A Perspective on Decentralizing AI

Abhishek Singh[✿] **Pradyumna Chari**[✿] **Charles Lu**[✿] **Gauri Gupta**[✿] **Ayush Chopra**[✿]

Jonas Blanc[✿] **Tzofi Klinghoffer**[✿] **Kushagra Tiwary**[✿] **Ramesh Raskar**[✿]

✿ MIT Media Lab

Recent progress in AI has demonstrated unprecedented problem-solving capabilities, yet deployment remains highly centralized, limiting impact in domains where data and computation are distributed across organizations and geographies. This paper introduces a perspective for decentralizing the development and deployment of AI. We identify five key challenges to unlocking the potential of decentralized AI — (1) privacy, (2) verifiability, (3) incentives, (4) orchestration, and 5) crowd UX. Our framework provides an integrated approach to these challenges, enabling otherwise distrusting and competing entities to collectively solve global problems while pursuing local objectives, advancing towards a more participatory and resilient AI ecosystem. This perspective aims to establish new design principles for decentralized AI systems and catalyze their adoption in domains where existing centralized approaches fall short.

1 Introduction

Current progress in AI is dominated by a few large organizations with centralized data and compute resources. 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 decentralized approach to AI, to promote collaboration between disparate entities through incentivization and orchestration of data and compute.

Recent Trends: Three recent trends in ML demonstrate an urgent need to transition toward decentralized AI :

- **Personal agents:** Recent progress in foundation models is enabling personalized AI agents (assistants, co-pilots, etc.). These agents require secure access to private user data, and a comprehensive understanding of preferences. Scaling such a system to population levels requires orchestrating billions of agents. A decentralized framework is needed to achieve this without creating a surveillance state.
- **AI-PC:** AI-embedded Personal Computers [Kin24] with integrated hardware accelerators (GPUs and NPUs), are experiencing rapid market growth [Lan23]. These systems facilitate a decentralized computational paradigm by enabling inference and training of models locally. This approach offers benefits such as reduced latency and enhanced privacy. However, the distributed nature of this ecosystem necessitates an orchestration layer to address challenges in synchronization and coordination for collective operation.
- **From Monolithic to Polylithic models:** Compound systems [Zah+24] and multi-agent approaches [Hua+24] to machine learning models indicate a shift from single, large monolithic models towards integrated systems of multiple coordinating components. This trend highlights the increasing complexity of tasks, where a single organization cannot be expected to possess the necessary

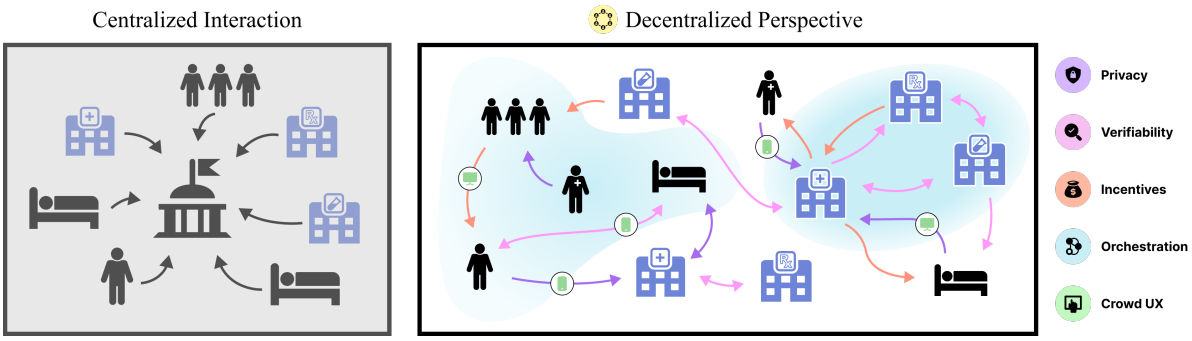

Figure 1: **Missed opportunities in today's AI.** The left panel shows the existing paradigm: interactions are mediated through dominant institutions, limiting participation and innovation. The right panel shows our proposed decentralized framework for self-organized collaboration using key primitives: privacy-preserving computation, verifiable knowledge sharing, equitable incentive mechanisms, resource orchestration, and intuitive user experience. This approach breaks down silos across sectors like healthcare, supply chain, and finance while democratizing participation and value distribution.

components to solve complex problems. Consequently, this shift introduces new challenges in synchronization and coordination.

Problems with the Centralized AI Paradigm: The following recent events expose the issues with a centralized approach.

- **Privacy Risks and Collaboration friction:** Data misuse by large companies and recent cybersecurity breaches [DeG24] have exposed the vulnerability of centralized repositories holding vast amounts of sensitive health information. Such incidents underscore the risks associated with a single entity storing large volumes of personally identifiable health data.
- **Governance Pitfalls:** Large companies like OpenAI and Google have struggled recently with governance decisions that satisfy all stakeholders [Was23; McA24]. It puts an unreasonable burden on a small group of individuals to deploy AI services for the rest of the world.
- **Compensation Conflicts:** Lawsuits against major AI companies highlight the problem of a single entity extracting value from data producers without their consent, leading to disputes over intellectual property rights and compensation [SB24b; SB24a].
- **Innovation Friction** — Centralized corporate networks lock users into their platforms to reduce competition [Dix24]. However, such practices stifle innovation and concentrate power in the hands of service providers.

