in Decentralized AI is orchestrating collaboration without a centralized orchestrator. The problem with a centralized orchestrator is that of distribution channel and access control. In Sarah's example, if Sarah and all care providers have to go through a single corporation to share health reports and treatment respectively, then the corporation effectively controls and regulates the access to health and treatment. Hence, incentives for all stakeholders will have to be aligned with this central cooperation. This contradicts our goal of enabling coordination between disincentivized entities. We envision a *Coordinatorless* system where a network of individuals and organizations can self-organize and connect autonomously without requiring a single or few bottlenecks.

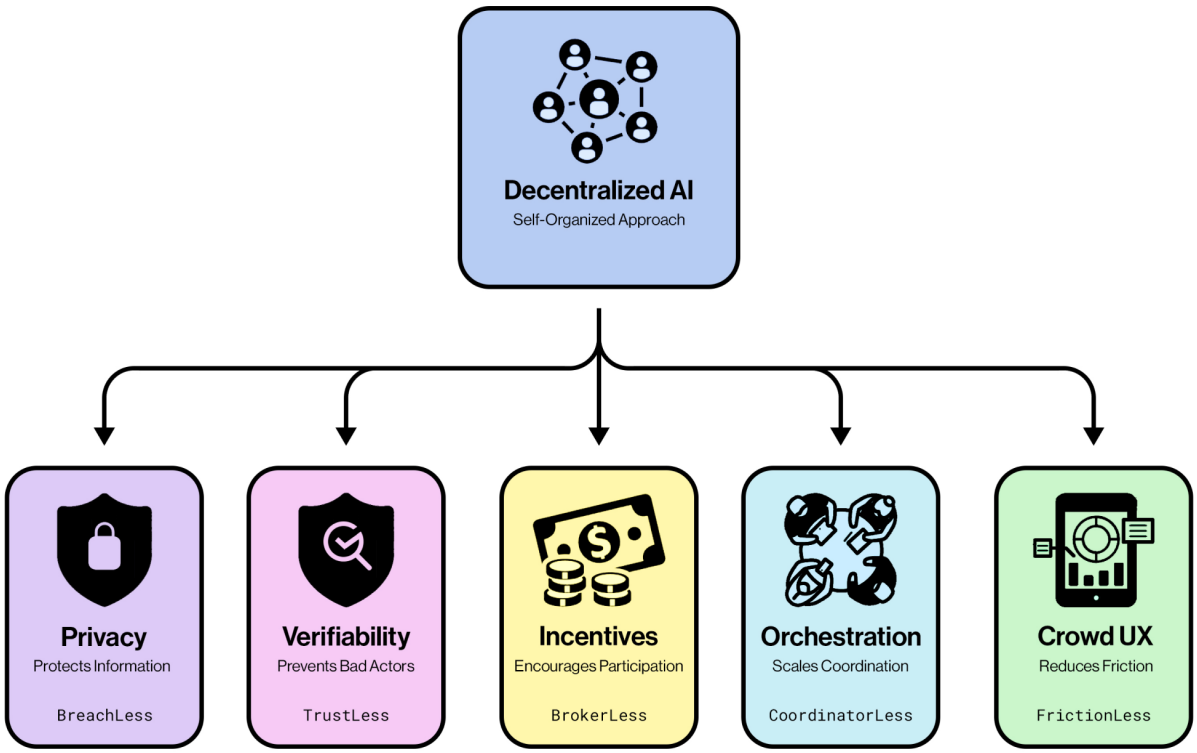

Fig. 3. Five pillars of Decentralized AI. We propose a self-organized approach towards Decentralized AI by bringing together algorithms and systems that enable distrusting, disincentivized, and disorganized entities to collaborate.

E: Crowd UX is the vital interface between Decentralized AI systems and users, promoting adoption and trust. It enables discovery, recommendation, and collaboration among distributed entities without pre-existing relationships. A robust Decentralized UX would allow users like Sarah to easily upload medical data, set preferences, and view diagnoses across various options via interpretable decision support systems. By facilitating collaborations across diverse resources, users needn't understand the complexities of tasks performed by other entities. Examples of centralized systems include marketplaces such as financial exchanges and travel planners such as Expedia that help users to make decisions across a wide variety of choices. We envision a *Frictionless* system that enhances user experience and encourages participation from a large number of entities.

4. Research Opportunities for Decentralized AI

Building upon the key pillars of Decentralized AI, we now shift our focus to specific research challenges that hinder the real-world deployment of Decentralized AI systems. These challenges, derived from the core pillars of Decentralized AI, highlight areas where progress in related fields has been made but require further advancement to address the unique constraints of decentralization. We categorize problems into two categories — 1) problems that are more difficult under the constraints of decentralization, and 2) new problems that emerge in the context of decentralization. We focus more on the second category. While not an exhaustive list, our goal is to highlight significant problems and bring them to the attention of the research community.

A. Privacy Challenge: Private computing over decentralized Data. Existing secure computation techniques such as homomorphic encryption and confidential computing protect the privacy of data during the computation stage. However, secure computation over decentralized data remains practically infeasible. To understand the challenge, let us return to the example of Sarah. Consider a startup that can compute personalized risk for Sarah with an ML model capable of holistically processing different modalities of her health information such as X-ray, DNA, and blood test results. With existing secure computing techniques, Sarah can put all three health records together, encrypt them, and give them to the startup. With existing secure computing techniques, Sarah can aggregate all three health records, encrypt them, and provide them to the startup. The startup can run its proprietary algorithm on the encrypted data and return the encrypted results back to Sarah, which can be decrypted only by Sarah and not even by the startup itself.

While this scenario protects Sarah's privacy while providing high utility, it is only possible because her health information is

centralized at a single location. A more common scenario in today's world is where Sarah's X-ray is present with a hospital, DNA with a DNA testing startup, and her blood test results with a diagnostic company. For such a decentralized data ecosystem, applying secure computing techniques is not trivial and requires addressing several technical challenges.

While techniques like homomorphic encryption (24, 25), secure multi-party computation (MPC) (26, 27), and trusted execution environments (TEEs) (28, 29) have been recently used to perform inference over ML models on encrypted data, they typically assume data originates from a single source. For decentralized data originating from different sources, different fragments of data will be encrypted with different keys making it challenging to run computation on it simultaneously. Analyzing such data requires aggregating disjointed inputs with complex cryptographic key exchanges and extra computation overhead because of non-linear computation over this aggregated input.

The challenge is not only specific to decentralized data belonging to a single user but rather generally applies to the settings where the output of an ML model is dependent on the data from other users. For instance, when applying computation over graph data such as a connection graph in a social network or a treatment-outcome graph in a health graph, the answer to an encrypted input also depends on the other encrypted inputs over the graph. Such decentralized data scenarios are common in siloed and fragmented industries like healthcare, finance, and mobility. Current secure computing paradigms in machine learning have not paid enough attention to this multi-party dynamic.

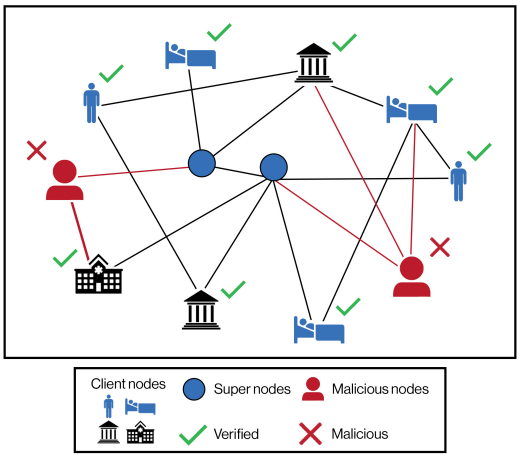

Fig. 4. Identifying and removing malicious actors reduces the need for trust in decentralized AI systems. In a decentralized ecosystem with anonymous participants, malicious actors can report or amplify misleading data or statistics, leading to unintended outcomes. Therefore, guardrails and accountability mechanisms that preserve individual privacy are essential. These measures reduce the need for trusting other participants, encouraging higher participation rates while maintaining system integrity. Drawing inspiration from blockchains, we propose a network of resource-rich super-nodes to enforce these guardrails without compromising the decentralized nature of the system.

B. Verifiability Challenge: Protection against Bad Actors. While fostering collaboration and scalability, the permissionless nature of decentralized AI also introduces vulnerabilities that bad actors can exploit. Different kinds of bad actors with different capabilities and goals can be expected in such a system. Hence, verifiability primitives provide effective guardrails to ensure individuals and organizations can collaborate without having to trust each other.

Malicious attackers: Several known attacks during both individual model training (30) and aggregation (31) threaten the privacy (32–35) and membership (36, 37) of local data contributions. These problems are more challenging in Decentralized AI settings where no trusted central authority oversees the process. Malicious actors can perform model inversion attacks, reconstructing training data and leaking sensitive information from local datasets (38, 39). Beyond privacy, they may tamper with models, introducing backdoor functionality or compromising the updates of other clients (40, 41). Two strategies to protect against bad actors are 1) identification and isolation, and 2) protection against their bad contribution. The first strategy aims to purge the "bad" actors from the system while the second category aims to accept contributions from the "good" actors.

Free riders: Additionally, clients might try to benefit from the value and goods in a decentralized AI ecosystem without contributing anything in return. Free-riding is prevalent in many peer-to-peer systems (42–45) with bad actors employing different strategies based on constraints in the system.

Verifying contributors: Drawing inspiration from trust management systems in the Internet of Things (IoT) (46, 47), we can enhance reliable communication and interactions among participants. Existing proof-based algorithms (48–50) require algorithmically verifiable mechanisms of contribution from the participants. Additionally, several other trust mechanisms have been proposed to defend against model poisoning attacks and increase byzantine robustness (51–53). Reputation mechanisms track a dynamic score for users to identify non-contributing or malicious participants either based on gradient similarity (54) or historical accuracy contributions (55–58). Blockchain-based reputation systems may also be useful in providing more auditable and accountable AI systems by ensuring model integrity and detecting malicious behaviours (59–64).

Participants must verify the uploaded model parameters before performing model aggregation and updates (62, 65). PoW

algorithms can be employed where one party proves to another that it has expended computational resources towards a computation result. Participants either provide proof of training (66) or evidence of the correctness of aggregation results (31).

Tracking contributions: Lastly, developing a decentralized consent mechanism is essential to enable tracking and routing of assets over multiple nodes in a graph. This mechanism should grant participants control over their data, including the right to be forgotten (67). This concept can extend to the verification of machine unlearning (68), ensuring that participants can revoke their contributions when necessary.

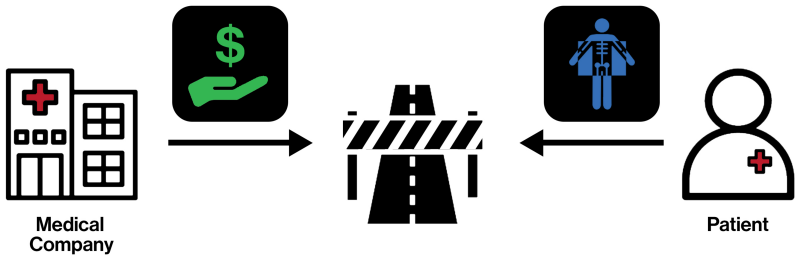

Fig. 5. How to measure the dollar value of data without accessing it? Because data is easily copied, a data owner such as a patient would not allow data access before compensation. However, a data buyer such as a medical company that potentially finds that patient's data valuable would not pay without first being able to assess the value and relevance of the patient's data. This leads to increased friction and search costs in a decentralized data market. New private and federated techniques for data valuation and buyer-seller matching need to be developed to address this roadblock.

C. Incentives Challenge: Data markets and decentralized data governance. Data Markets: Access to large amounts of training data is crucial for the current paradigm of developing foundational models. Therefore, encouraging greater data access will be important to enable AI's impact in areas where data is private, limited, or otherwise restricted, such as in healthcare. Recently, data markets have been promoted to incentivize participants who would not otherwise undergo the costs of processing and sharing data (69–71). Decentralized data markets have the potential to address underlying power imbalances in the current data economy with highly centralized data brokers and AI companies, such as privacy erosion and lack of data consent (12, 13, 72, 73).

Data Valuation: Several challenges need to be solved for decentralized data markets to become a practical reality. The first challenge relates to the discovery and valuation of data in a federated ecosystem. In a perfect market with intermediate brokers, the buyers and sellers could be directly matched through the broker that facilitates each step of the transaction, from validating data value to payment escrow. However, in a decentralized, two-sided marketplace, federated and privacy-preserving strategies are needed to match buyers with sellers and price data (27). Insights from mechanism design, which has been applied in FL settings, could help incentivize desirable behaviors among participants (74, 75). Designing incentive-compatible mechanisms will help prevent adversarial actors that lead to inefficient and undesirable behavior in the marketplace.

Privacy and efficiency: Importantly, these new data discovery and valuation operations cannot assume "white-box" access to the seller's data (76), as data can be easily copied otherwise (see Arrow's Information Paradox (77)). In addition to relying on centralized data access, current data valuation approaches, such as Data Shapley (78), are also costly to compute since many models need to be trained on different data subsets to estimate the value of datapoints. New decentralized valuation algorithms must be scalable and cheap to compute, even for large datasets with billions of datapoints.

Decentralized data governance is a major challenge that entails the management of data controls and consent among many distributed data owners. For instance, how does a pharmaceutical company targeting a rare disease obtain access to the data of thousands of patients with the condition distributed around the world? Each patient would not have the time, energy, or resources to engage in negotiations with every company that wants to use their data. New data governance models, such as decentralized autonomous organizations, data cooperatives, and data unions, could provide mechanisms for collective oversight and stewardship of aggregated data (79). These data intermediates could act as fiduciaries for patient interests and collectively bargain for patients to have increased leverage with interested parties such as commercial companies (80).

Consent: This governing body could also assist with educating its members on data rights and managing data consent and access preferences for each individual. For instance, a meta-consent mechanism could allow greater fine-grained data controls by specifying higher-level preferences for different contexts and avoid the need to obtain specific consent for every secondary use (81, 82). Patients should be able to leave the bargaining unit and take their data with them; ideally, they would also have freedom of choice between multiple data collectives that best match their preferences and goals (83). Additionally, AI governance models inspired by decentralized autonomous organizations may help communities vote and reach consensus on how data is acquired and how models are trained and deployed (84).

D. Orchestration Challenges: Coordinating Training and Managing Heterogeneous Resources. The key challenges in coordinating the training of an ML model over distributed data and compute become apparent in the absence of a centralized coordinator. In federated learning, a central server coordinates a fleet of clients, however, a central coordinator introduces similar issues to those in centralized learning — faith in a single entity, limitations in terms of the available resources, and governance of the model. Instead, decentralized FL works for peer-to-peer (P2P) communication between clients (85, 86). This introduces a new set of challenges, as clients now require *self-coordination*.