2 Decentralized AI

In real-world scenarios, assets for developing and deploying AI are distributed across individuals and organizations. Decentralized AI enables collaboration between such entities with complementary assets, such as data and computation, without requiring central oversight. Figure 1 illustrates the contrast between such a system and the prevailing paradigm for building ML systems today, that requires centralized access and control over these assets. Decentralized AI is motivated by the following factors:

Decentralized Data: High-quality training data exists in isolated silos: hospitals have patient records, research labs have trial data, and individuals have personal health metrics. This fragmentation, driven by privacy concerns and competitive advantages, creates a significant bottleneck in AI advancement, that decentralized paradigms are capable of solving.

Decentralized Computation: Training deep learning models at scale requires substantial computing resources, which are often concentrated within a few organizations. This hinders the ability of smaller entities to explore and innovate at the same level. Decentralized AI aims to democratize access to compute, through a network of devices with limited individual capacity (phones, laptops, edge devices).

Decentralized Coordination: Decentralized AI also aims to enable decentralized interactions. This aspect is crucial to prevent reliance on a few central organizations as coordinators. We propose that Decentralized

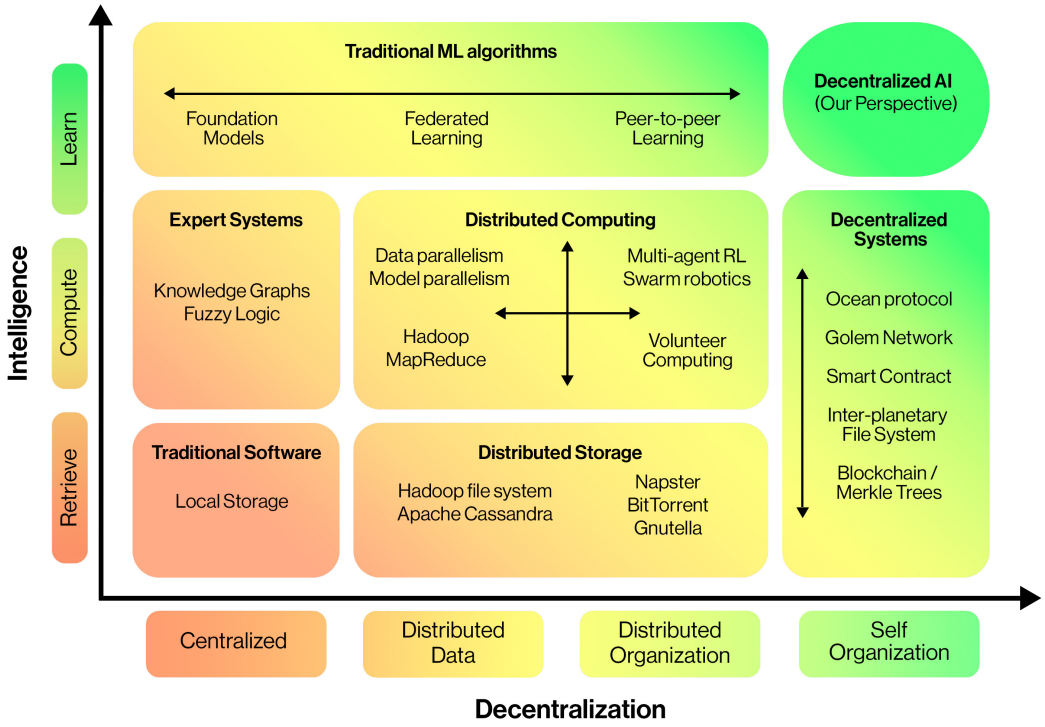

Figure 2: **Landscape of existing paradigms and the path towards decentralized AI.** ML algorithms like foundation models excel in AI capabilities but remain centralized. Decentralized systems, like blockchains and volunteer computing, distribute storage and computation but lack intelligence. We argue that bringing the two capabilities together 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 can give rise to a new generation of AI systems that are both highly capable and aligned with the values of a decentralized society.

AI can create an overlay network, similar to how the web operates on top of the internet, to facilitate self-coordination between individual entities.