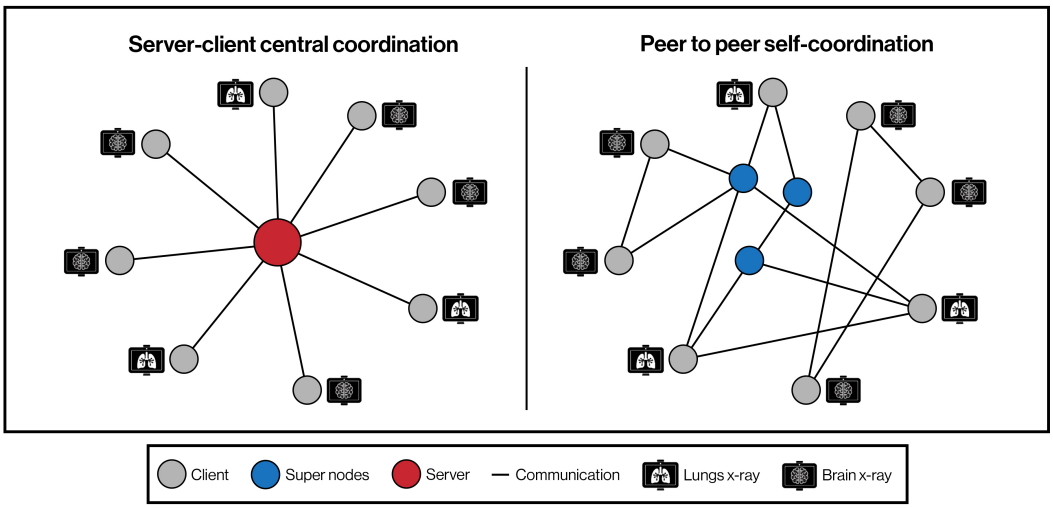

Fig. 6. Self-coordination for decentralized collaborative learning. Current collaborative learning approaches, such as federated learning, rely on a central coordinator or assume a fixed topology. However, in a decentralized network, users can freely interact and exchange information, leading to a diverse set of participants with heterogeneous tasks, data distributions, and privacy preferences. This heterogeneity poses challenges for effective collaboration. In the given example, patient data can be separated into homogeneous clusters, improving the quality of collaboration. To address these challenges, a "smart routing" mechanism is needed to enable users to efficiently extract relevant information from the vast amounts of decentralized data. By dynamically adapting the collaboration topology based on user similarities and information relevance, our approach optimizes the learning process in a self-coordinated manner without relying on a central authority.

Data Heterogeneity: In decentralized learning, heterogeneous collaboration poses a major challenge that afflicts both data and model architectures. Data varies in terms of distribution, scale, and features, leading to challenges in aggregating information cohesively. For instance, medical data varies greatly in scale and source, from electronic health records to wearable devices, spanning different geographies and populations, which makes harmonization and training more difficult. Recent studies (87–92) show that FL with heterogeneous data (not independent and identically distributed, i.e. non-IID) result in slow training convergence and suboptimal performance compared to IID data. Most work addressing data heterogeneity in FL relies upon a centralized server to "correct" individuals' contributions, which becomes difficult to apply in decentralized settings without a central orchestrator.

Model Heterogeneity: There is often also significant heterogeneity in terms of model architecture in decentralized setups, where each user is equipped with varying compute resources and bandwidth capabilities. We believe that Decentralized AI platforms should accommodate this diversity of resources rather than mandating uniform standards. Incorporating this heterogeneity enhances inclusivity and adaptability across users but also creates interoperability roadblocks that complicate collaboration. For instance, most FL techniques require identical models or the same family of model architecture, limiting coordination between heterogeneous resources. More adaptive aggregation techniques need to be developed that enable interoperability between customized models and specialized representational spaces at scale. For instance, decentralized methods could integrate knowledge across data and architectural modalities with minimal conformity requirements through synthetic data representations from trained model weights (93).

Collaborator selection: How can clients with limited resources strategically choose their collaborators at scale? Current systems mostly rely on random communication (94); however, this greatly suffers from the heterogeneity in the clients' data distributions. In the context of non-IID data, some approaches assign *trust* or collaboration weights to other clients, either by learning them (95), measuring similarity on an unlabelled public dataset (96), or by clustering clients (97). Another related challenge involves how to orchestrate virtual super-nodes (commonly used in P2P systems) to assist in client coordination. Super-nodes are used to validate, store, and relay the ledger state in Bitcoin or to resolve domain names (DNS servers) in the case of the Internet. In the context of collaborative learning, how can these super-nodes accumulate and distribute useful information to users who will join and drop out on a need-to-need basis? The question of client drop-out and, more generally, heterogeneity in the clients' availability, responsiveness, and resources are also raised in FL. Slow clients impede the overall convergence rate, and heterogeneity leads to system-induced bias, such as over-representing certain demographics with high internet quality (90).

Asynchronous computing: How can geographically distributed computing devices can train a model together? Addressing this challenge requires eliminating communication bottlenecks and synchronization among parameters in the training procedure. When performing the sequential computation of neural networks across multiple nodes with the standard forward and backward propagation, there are two problems: 1) under-utilization of nodes because only one partition is active at a time and 2) the requirement of synchronous communication across nodes since each node depends upon data from neighboring nodes. The first problem has been studied extensively because it allows the training of large models within a single data center with many GPU nodes by reducing the idle time for each node and communication between nodes. The solution to the first problem involves a certain kind of parallelization such as data parallelism (98), tensor parallelism (99), pipeline parallelism (100–102) and hybrid modes of parallelism (103). However, unlike a data center where nodes are connected via a high bandwidth and low

latency communication network (for example, InfiniBand), decentralized AI requires parallelizing computation when nodes are connected via a low bandwidth and high latency global network. Enabling computation in this scenario requires eliminating synchronization bottlenecks — a challenging task due to the synchronous nature of backpropagation. Except for a few recent works (104), the second problem of communication synchronization has not attracted as much attention. We believe making the training process more asynchronous is essential for geographically distributed nodes with different partitions of data and parameters to collaboratively train large neural networks.

E. Crowd-sourced UX challenge: Platforms for Decentralized Interaction. The research challenge in this category lies in making large-scale decentralized systems compatible with intuitive user interfaces. For instance, how can Sarah choose a relevant care provider from multiple diagnostic model providers in a decentralized marketplace? How can the system convey the privacy-utility trade-offs effectively to Sarah? How can we design data markets that help Sarah understand the value of her contribution and participation in the ecosystem?

A key research challenge lies in creating a decision support system that is interpretable and explainable while involving interaction and collaboration with a large number of decentralized assets. Returning to Sarah's example, consider thousands of model providers each with their trade-offs along cost, privacy, and accuracy. Designing a decision support system for Sarah so that she can share her information securely, understand trade-offs, and augment her care providers with actionable information requires a system design approach that works for multiple stakeholders simultaneously. Existing works (105, 106) in the context of healthcare, have looked at the problem from a clinical validity and interpretability point of view. However, we would like to draw researchers' attention to challenges arising due to decentralized data and models.

An analogy can be drawn from internet technologies such as browsers, domain name servers (DNS), and secure sockets layer (SSL) protocols, which authenticate websites and ensure secure communication. While the absence of these technologies would not preclude internet use, their accessibility and usability have contributed to the widespread adoption of the internet. Similarly, the utility of Decentralized AI hinges on widespread participation from individuals and, ultimately, on the interfaces that reduce friction in participation.

F. Overall Challenge: Standards. While the previous challenges focused on algorithms to enable decentralization, well-defined, agreed-upon standards are equally important for the practical deployment of these algorithms. Similar to the suite of standards (TCP/IP) that enable today's internet, we need standards for the aforementioned five pillars. They will enable interoperability between different interfaces and hardware utilized by different entities, such as individuals and institutions. We anticipate these standards might be domain-specific and rely upon existing standards such as FHIR (107) for electronic health records, DICOM (108) for medical imaging, COSMOS (109) for blockchain interoperability. Insights from existing machine learning standards and benchmarking can carry over to designing Decentralized AI benchmarks (110, 111).

Standards will also help increase trust and security in a decentralized ecosystem. For instance, a protocol that provides differential privacy needs to have an agreement protocol that ensures both parties agree on a privacy budget. Similarly, an MPC-based confidential computing protocol needs agreement on cryptographic keys and related metadata in order to work effectively. The need for these protocols and standards only appears when no central institution regulates the interaction between entities. Examples include the Robot Exclusionary Standard (112), which is based on voluntary compliance, the ONNX (113) format that allows transforming neural network models across different libraries, and SSL protocol (114) that creates encrypted communication channels between applications.

5. Opportunities and Impact of Decentralized AI

Healthcare and AI A recent work by (115) identifies five key challenges that need to be addressed for obtaining a generalist medical artificial intelligence (GMAI) that advances current medical AI models. Quoting the authors -

> *We also describe critical challenges that must be addressed to ensure safe deployment, as GMAI models will operate in particularly high-stakes settings, compared to foundation models in other fields.*

Now we discuss these challenges one by one and provide key insights on how decentralized AI can help in addressing some of these challenges. We note that innovation in decentralized AI would not completely eliminate these issues but alleviate several of these concerns meaningfully.