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, can benefit from a decentralized ecosystem. For example, in healthcare, sharing data across organizations is a big concern. Decentralized AI incentivizes collaboration by preserving data privacy.
- **Collaborative and Responsible AI:** Responsible AI development requires multiple entities to ensure safety and auditability throughout the lifecycle of AI systems. A decentralized ecosystem will promote greater plurality and transparency over a centralized paradigm. By distributing responsibilities and control across multiple entities, decentralized AI reduces the risk of catastrophic failures stemming from a single compromised component. Decentralized AI aims to enable greater transparency and verifiability without compromising intellectual property.
- **Incentivized and Participatory AI:** Decentralized AI can lead to a more equitable distribution of technological benefits. The participatory and permissionless nature allows individuals from diverse demographics to benefit from and contribute to such a system. Incentive systems that reward participation based on the quality of contribution can also foster increased collaboration.
- **Improved accessibility of resources:** Decentralized AI enables researchers to tap into vast datasets, computational resources, and aggregated statistics, enabling large-scale experiments and hypothesis generation previously only possible for big organizations.

The following technologies offer insights and lay groundwork for decentralized AI, but are insufficient on their own.

- **Federated Learning (FL)** enables training on decentralized data. However, it is limited by centralized orchestration, coupling between data and computation ownership, and focusing on model training. For Decentralized AI, we must extend decentralization to the entire ML lifecycle, decouple data and computation ownership, and address aspects such as incentives, verifiability, and attribution. Recent peer-to-peer FL approaches [Yua+23] remove centralized orchestration but still focus on collaborative training. We consider a broader scope, including synthetic data sharing [Bau+] and collaborative inference [Sin+].
- **Web3** aims to advance a more decentralized web ecosystem using blockchains. However, blockchains do not address several problems relevant to Decentralized AI (as discussed in the next section) and have mostly focused on monetary aspects such as cryptocurrency. Nevertheless promising directions have been proposed at the intersection of Web3 and AI (see [But24] and Fig2), and several cryptographic approaches such as distributed consensus, zero-knowledge proofs, homomorphic encryption, and multi-party computations, will be important for Decentralized AI.
- **Distributed AI** has enabled scaling of deep learning workloads across data centers efficiently. Prior work spans research in data [Aac+23], model [BOV24] and pipeline parallelism [Nic+21]. These approaches scale well in trusted, synchronized, homogeneous, and high-performing compute clusters. However, these are constraints that decentralized AI aims to remove, leading to unique challenges.
- **Volunteer computing** projects like Folding@home and SETI@home have distributed large-scale computing tasks across geographically distributed machines. However, they lack sophisticated verifiability and incentive measures. Privacy requirements in settings such as scientific computing may also not be stringent. In contrast, Decentralized AI faces unique challenges due to the dynamic and private nature of data.
- **Open-Source Software (OSS) and Open-access** have spurred recent advancements in ML research. Platforms like arXiv, GitHub, and HuggingFace have enabled distributed collaborations at scale. However, decentralized AI requires going beyond the existing paradigm. achine learning requires collaboration over additional assets (beyond software), such as datasets, computation, and network infrastructure. Not all of these can be made openly available to the public due to privacy, cost etc.

3 Pillars of Decentralized AI

Decentralized systems have diverse entities with limited resources that must self-organize to utilize resources effectively. Coordination on the scale of individuals and their data has unique machine learning challenges requiring new kinds of interactions. Figure 1 shows this. In this scenario, the entity requiring assets can request them *autonomously* without relying on a central orchestrator. However, it is important to note that third parties still play a valuable role within this ecosystem: existing actors can contribute to improving access to resources and services within a decentralized ecosystem.

We believe that the path for decentralization in AI should be similar to the development of internet infrastructure, where standards and protocols exist at several layers ranging from the physical layer to the application layer. Such protocols enable any individual to start a website and serve content. While the Internet ecosystem is helped by larger entities, the ecosystem does not rely upon them to function: the only requirement for a participating entity is adherence to agreed-upon standards and protocols of the decentralized system. Given thse challenges, five key problems need to be addressed: privacy, verifiability, incentives, orchestration, and Decentralized UI/UX. As shown in Fig. 7, these pieces need to come together to enable collaboration between decentralized entities.

Within each pillar, we also discuss challenges to implementation. We categorize these into two categories: 1) problems that are more difficult with decentralization, and 2) new problems that emerge in the context of decentralization. We focus more on the latter. While not an exhaustive list, our goal is to highlight significant problems and bring them to the attention of the research community.

Privacy
Privacy is essential to unlock value from sensitive data while maintaining organizational boundaries and

user trust. While centralized, impartial, and trusted brokers can mitigate these concerns, the ultimate aspiration of decentralization is to transition towards a *Breachless* future where privacy is assured and provable.

Challenges

Existing secure computation techniques such as homomorphic encryption and confidential computing protect the privacy of data during computation. However, secure computation over decentralized data remains practically infeasible.

A fundamental challenge emerges when secure computing intersects with model training: existing homomorphic encryption schemes dramatically increase computational overhead, making real-time healthcare diagnostics or financial fraud detection impractical. Future systems need novel lightweight encryption methods optimized for neural network operations. Additionally, techniques such as homomorphic encryption [Man+23], secure multi-party computation (MPC) [ZBL23], and trusted execution environments (TEEs) [Muñ+23] have been used for inference over ML models on encrypted data, but they assume data originates from a single source. For decentralized data, different data fragments will be encrypted with different keys, making simultaneous computation challenging. Analyzing such data requires aggregating inputs with complex cryptographic key exchanges and computation overhead because of non-linear computation over this aggregated input.

This challenge is not specific to decentralized data belonging to one user, but is also applicable when the output of an ML model is dependent on data from other users. For instance, when applying computation over graph data such as 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 data scenarios are common in siloed and fragmented industries such as healthcare, finance, and mobility. Current secure computing paradigms have not paid enough attention to this multi-party dynamic. A decentralized AI paradigm would require addressing these constraints.

Verifiability

Verifiability is important for permissionless and private decentralized systems, and provides protection from and robustness to malicious actors. The problem is particularly challenging with privacy: anonymity allows malicious actors to poison the system without accountability. Systems need continuous differential privacy guarantees that remain valid even as models are updated over time. This requires developing privacy accounting mechanisms that work across organizational boundaries and track cumulative information leakage through model updates. We believe algorithms and collaboration need to transition from a trusted and permission-based to a *Trustless* system where legitimate contribution can be proved by contributors and verified by other participants.

Challenges

1. *Malicious attackers:* Several known attacks during both individual model training [Par+21] and aggregation [Xu+19] threaten privacy [LYY20] and membership [Sho+17] of local data contributions. These problems are more challenging in decentralized settings without an overseeing central authority. Malicious actors can perform model inversion attacks, reconstructing training data and leaking sensitive information [FJR15]. They may also tamper with models, introducing backdoor functionality or compromising updates of other clients [Bha+19]. Two strategies to protect against bad actors are: 1) identification and isolation, and 2) protection against bad contributions and relying on contributions from "good" actors.

2. *Free riders:* Clients may try to benefit from resources in a decentralized AI ecosystem without contributing in return. Free-riding is prevalent in many peer-to-peer systems [Lyu+20; FVL21]. To mitigate this, the system must implement contribution verification protocols to detect and penalize free-riding behavior without compromising privacy, using techniques such as zero-knowledge proofs.

3. *Verifying contributors:* Drawing inspiration from trust management systems in Internet of Things (IoT) [Yu+13; Ud +19] and blockchain systems, we can enhance reliable interactions among participants. Existing proof-based algorithms [Bac+02; Nak08] require algorithmically verifiable mechanisms of contribution from participants. Several other trust mechanisms have been proposed to defend against model poisoning attacks and increase byzantine robustness [Cao+20; LSP19]. Reputation mechanisms track a dynamic score for users to identify malicious participants, either based on gradient similarity [XL] or historical accuracy contributions [Liu+]. Blockchain-based reputation

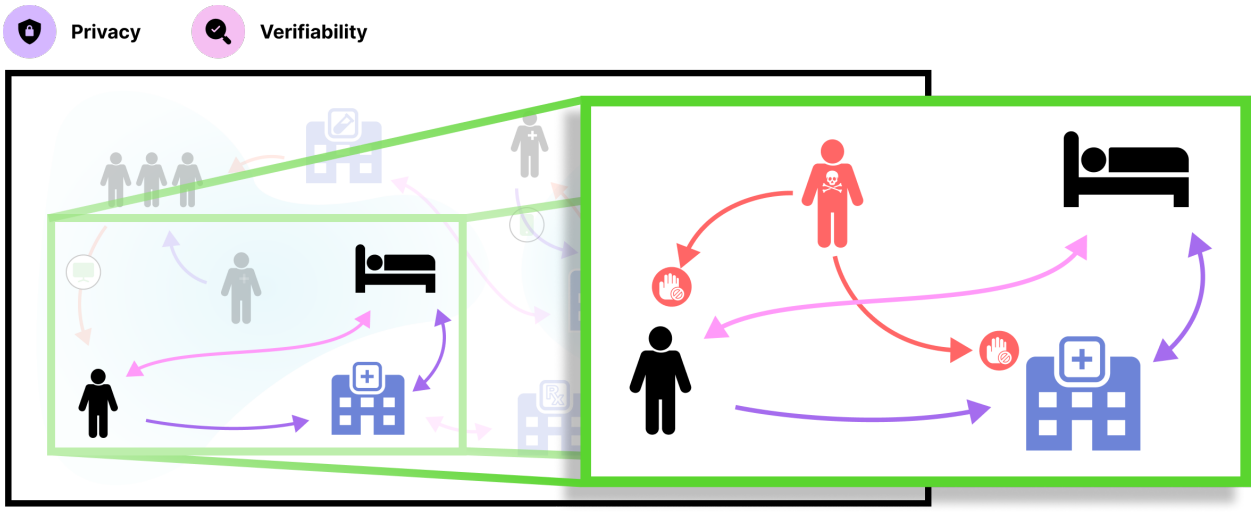

Figure 3: **Protecting privacy while preventing bad actors**. In a decentralized ecosystem with anonymity and privacy, bad actors can report or amplify misleading data or statistics, leading to unintended outcomes. Therefore, guardrails and accountability mechanisms that preserve individual privacy are 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 supernodes to enforce these without compromising the decentralized nature of the system.

systems may also be useful in ensuring model integrity and detecting malicious behaviors [MCK21; Zha+19]. Alternatively, participants may verify the uploaded model parameters before performing model aggregation and updates [Kim+19; Zha+19]. Proof-of-Work algorithms can also be employed where one party proves to another that it has expended computational resources [Jia+21] or proves correctness of aggregation results [Xu+19].