- Validation — The authors note that existing benchmarking techniques are designed for ML models that solve only one task. In contrast, healthcare foundational models are expected to be used for several purposes. Using decentralized AI to perform distributed inference over secure data, validators can evaluate the model's performance without sharing raw data with model providers. This, in turn, prevents model providers from overfitting on evaluation data because the evaluation data is not visible to them. Simultaneously, model validators do not have access to all of the model parameters, hence, the model providers do not have to worry about sharing their proprietary assets. Additionally, we argue that decentralized AI will result in millions of models that are personalized for different user groups and hence model personalization would alleviate the critical reliance on model validation.

- Verification — The problem of verification focuses on explainability and interpretability that helps decision makers such as clinicians to work synergistically with the system. We highlight this research challenge in crowd UX E. While decentralized AI does not address the problem of interpretability and hallucination in ML, we argue that addressing

the crowd UX challenge enhances the trust and accessibility of the system. Specifically, a successful deployment of the crowdUX system would allow a patient like Sarah to connect with her general physician, pathologist, and other experts along the different stages of her patient journey.

- Social biases — The authors argue that social bias in model predictions can increase with the model scale, making the model's utility worse for minority demographics and rare diseases. The permissionless and incentivized nature of decentralized AI can partially alleviate this concern. We highlight several challenges around the orchestration of data and models to improve model performance on heterogeneous data and perform collaborator selection to identify the most relevant model for a given demographic.
- Privacy — The authors note that foundation models can pose serious privacy risks for the patients because they will capture a rich set of multi-modal information about the patients. Privacy enhancement, being one of the key pillars of decentralized AI, can help alleviate all of the privacy concerns associated with the training and deployment of foundation models for healthcare.
- Scale — The authors highlight three critical factors when moving from a small task-specialist model paradigm to a generalist large foundation model paradigm - 1) Data acquisition cost, 2) Model training cost, and 3) Deployment cost. All three costs can be dramatically reduced with the help of appropriate incentives and privacy-preserving mechanisms that allow individuals to join a network and contribute their data or computation in a verifiable manner. The current system of acquiring data either requires web scraping (that does not include most healthcare data) or going via data brokers (an inefficient system). We instead argue for a brokerless vision for decentralized AI where individuals and organizations can share data and get rewarded appropriately.

Opportunities in decentralized AI are not just limited to healthcare but also enable application in several other industries that involve multiple stakeholders and fragmented information ecosystems -

Finance is poised to benefit from a decentralized ecosystem because like healthcare, data and insights stay isolated in siloes due to regulatory constraints. By addressing the challenge of privacy-preserving analytics over decentralized data, banks and financial institutions can collaborate on fraud detection, credit scoring, and risk assessment without sharing sensitive customer data. This allows for more robust models while maintaining regulatory compliance and customer privacy. Beyond, transactions, peer-to-peer lending platforms can leverage verifiability mechanisms in decentralized AI to assess creditworthiness across multiple data sources without centralizing sensitive information.

Supply Chain can be enhanced by integrating data across multiple jurisdictions and creating orchestration algorithms that improve traceability and risk assessment. Specifically, end-to-end visibility can be improved if companies across the supply chain can share data and insights without exposing sensitive information, leading to better demand forecasting and inventory management. Quality control and traceability can be improved with collaborative learning across multiple parties to improve product quality and traceability without centralizing proprietary manufacturing data. Organizations can work together to optimize for sustainability metrics by route optimization and capacity planning without exposing competitive information about their operations.

Decentralized orchestration platforms can coordinate just-in-time production and logistics across multiple factories and carriers, optimizing resource utilization. Crowd UX innovations can allow small suppliers and individual consumers to easily participate in and benefit from these complex, global supply chains through user-friendly interfaces and mobile apps.

Mobility can be improved by integrating data at a population scale. Cities and transportation agencies can collaborate on traffic prediction and management without centralizing sensitive data about individual movements. Data markets can be used to create incentives for people to participate and contribute their movement data. Similarly, Car manufacturers and tech companies can pool data to improve autonomous driving algorithms while protecting proprietary technologies. Verifiability mechanisms can ensure the integrity and provenance of shared data, critical for the safety and reliability of autonomous systems.

Transit agencies can work together using orchestration algorithms to optimize routes and schedules across regions without centralizing all operational data. Finally, energy companies and automotive manufacturers can collaborate on optimizing charging station placement and usage without sharing sensitive market data.

6. Risks of Decentralization

This paper advocates decentralizing the entire machine learning pipeline, citing the numerous advantages this confers over centralized systems. However, we want to be careful not to paint decentralization as a utopian panacea devoid of its own unique challenges. On the contrary, decentralizing AI does not solve many problems that AI systems face, such as hallucination, bias, etc. Furthermore, decentralization introduces new distinct problems and dangers that the community must navigate judiciously. Fig. 7 shows two key dimensions of risks in Decentralized AI. The debate parallels that between free market versus centrally planned economic systems, where both extremes have their unique pitfalls, yet one paradigm is more tenable. We discuss certain hazards intrinsic to Decentralized AI and propose potential mitigation strategies. Our goal is not to present decentralization as an idyllic solution but rather to have an honest dialogue about its merits and difficulties so we may adopt it judiciously where appropriate. By scrutinizing its drawbacks and self-correcting course accordingly, we can realize the many benefits of Decentralized AI while containing its risks.

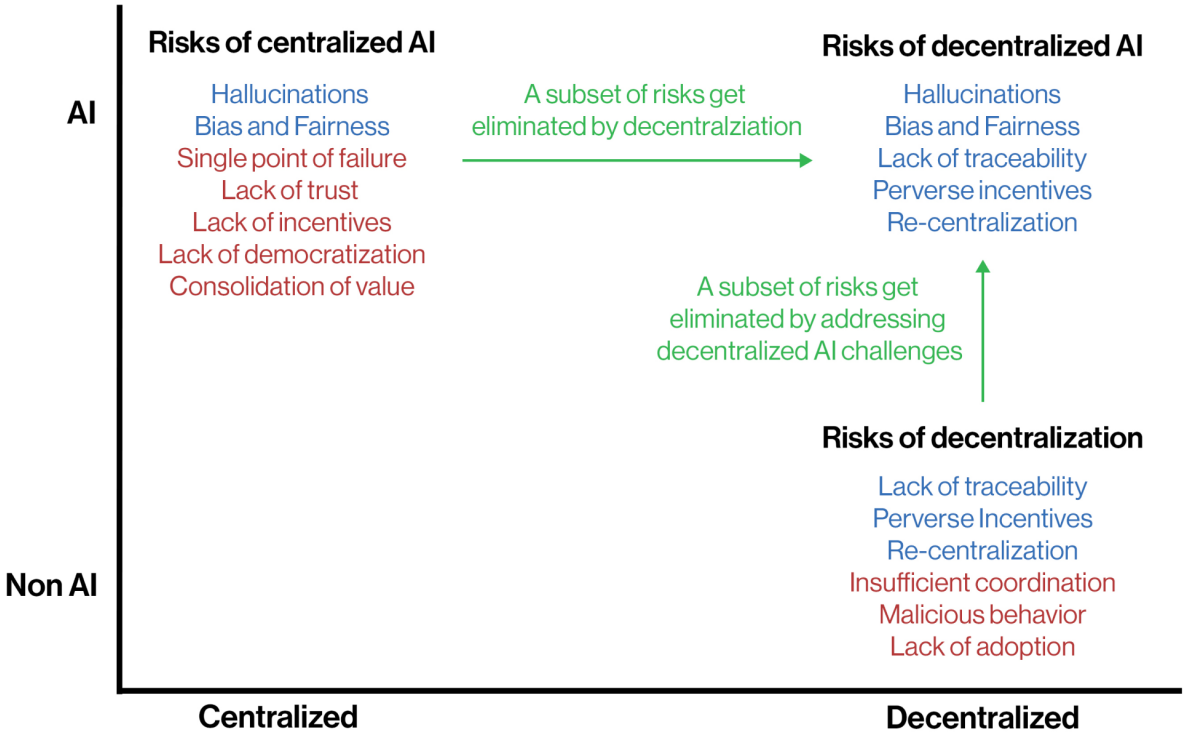

Fig. 7. Risks of Decentralized AI: There are several risks associated with AI. A subset of them can be eliminated by introducing decentralization in the system. However, decentralization itself introduces new risks. We have discussed technical problems to address some of these risks, but a subset of the risks introduced by decentralization are expected to creep into any Decentralized AI system. Do the benefits outweigh the risks?