4. *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 [Ros11]. This can include verification of machine unlearning [Bou+21], ensuring that participants can revoke their contributions.

Incentives

The primary objective of decentralization is fostering collaboration among entities with distinct assets and objectives. Fair and transparent incentive mechanisms must be developed, that encourage user involvement. Today, large AI companies use a broker-like system to purchase data from other entities. We, however, envision a *Brokerless* system.

Challenges

1. *Data Markets:* Greater data access is needed to enable AI impact in areas where data is private, limited, or otherwise restricted, such as healthcare. Data markets have been promoted to incentivize participants who would otherwise not incur the costs of processing and sharing data [LAR24]. Decentralized data markets can address underlying power imbalances in the current centralized data economy, such as privacy erosion and lack of consent [SB24b; SB24a].
2. *Data Valuation:* A key challenge is developing universal valuation metrics to assess data importance. These metrics must account for data uniqueness, and cross-domain/task applicability while being resistant to manipulation. Another challenge relates to the discovery and valuation of data. In a perfect market with intermediate brokers, the buyers and sellers can be directly matched through the broker. However, in a decentralized, two-sided marketplace, federated and privacy-preserving strategies are needed to match buyers and sellers, and price data [ZBL23]. Insights from mechanism design could help incentivize desirable behaviors [Zha+21].
3. *Privacy, security, and efficiency:* New data discovery and valuation operations cannot assume "white-box" access to the seller data [Che+23], as data can be easily copied (see Arrow's Information Paradox [Arr72]). In addition to relying on centralized data access, existing data valuation approaches, such as Data Shapley [GZ19], are costly to compute. New decentralized valuation

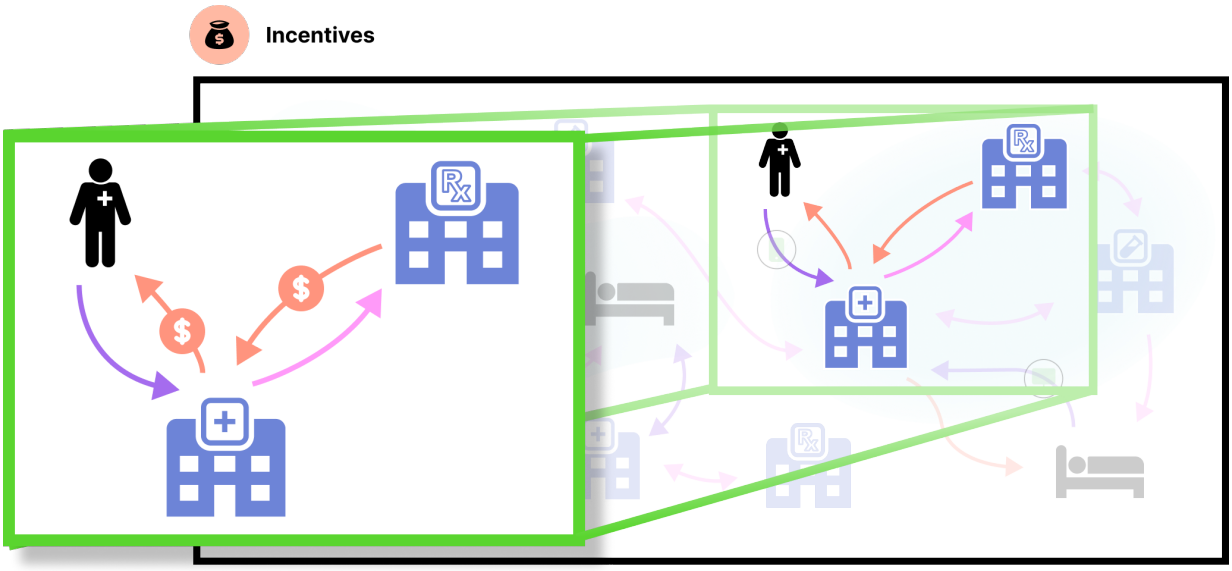

Figure 4: **How to measure dollar value of data without accessing it?** Because data is easily copied, a data owner such as a patient would not allow data access before compensation. However, a data buyer such as a medical company would not pay without being able to assess the value and relevance of the data. This leads to 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.

algorithms must be scalable and cheap to compute, even for billion-scale datasets. Markets need automated quality assessment mechanisms that can detect synthetic or adversarial data without accessing the raw content. This requires developing new metrics for authenticity and information content that work on encrypted or privacy-preserved data representations.

4. *Decentralized data governance:* This entails management of control and consent among distributed data owners. Individual owners usually would not have the time, energy, or resources to engage in negotiations with buyers. New governance models, such as decentralized autonomous organizations, data cooperatives, and data unions, could provide mechanisms for collective oversight and stewardship [Dun23]. Decentralized governance protocols must automate routine decisions while escalating critical choices to stakeholders. For example, data retention policies could be enforced by smart contracts, while major model architecture changes require distributed consensus voting. These intermediates could act as fiduciaries, for example to represent patient interests in having increased leverage with interested parties [Gra23].
5. *Consent:* The above governing bodies could also assist with educating members on data rights and managing consent and access. For instance, a meta-consent mechanism could allow fine-grained controls by specifying preferences for different contexts and avoid the need to obtain consent for every secondary use [PH17]. Patients should be able to leave the bargaining unit and take their data with them, while ideally having freedom of choice between data collectives that best represent their interests [DL19]. Additionally, AI governance models inspired by decentralized autonomous organizations may help communities vote and reach consensus on data acquisition and model training and deployment [AXS23].

Orchestration

Orchestration is essential to enable coordination between entities with unique assets and objectives. A key dilemma in Decentralized AI is orchestration without a centralized orchestrator. The problem with a centralized orchestrator (as in federated learning (FL)) is that it concentrates control of access and distribution in a few entities. Hence, incentives for all stakeholders will have to align with this central entity. This contradicts the goal of decentralization. We envision a *Coordinatorless* system where a network of individuals and organizations can self-organize and connect autonomously, similar to decentralized FL works for peer-to-peer (P2P) communication between clients [Roy+19].

Challenges

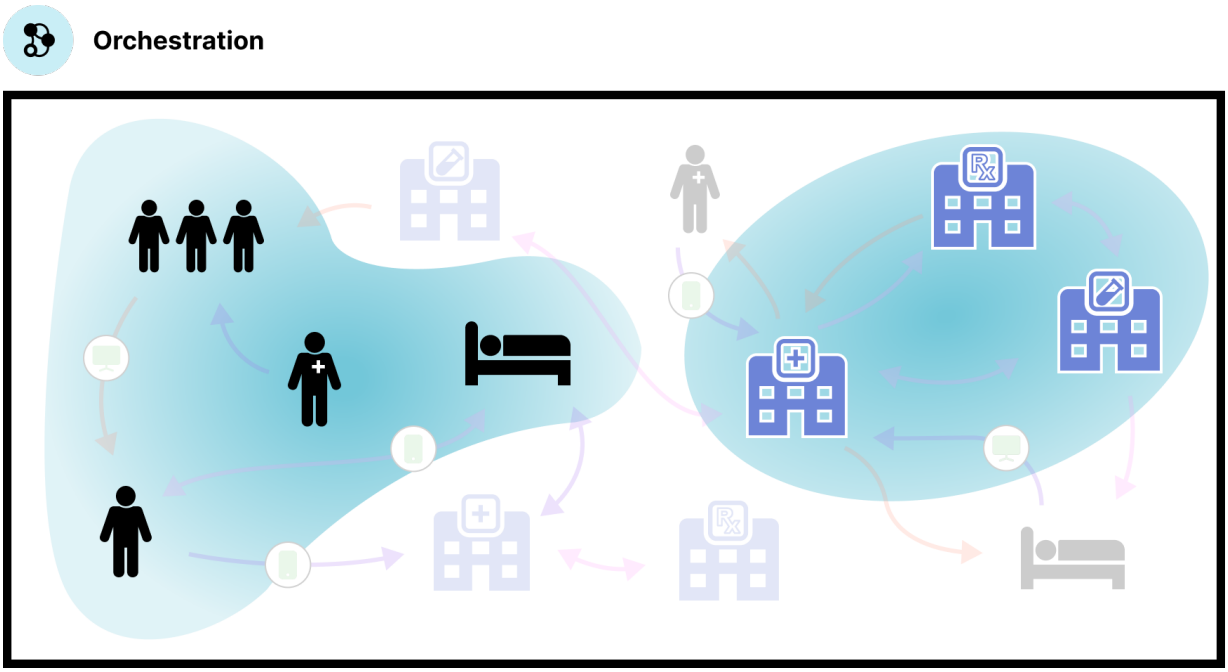

Figure 5: **Self-coordination for decentralized collaborative learning.** Existing approaches, like federated learning, rely on a central coordinator or assume a fixed topology. In a decentralized network, users can freely interact and exchange information, leading to a diverse set of participants with heterogeneous tasks, data, and privacy preferences. This poses challenges for 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 extract relevant information from vast amounts of decentralized data, by dynamically adapting the collaboration topology based on user similarities and information relevance.