Lack of Traceability: Decentralizing machine learning development and deployment minimizes dependence on centralized institutions. This facilitates collaboration among entities that otherwise lack mutual trust, incentive, or coordination. However, it also becomes less clear where the fault lies if things go awry. Without a central authority, the system lacks an accountable linchpin. This trade-off is fundamental. The autonomy afforded by decentralization is defined partly by the absence of overarching control. Still, for a decentralized system to remain reliably self-correcting, it must incorporate safeguards and accountability chains that trace culpability to specific sources when necessary. Enabling anonymity and confidentiality while still embedding auditability is an open research challenge. Achieving this balance will allow decentralized systems to mitigate misconduct through collective self-policing rather than top-down intervention. The solutions will likely involve cryptographic schemes that certify origin and intent without compromising privacy and game theoretic interactions that incentivize good behavior.

Perverse Incentives: Currently, many individuals and organizations donate resources to collective efforts like open datasets and volunteer computing purely for altruistic reasons. As we build explicit incentive structures to reward contributions in decentralized systems, this risks crowding out altruism and diminishing participation from those seeking help rather than profit.

There is a behavioral phenomenon (116, 117) where extrinsic rewards can override intrinsic motivations over time. When we compensate people for activities they once did voluntarily, they tend to lose intrinsic interest in those activities later on. As such, designing effective incentive programs for decentralized networks requires careful consideration of community norms, social motivations, and human psychology alongside conventional economic factors. The goal should be complementing extant altruism without supplanting it. Hybrid approaches that balance incentives with opportunities for voluntary participation could help avoid crowding out those driven by intrinsic motivations.

Consolidation by Re-centralization: Decentralized systems can unintentionally re-centralize over time if adequate safeguards are lacking. Dominant centralized institutions may emerge organically, which is not inherently problematic. However, this does risk reconstituting the issues of freedom and competition that decentralization aims to resolve.

For instance, cryptocurrency exchanges have become centers of immense centralized control, and services like FreeBasics have threatened to bypass net neutrality (118, 119). Such re-centralizing forces can increase efficiency but simultaneously undermine decentralization's openness. Therefore, decentralized networks should institute mechanisms that allow dominant players to operate but maintain ease of entry and participation by individuals and startups. Architecting frictionless competition is key. As certain centralized institutions inevitably gain prominence, decentralized systems must facilitate alternative providers challenging their primacy. This could involve decoupling platform interoperability from these powerful intermediaries, implementing trust-minimized open standards, and not locking users into proprietary formats. By designing infrastructure independent of specific intermediaries, re-centralization can be prevented.

The intent is not to artificially prop up decentralization where centralization is more efficient. Rather, both should organically co-exist in balance. If decentralized participation remains simple, open, and impartial, dominant institutions will rise and fall based on merit rather than monopolistic factors. This dynamism provides the right incentives for innovation within centralized players as well, creating a vibrant, evolving ecosystem.

7. Conclusion

In conclusion, this paper has elucidated the merits, use cases, and challenges of decentralized AI. We have argued that decentralizing AI development can unlock previously inaccessible data and computing resources, enabling AI systems to flourish in data-sensitive domains such as healthcare. We have presented a self-organizing perspective and argue that five key components need to come together to enable self-organization between decentralized entities: privacy, verifiability, incentives, orchestration, and crowd UX. This self-organized approach addresses several limitations of the current centralized paradigm, which relies heavily on consolidation and trust in a few dominant entities. The convergence of recent trends — including the rise of personal AI assistants, advancements in on-device computing, and the development of sophisticated cryptographic and statistical mechanisms for privacy and verifiability — creates an opportune moment to synthesize these primitives into a practical decentralized AI framework. We posit that decentralized AI has the potential to empower individuals, catalyze innovation, and shape a future where AI benefits society at large.

References

1. Adrian Kingsley-Hughes. What is an ai pc? (and should you buy one?). *ZDNet*, 2024. URL https://www.zdnet.com/article/what-is-an-ai-pc-and-should-you-buy-one/.
2. Luke Lango. Why ai will drive major pc market growth in 2024. *InvestorPlace*, 2023.
3. Ishan Dutt and Kieren Jessop. Now and next for the pc market in 2024. *Canalysis*, 2024. URL https://canalys.com/newsroom/ai-pc-market-2024.
4. Matei Zaharia, Omar Khattab, Lingjiao Chen, Jared Quincy Davis, Heather Miller, Chris Potts, James Zou, Michael Carbin, Jonathan Frankle, Naveen Rao, and Ali Ghodsi. The shift from models to compound ai systems. https://bair.berkeley.edu/blog/2024/02/18/compound-ai-systems/, 2024.
5. Qiuyuan Huang, Naoki Wake, Bidipta Sarkar, Zane Durante, Ran Gong, Rohan Taori, Yusuke Noda, Demetri Terzopoulos, Noboru Kuno, Ade Famoti, et al. Position paper: Agent ai towards a holistic intelligence. *arXiv preprint arXiv:2403.00833*, 2024.
6. Aoran Jiao, Tanmay P Patel, Sanjmi Khurana, Anna-Mariya Korol, Lukas Brunke, Vivek K Adajania, Utku Culha, Siqi Zhou, and Angela P Schoellig. Swarm-gpt: Combining large language models with safe motion planning for robot choreography design. *arXiv preprint arXiv:2312.01059*, 2023.
7. Daniel Hooven. $1 Billion a Day: Unpacking the Financial Aftershock of the Change Healthcare Cyber-Attack. https://www.schneiderdowns.com/our-thoughts-on/the-financial-aftershock-of-change-healthcare-cyberattack, 2024.
8. Mack DeGeurin. Hackers got nearly 7 million people's data from 23andMe. https://www.theguardian.com/technology/2024/feb/15/23andme-hack-data-genetic-data-selling-response, 2024.
9. Noam Wasserman. Openai's failed experiment in governance. *Harvard Business Review*, 2023. URL https://hbr.org/2023/11/openais-failed-experiment-in-governance.
10. Megan McArdle. Female popes? google's amusing ai bias underscores a serious problem. *Washington Post*, 2024. URL https://www.washingtonpost.com/opinions/2024/02/27/google-gemini-bias-race-politics/.
11. Michael Grynbaum, M. and Ryan Mac. The Times Sues OpenAI and Microsoft Over A.I. Use of Copyrighted Work. https://www.nytimes.com/2023/12/27/business/media/new-york-times-open-ai-microsoft-lawsuit.html, 2023.
12. Joseph Saveri and Matthew Butterick. Stable diffusion litigation. https://stablediffusionlitigation.com, 2024. Accessed: 2024-06-03.
13. Joseph Saveri and Matthew Butterick. Github copilot litigation. https://githubcopilotlitigation.com, 2024. Accessed: 2024-06-03.
14. Chris Dixon. Read write own. building the next era of the internet. https://readwriteown.com/, 2024.
15. Liangqi Yuan, Lichao Sun, Philip S Yu, and Ziran Wang. Decentralized federated learning: A survey and perspective. *arXiv preprint arXiv:2306.01603*, 2023.
16. André Bauer, Simon Trapp, Michael Stenger, Robert Leppich, Samuel Kounev, Mark Leznik, Kyle Chard, and Ian Foster. Comprehensive exploration of synthetic data generation: A survey. *arXiv preprint arXiv:2401.02524*, 2024.
17. Abhishek Singh, Praneeth Vepakomma, Vivek Sharma, and Ramesh Raskar. Posthoc privacy guarantees for collaborative inference with modified propose-test-release. *Advances in Neural Information Processing Systems*, 36, 2024.
18. Vitalik Buterin. The promise and challenges of crypto + ai applications. https://vitalik.eth.limo/general/2024/01/30/cryptoai.html, 2024.
19. Marcel Aach, Eray Inanc, Rakesh Sarma, Morris Riedel, and Andreas Lintermann. Large scale performance analysis of distributed deep learning frameworks for convolutional neural networks. *Journal of Big Data*, 10(1):96, 2023.
20. Felix Brakel, Uraz Odyurt, and Ana-Lucia Varbanescu. Model parallelism on distributed infrastructure: A literature review from theory to llm case-studies. *arXiv preprint arXiv:2403.03699*, 2024.
21. Daniel Nichols, Siddharth Singh, Shu-Huai Lin, and Abhinav Bhatele. A survey and empirical evaluation of parallel deep learning frameworks. *arXiv preprint arXiv:2111.04949*, 2021.
22. Teuvo Kohonen. Self-organized formation of topologically correct feature maps. *Biological cybernetics*, 43(1):59–69, 1982.
23. David Ha and Yujin Tang. Collective intelligence for deep learning: A survey of recent developments. *Collective Intelligence*, 1(1):26339137221114874, 2022.
24. Chiara Marcolla, Victor Sucasas, Marc Manzano, Riccardo Bassoli, Frank HP Fitzek, and Najwa Aaraj. Survey on fully homomorphic encryption, theory, and applications. *Proceedings of the IEEE*, 110(10):1572–1609, 2022.
25. Zoltán Ádám Mann, Christian Weinert, Daphnee Chabal, and Joppe W Bos. Towards practical secure neural network inference: the journey so far and the road ahead. *ACM Computing Surveys*, 56 (5):1–37, 2023.
26. Yehuda Lindell. Secure multiparty computation. *Communications of the ACM*, 64(1):86–96, 2020.
27. Mengxiao Zhang, Fernando Beltrán, and Jiamou Liu. A survey of data pricing for data marketplaces. *IEEE Transactions on Big Data*, 2023.
28. Xiaoguo Li, Bowen Zhao, Guomin Yang, Tao Xiang, Jian Weng, and Robert H Deng. A survey of secure computation using trusted execution environments. *arXiv preprint arXiv:2302.12150*, 2023.
29. Antonio Muñoz, Ruben Rios, Rodrigo Román, and Javier López. A survey on the (in) security of trusted execution environments. *Computers & Security*, 129:103180, 2023.
30. Jungwuk Park, Dong-Jun Han, Minseok Choi, and Jaekyun Moon. Sageflow: Robust federated learning against both stragglers and adversaries. *Advances in neural information processing systems*, 34:840–851, 2021.
31. Guowen Xu, Hongwei Li, Sen Liu, Kan Yang, and Xiaodong Lin. Verifynet: Secure and verifiable federated learning. *IEEE Transactions on Information Forensics and Security*, 15:911–926, 2019.
32. Shuang Song, Kamalika Chaudhuri, and Anand D Sarwate. Stochastic gradient descent with differentially private updates. In *2013 IEEE global conference on signal and information processing*, pages 245–248. IEEE, 2013.
33. Lingjuan Lyu, Han Yu, and Qiang Yang. Threats to federated learning: A survey. *arXiv preprint arXiv:2003.02133*, 2020.
34. Yingqi Liu, Shiqing Ma, Yousra Aafer, Wen-Chuan Lee, Juan Zhai, Weihang Wang, and Xiangyu Zhang. Trojaning attack on neural networks. In *25th Annual Network And Distributed System Security Symposium (NDSS 2018)*. Internet Soc, 2018.
35. Weilin Xu, David Evans, and Yanjun Qi. Feature squeezing: Detecting adversarial examples in deep neural networks. *arXiv preprint arXiv:1704.01155*, 2017.
36. Reza Shokri, Marco Stronati, Congzheng Song, and Vitaly Shmatikov. Membership inference attacks against machine learning models. In *2017 IEEE symposium on security and privacy (SP)*, pages 3–18. IEEE, 2017.
37. Briland Hitaj, Giuseppe Ateniese, and Fernando Perez-Cruz. Deep models under the gan: information leakage from collaborative deep learning. In *Proceedings of the 2017 ACM SIGSAC conference on computer and communications security*, pages 603–618, 2017.
38. Matthew Fredrikson, Eric Lantz, Somesh Jha, Simon Lin, David Page, and Thomas Ristenpart. Privacy in pharmacogenetics: An end-to-end case study of personalized warfarin dosing. In *Proceedings of the 23rd USENIX Conference on Security Symposium*, SEC'14, page 17–32, USA, 2014. USENIX Association. ISBN 9781931971157.
39. Matt Fredrikson, Somesh Jha, and Thomas Ristenpart. Model inversion attacks that exploit confidence information and basic countermeasures. In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, CCS '15, page 1322–1333, New York, NY, USA, 2015. Association for Computing Machinery. ISBN 9781450338325. . URL https://doi.org/10.1145/2810103.2813677.
40. Eugene Bagdasaryan, Andreas Veit, Yiqing Hua, Deborah Estrin, and Vitaly Shmatikov. How to backdoor federated learning. In Silvia Chiappa and Roberto Calandra, editors, *Proceedings of the Twenty Third International Conference on Artificial Intelligence and Statistics*, volume 108 of *Proceedings of Machine Learning Research*, pages 2938–2948. PMLR, 8 2020. URL https://proceedings.mlr.press/v108/bagdasaryan20a.html.
41. Arjun Nitin Bhagoji, Supriyo Chakraborty, Prateek Mittal, and Seraphin Calo. Analyzing federated learning through an adversarial lens, 2019.
42. Lingjuan Lyu, Jiangshan Yu, Karthik Nandakumar, Yitong Li, Xingjun Ma, Jiong Jin, Han Yu, and Kee Siong Ng. Towards fair and privacy-preserving federated deep models. *IEEE Transactions on Parallel and Distributed Systems*, 31(11):2524–2541, 2020.
43. Michal Feldman and John Chuang. Overcoming free-riding behavior in peer-to-peer systems. *ACM sigecom exchanges*, 5(4):41–50, 2005.
44. Jierui Lin, Min Du, and Jian Liu. Free-riders in federated learning: Attacks and defenses. *arXiv preprint arXiv:1911.12560*, 2019.
45. Yann Fraboni, Richard Vidal, and Marco Lorenzi. Free-rider attacks on model aggregation in federated learning. In *International Conference on Artificial Intelligence and Statistics*, pages 1846–1854. PMLR, 2021.
46. Han Yu, Zhiqi Shen, Cyril Leung, Chunyan Miao, and Victor R. Lesser. A survey of multi-agent trust management systems. *IEEE Access*, 1:35–50, 2013. .
47. Ikram Ud Din, Mohsen Guizani, Byung-Seo Kim, Suhaidi Hassan, and Muhammad Khurram Khan. Trust management techniques for the internet of things: A survey. *IEEE Access*, 7:29763–29787, 2019. .
48. Cynthia Dwork and Moni Naor. Pricing via processing or combatting junk mail. In *Annual international cryptology conference*, pages 139–147. Springer, 1992.
49. Adam Back et al. Hashcash-a denial of service counter-measure. 2002.
50. Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. 2008.
51. Anousheh Gholami, Nariman Torkzaban, and John S. Baras. Trusted decentralized federated learning. In *2022 IEEE 19th Annual Consumer Communications & Networking Conference (CCNC)*, pages 1–6, 2022. .
52. Xiaoyu Cao, Minghong Fang, Jia Liu, and Neil Zhenqiang Gong. Fltrust: Byzantine-robust federated learning via trust bootstrapping. *arXiv preprint arXiv:2012.13995*, 2020.
53. Leslie Lamport, Robert Shostak, and Marshall Pease. The byzantine generals problem. In *Concurrency: the works of leslie lamport*, pages 203–226. 2019.
54. Xinyi Xu and Lingjuan Lyu. A reputation mechanism is all you need: Collaborative fairness and adversarial robustness in federated learning. *arXiv preprint arXiv:2011.10464*, 2020.
55. Zelei Liu, Yuanyuan Chen, Han Yu, Yang Liu, and Lizhen Cui. Gtg-shapley: Efficient and accurate participant contribution evaluation in federated learning. *ACM Transactions on Intelligent Systems and Technology (TIST)*, 13(4):1–21, 2022.
56. Zelei Liu, Yuanyuan Chen, Yansong Zhao, Han Yu, Yang Liu, Renyi Bao, Jinpeng Jiang, Zaiqing Nie, Qian Xu, and Qiang Yang. Contribution-aware federated learning for smart healthcare. In