1. *Data Heterogeneity:* Collaboration poses a major challenge: data varies in terms of distribution, scale, and features, leading to challenges in aggregating information cohesively. Recent studies [Kar+20; Kai+21] show that FL with heterogeneous (i.e. non-IID) data results in slow convergence and suboptimal performance. To address this, existing work relies on a central server to "correct" individual contributions, which is difficult in decentralized settings. A distributed orchestration protocol must dynamically form training clusters based on data similarity, computational resources, and network conditions. These self-organizing clusters should redistribute workload across participants without compromising model convergence.
2. *Model Heterogeneity:* There is significant heterogeneity in terms of model architecture in decentralized setups, due to varying compute and bandwidth capabilities. We believe that Decentralized AI platforms should accommodate this diversity, rather than mandating standardization. This enhances inclusivity and adaptability, but also creates interoperability roadblocks. For instance, most FL techniques require identical, or the same family of model architectures. More adaptive aggregation techniques need to be developed to enable interoperability between custom models at scale. One approach for this is through synthetic data representations from trained model weights [Sin+23].
3. *Collaborator selection:* Current systems largely rely on random communication [Jel+]; however, this greatly suffers due to heterogeneity in data distributions. In a decentralized system, selection requires dynamic reputation scoring that considers both historical performance and current resource availability. Smart collaboration protocols should match participants based on complementary datasets, computational resources, and historical success rates while ensuring no single participant can reconstruct sensitive information by strategically choosing collaboration partners. In the context of non-IID data, some approaches assign trust or collaboration weights to other clients, either by learning them [Li+22], measuring similarity on unlabelled public datasets [FMJ], or by clustering clients [Sui+22]. A related challenge involves orchestrating virtual super-nodes (used in P2P systems) to assist in coordination. For decentralized AI systems, super-nodes must become intelligent coordinators that optimize training across heterogeneous devices, validate model qual-

ity without accessing private data, and detect potential security threats while maintaining system decentralization. Another challenge to be addressed is that of client drop-out and, generally, heterogeneity in client availability, responsiveness, and resources. Slow clients can impede convergence rate, and lead to system-induced bias, such as over-representing demographics with high internet quality [Kai+21] in FL.

4. *Asynchronous computing:* Making training asynchronous is essential for geographically distributed nodes with different partitions of data and parameters. Addressing this requires eliminating communication bottlenecks and synchronization among training parameters. Sequential computation on neural networks across nodes with standard training procedures has two problems: 1) underutilization of nodes because only one partition is active at a time and 2) requirement of synchronous communication since each node depends upon data from neighboring nodes. The first problem has been studied extensively in the context of multi-GPU training in data centers. However, distributed training requires new parallelization strategies (data parallelism [Dea+12], tensor parallelism [Nar+21a], pipeline parallelism [Nar+21b] and hybrid modes of parallelism [Fan+21]) that can handle unstable network conditions, varying computational capabilities, and dynamic participant availability while maintaining convergence guarantees. Additionally, enabling computation in this scenario requires eliminating synchronization bottlenecks: challenging due to the nature of backpropagation. Except for a few recent works [Yua+22], the second problem of communication synchronization has not attracted as much attention.

Crowd UX
Crowd UX is the interface between Decentralized AI systems and users. It enables discovery, recommendation, and collaboration among entities without prior relationships. Through collaboration across diverse resources, users need not understand the complexities of tasks performed by other entities. We envision a *Frictionless* system that enhances user experience and encourages participation across entities.

Challenges
The research challenge in this category lies in making large-scale decentralized systems compatible with intuitive user interfaces. A key 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. Existing works [Thw+21; Bia+23] 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 like browsers, domain name servers (DNS), and secure sockets layer (SSL) protocols, which authenticate websites and ensure secure communication. The absence of these technologies would not preclude internet use, but their accessibility and usability have contributed to widespread adoption. Similarly, the utility of Decentralized AI hinges on widespread participation from individuals and interfaces that reduce friction in participation.

Overarching Challenge: Standards
While the previous challenges focused on algorithms and systems, well-defined, agreed-upon standards are equally important. Like TCP/IP for the internet, and HTTPS for web browsing, we need foundational standards for each pillar. For example, privacy standards would define acceptable levels of differential privacy, encryption requirements, and data anonymization protocols. The decentralized AI ecosystem needs a layered protocol stack: a base layer for secure computation and data exchange, a middle layer for model training and verification, and an application layer for domain-specific implementations like healthcare or finance. Each layer must define clear interfaces while allowing implementation flexibility.

Like W3C for web standards, we need collaborative bodies to develop and maintain decentralized AI protocol interoperability across interfaces and hardware. We expect these standards to be domain-specific and rely upon existing standards such as FHIR [BS] for electronic health records, DICOM [Kah+07] for medical imaging, and COSMOS [24] for blockchain interoperability. Insights from prior machine learning standards and benchmarking can also carry-over [Mat+20; Maz+22].

4 Opportunities and Impact of Decentralized AI

Opportunities in decentralized AI extend to industries involving multiple stakeholders and fragmented information ecosystems. We discuss some of these below. By no means is this list exhaustive: it only serves to demonstrate the impact of a decentralized ecosystem across these domains.