Proceedings of the AAAI Conference on Artificial Intelligence, volume 36, pages 12396–12404, 2022.
57. Yue Zou, Fei Shen, Feng Yan, Jing Lin, and Yunzhou Qiu. Reputation-based regional federated learning for knowledge trading in blockchain-enhanced iov. In *2021 IEEE wireless communications and networking conference (WCNC)*, pages 1–6. IEEE, 2021.
58. Yuwei Wang and Burak Kantarci. A novel reputation-aware client selection scheme for federated learning within mobile environments. In *2020 IEEE 25th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD)*, pages 1–6. IEEE, 2020.
59. Muhammad Habib ur Rehman, Ahmed Mukhtar Dirir, Khaled Salah, Ernesto Damiani, and Davor Svetinovic. Trustfed: A framework for fair and trustworthy cross-device federated learning in iiot. *IEEE Transactions on Industrial Informatics*, 17(12):8485–8494, 2021. .
60. Xianglin Bao, Cheng Su, Yan Xiong, Wenchao Huang, and Yifei Hu. Flchain: A blockchain for auditable federated learning with trust and incentive. In *2019 5th International Conference on Big Data Computing and Communications (BIGCOM)*, pages 151–159, 2019. .
61. Hajar Moudoud, Soumaya Cherkaoui, and Lyes Khoukhi. Towards a secure and reliable federated learning using blockchain. In *2021 IEEE Global Communications Conference (GLOBECOM)*, pages 01–06. IEEE, 2021.
62. Yang Zhao, Jun Zhao, Linshan Jiang, Rui Tan, and Dusit Niyato. Mobile edge computing, blockchain and reputation-based crowdsourcing iot federated learning: A secure, decentralized and privacy-preserving system. *arXiv preprint arXiv:1906.10893*, pages 2327–4662, 2019.
63. Muhammad Habib ur Rehman, Khaled Salah, Ernesto Damiani, and Davor Svetinovic. Towards blockchain-based reputation-aware federated learning. In *IEEE INFOCOM 2020-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, pages 183–188. IEEE, 2020.
64. Jiawen Kang, Zehui Xiong, Dusit Niyato, Shengli Xie, and Junshan Zhang. Incentive mechanism for reliable federated learning: A joint optimization approach to combining reputation and contract theory. *IEEE Internet of Things Journal*, 6(6):10700–10714, 2019.
65. Hyesung Kim, Jihong Park, Mehdi Bennis, and Seong-Lyun Kim. Blockchained on-device federated learning. *IEEE Communications Letters*, 24(6):1279–1283, 2019.
66. Hengrui Jia, Mohammad Yaghini, Christopher A Choquette-Choo, Natalie Dullerud, Anvith Thudi, Varun Chandrasekaran, and Nicolas Papernot. Proof-of-learning: Definitions and practice. In *2021 IEEE Symposium on Security and Privacy (SP)*, pages 1039–1056. IEEE, 2021.
67. Jeffrey Rosen. The right to be forgotten. *Stan. L. Rev. Online*, 64:88, 2011.
68. Lucas Bourtoule, Varun Chandrasekaran, Christopher A Choquette-Choo, Hengrui Jia, Adelin Travers, Baiwu Zhang, David Lie, and Nicolas Papernot. Machine unlearning. In *2021 IEEE Symposium on Security and Privacy (SP)*, pages 141–159. IEEE, 2021.
69. Charles Lu, Mohammad Mohammadi Amiri, and Ramesh Raskar. Data measurements for decentralized data markets. *arXiv preprint arXiv:2406.04257*, 2024.
70. Raul Castro Fernandez. Data-sharing markets: Model, protocol, and algorithms to incentivize the formation of data-sharing consortia. *Proceedings of the ACM on Management of Data*, 1(2):1–25, 2023.
71. Anish Agarwal, Munther Dahleh, and Tuhin Sarkar. A marketplace for data: An algorithmic solution. In *Proceedings of the 2019 ACM Conference on Economics and Computation*, pages 701–726, 2019.
72. Leanne Roderick. Discipline and power in the digital age: The case of the us consumer data broker industry. *Critical Sociology*, 40(5):729–746, 2014. . URL https://doi.org/10.1177/0896920513501350.
73. Matthew Crain. The limits of transparency: Data brokers and commodification. *New Media & Society*, 20(1):88–104, 2018. . URL https://doi.org/10.1177/1461444816657096.
74. Yufeng Zhan, Jie Zhang, Zicong Hong, Leijie Wu, Peng Li, and Song Guo. A survey of incentive mechanism design for federated learning. *IEEE Transactions on Emerging Topics in Computing*, 10 (2):1035–1044, 2021.
75. Rongfei Zeng, Chao Zeng, Xingwei Wang, Bo Li, and Xiaowen Chu. A comprehensive survey of incentive mechanism for federated learning. *arXiv preprint arXiv:2106.15406*, 2021.
76. Lingjiao Chen, Bilge Acun, Newsha Ardalani, Yifan Sun, Feiyang Kang, Hanrui Lyu, Yongchan Kwon, Ruoxi Jia, Carole-Jean Wu, Matei Zaharia, et al. Data acquisition: A new frontier in data-centric ai. *arXiv preprint arXiv:2311.13712*, 2023.
77. Kenneth Joseph Arrow. *Economic welfare and the allocation of resources for invention*. Springer, 1972.
78. Amirata Ghorbani and James Zou. Data shapley: Equitable valuation of data for machine learning. In *International Conference on Machine Learning*, pages 2242–2251. PMLR, 2019.
79. Jamie Duncan. Data protection beyond data rights: Governing data production through collective intermediaries. *Internet Policy Review*, 12(3):1–22, 2023.
80. Mackenzie Graham. Data for sale: trust, confidence and sharing health data with commercial companies. *Journal of Medical Ethics*, 49(7):515–522, 2023.
81. Thomas Ploug and Søren Holm. Meta consent–a flexible solution to the problem of secondary use of health data. *Bioethics*, 30(9):721–732, 2016.
82. Thomas Ploug and Søren Holm. Eliciting meta consent for future secondary research use of health data using a smartphone application-a proof of concept study in the danish population. *BMC medical ethics*, 18:1–8, 2017.
83. Sylvie Delacroix and Neil D Lawrence. Bottom-up data trusts: Disturbing the 'one size fits all' approach to data governance. *International data privacy law*, 9(4):236–252, 2019.
84. Dana Alsagheer, Lei Xu, and Weidong Shi. Decentralized machine learning governance: Overview, opportunities, and challenges. *IEEE Access*, 11:96718–96732, 2023. .
85. Lie He, An Bian, and Martin Jaggi. Cola: Decentralized linear learning. *Advances in Neural Information Processing Systems*, 31, 2018.
86. Abhijit Guha Roy, Shayan Siddiqui, Sebastian Pölsterl, Nassir Navab, and Christian Wachinger. Braintorrent: A peer-to-peer environment for decentralized federated learning, 2019.
87. Sai Praneeth Karimireddy, Satyen Kale, Mehryar Mohri, Sashank Reddi, Sebastian Stich, and Ananda Theertha Suresh. Scaffold: Stochastic controlled averaging for federated learning. In *International conference on machine learning*, pages 5132–5143. PMLR, 2020.
88. Tian Li, Anit Kumar Sahu, Manzil Zaheer, Maziar Sanjabi, Ameet Talwalkar, and Virginia Smith. Federated optimization in heterogeneous networks. *Proceedings of Machine learning and systems*, 2: 429–450, 2020.
89. Xiang Li, Kaixuan Huang, Wenhao Yang, Shusen Wang, and Zhihua Zhang. On the convergence of fedavg on non-iid data. *arXiv preprint arXiv:1907.02189*, 2019.
90. Peter Kairouz, H Brendan McMahan, Brendan Avent, Aurélien Bellet, Mehdi Bennis, Arjun Nitin Bhagoji, Kallista Bonawitz, Zachary Charles, Graham Cormode, Rachel Cummings, et al. Advances and open problems in federated learning. *Foundations and Trends® in Machine Learning*, 14(1–2):1–210, 2021.
91. Kevin Hsieh, Amar Phanishayee, Onur Mutlu, and Phillip Gibbons. The non-iid data quagmire of decentralized machine learning. In *International Conference on Machine Learning*, pages 4387–4398. PMLR, 2020.
92. Ahmed Khaled, Konstantin Mishchenko, and Peter Richtárik. Tighter theory for local sgd on identical and heterogeneous data. In *International Conference on Artificial Intelligence and Statistics*, pages 4519–4529. PMLR, 2020.
93. Abhishek Singh, Gauri Gupta, Charles Lu, Yogesh Koirala, Sheshank Shankar, Mohammed Ehab, and Ramesh Raskar. Co-dream: Collaborative data synthesis with decentralized models. In *ICML Workshop on Localized Learning (LLW)*, 2023.
94. Márk Jelasity, Spyros Voulgaris, Rachid Guerraoui, Anne-Marie Kermarrec, and Maarten van Steen. Gossip-based peer sampling. *ACM Trans. Comput. Syst.*, 25(3):8–es, 8 2007. ISSN 0734-2071. . URL https://doi.org/10.1145/1275517.1275520.
95. Shuangtong Li, Tianyi Zhou, Xinmei Tian, and Dacheng Tao. Learning to collaborate in decentralized learning of personalized models. In *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*, pages 9766–9775, 2022.
96. Dongyang Fan, Celestine Mendler-Dünner, and Martin Jaggi. Collaborative learning via prediction consensus, 2023.
97. Yi Sui, Junfeng Wen, Yenson Lau, Brendan Leigh Ross, and Jesse C Cresswell. Find your friends: Personalized federated learning with the right collaborators. *arXiv preprint arXiv:2210.06597*, 2022.
98. Jeffrey Dean, Greg Corrado, Rajat Monga, Kai Chen, Matthieu Devin, Mark Mao, Marc'aurelio Ranzato, Andrew Senior, Paul Tucker, Ke Yang, et al. Large scale distributed deep networks. *Advances in neural information processing systems*, 25, 2012.
99. Deepak Narayanan, Mohammad Shoeybi, Jared Casper, Patrick LeGresley, Mostofa Patwary, Vijay Korthikanti, Dmitri Vainbrand, Prethvi Kashinkunti, Julie Bernauer, Bryan Catanzaro, et al. Efficient large-scale language model training on gpu clusters using megatron-lm. In *Proceedings of the International Conference for High Performance Computing, Networking, Storage and Analysis*, pages 1–15, 2021.
100. Deepak Narayanan, Amar Phanishayee, Kaiyu Shi, Xie Chen, and Matei Zaharia. Memory-efficient pipeline-parallel dnn training. In *International Conference on Machine Learning*, pages 7937–7947. PMLR, 2021.
101. Shigang Li and Torsten Hoefler. Chimera: efficiently training large-scale neural networks with bidirectional pipelines. In *Proceedings of the International Conference for High Performance Computing, Networking, Storage and Analysis*, pages 1–14, 2021.
102. Yanping Huang, Youlong Cheng, Ankur Bapna, Orhan Firat, Dehao Chen, Mia Chen, HyoukJoong Lee, Jiquan Ngiam, Quoc V Le, Yonghui Wu, et al. Gpipe: Efficient training of giant neural networks using pipeline parallelism. *Advances in neural information processing systems*, 32, 2019.
103. Shiqing Fan, Yi Rong, Chen Meng, Zongyan Cao, Siyu Wang, Zhen Zheng, Chuan Wu, Guoping Long, Jun Yang, Lixue Xia, et al. Dapple: A pipelined data parallel approach for training large models. In *Proceedings of the 26th ACM SIGPLAN Symposium on Principles and Practice of Parallel Programming*, pages 431–445, 2021.
104. Binhang Yuan, Yongjun He, Jared Davis, Tianyi Zhang, Tri Dao, Beidi Chen, Percy S Liang, Christopher Re, and Ce Zhang. Decentralized training of foundation models in heterogeneous environments. *Advances in Neural Information Processing Systems*, 35:25464–25477, 2022.
105. Chu Myaet Thwal, Kyi Thar, Ye Lin Tun, and Choong Seon Hong. Attention on personalized clinical decision support system: Federated learning approach. In *2021 IEEE International conference on big data and smart computing (BigComp)*, pages 141–147. IEEE, 2021.
106. Tian Bian, Yuli Jiang, Jia Li, Tingyang Xu, Yu Rong, Yi Su, Timothy Kwok, Helen Meng, and Hong Cheng. Decision support system for chronic diseases based on drug-drug interactions. In *2023*

IEEE 39th International Conference on Data Engineering (ICDE), pages 3467–3480. IEEE, 2023.
107. Duane Bender and Kamran Sartipi. Hl7 fhir: An agile and restful approach to healthcare information exchange. In *Proceedings of the 26th IEEE international symposium on computer-based medical systems*, pages 326–331. IEEE, 2013.
108. Charles E Kahn, John A Carrino, Michael J Flynn, Donald J Peck, and Steven C Horii. Dicom and radiology: past, present, and future. *Journal of the American College of Radiology*, 4(9):652–657, 2007.
109. Cosmos protocol. 2024. URL https://cosmos.network/.
110. Peter Mattson, Vijay Janapa Reddi, Christine Cheng, Cody Coleman, Greg Diamos, David Kanter, Paulius Micikevicius, David Patterson, Guenther Schmuelling, Hanlin Tang, et al. Mlperf: An industry standard benchmark suite for machine learning performance. *IEEE Micro*, 40(2):8–16, 2020.
111. Mark Mazumder, Colby Banbury, Xiaozhe Yao, Bojan Karlaš, William Gaviria Rojas, Sudnya Diamos, Greg Diamos, Lynn He, Alicia Parrish, Hannah Rose Kirk, et al. Dataperf: Benchmarks for data-centric ai development. *arXiv preprint arXiv:2207.10062*, 2022.
112. Yang Sun, Ziming Zhuang, and C Lee Giles. A large-scale study of robots. txt. In *Proceedings of the 16th international conference on World Wide Web*, pages 1123–1124, 2007.
113. Junjie Bai, Fang Lu, Ke Zhang, et al. Onnx: Open neural network exchange, 2019.
114. Alan Freier, Philip Karlton, and Paul Kocher. Rfc 6101: The secure sockets layer (ssl) protocol version 3.0, 2011.
115. Michael Moor, Oishi Banerjee, Zahra Shakeri Hossein Abad, Harlan M Krumholz, Jure Leskovec, Eric J Topol, and Pranav Rajpurkar. Foundation models for generalist medical artificial intelligence. *Nature*, 616(7956):259–265, 2023.
116. Edward L Deci, Richard Koestner, and Richard M Ryan. A meta-analytic review of experiments examining the effects of extrinsic rewards on intrinsic motivation. *Psychological bulletin*, 125(6):627, 1999.
117. Peter D Ashworth. The gift relationship. *Journal of Phenomenological Psychology*, 44(1):1–36, 2013.
118. Niloofar Bayat, Richard Ma, Vishal Misra, and Dan Rubenstein. Zero-rating and net neutrality: Who wins, who loses? *ACM SIGMETRICS Performance Evaluation Review*, 48(3):130–135, 2021.
119. Nick Doty and Mallory Knodel. Slicing the network: Maintaining neutrality, protecting privacy, and promoting competition. *arXiv preprint arXiv:2308.05829*, 2023.