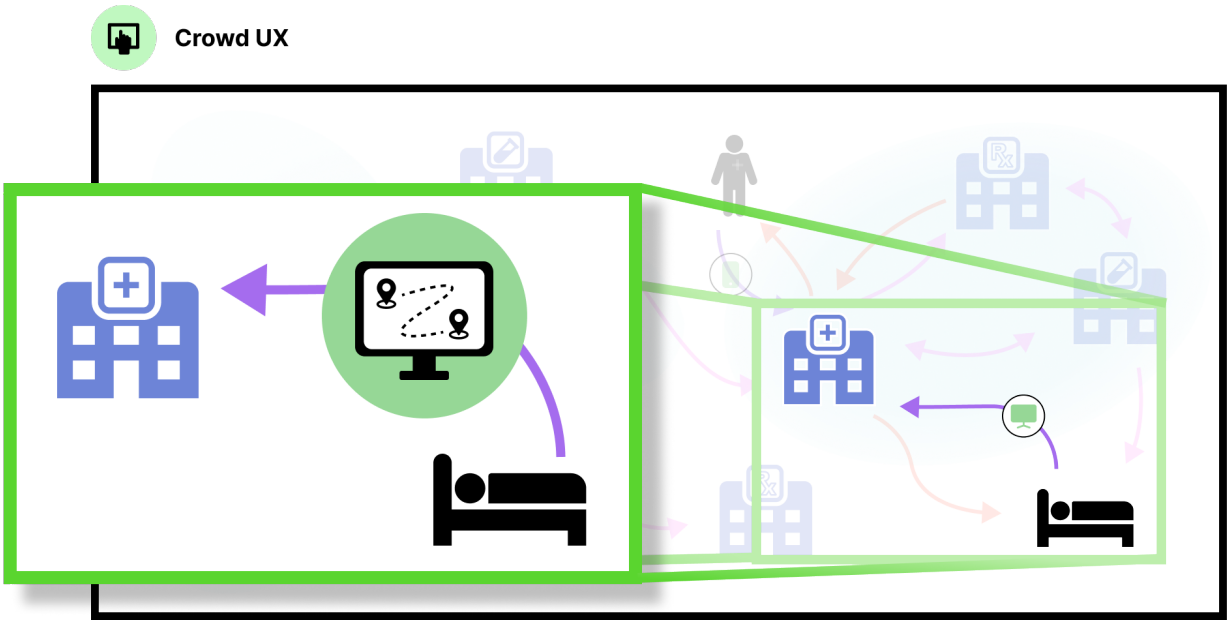

Figure 6: **Simplifying User Navigation in Decentralized Systems.** Just as navigation apps guide travelers and internet stack (DNS, HTTP, search) streamlines navigating the web, Crowd UX enables intuitive interaction with complex decentralized AI primitives. By providing decision support systems and collaborative tools, it transforms overwhelming technical choices into manageable user journeys, making decentralized AI accessible to users regardless of their technical expertise.

Healthcare: Moor et al. [Moo+] identify five challenges to generalist medical artificial intelligence that advances current medical AI models. Decentralized AI can help address these. The first is validation. Existing benchmarking techniques are designed for ML models that solve only one task, but healthcare foundational models are expected to be multi-purpose. Using decentralized AI and distributed inference over secure data, validators can evaluate model performance without sharing raw data. This prevents model providers from overfitting on evaluation data. Simultaneously, model validators do not have access to all model parameters, which may be proprietary assets. Additionally, personalized models enabled by decentralized AI will alleviate the critical reliance on model validation. The second is verification, or the explainability and interpretability that helps clinicians work with the system. We highlight this research challenge in crowd UX. While decentralized AI does not address interpretability and hallucinations in ML, addressing the crowd UX challenge enhances trust and accessibility of the system. The third is social biases. Model bias increases with scale, reducing utility for minorities and rare diseases. The permissionless and incentivized nature of decentralized AI can partially alleviate this concern, through robust and equitable orchestration on heterogeneous data, and collaborator selection to identify relevant models for a given demographic. The fourth is privacy. Foundation models can pose serious privacy risks. Privacy enhancement, being one of the key pillars of decentralized AI, can help alleviate concerns associated with training and deployment of such models. The final challenge is scale. When moving from the paradigm of a small task-specialist model to a generalist large foundation model, three factors are important - 1) data acquisition cost, 2) model training cost, and 3) deployment cost. All three can be reduced through incentives and privacy-preserving mechanisms that allow individuals to contribute their data or computation verifiably. The current system of acquiring data either requires web scraping (which does not include most healthcare data) or through brokers (an inefficient system). We instead argue for a brokerless system where individuals and organizations can share data and get rewarded appropriately. We note that innovation in decentralized AI would not eliminate all the abovementioned issues, but alleviate several of these concerns meaningfully.

Finance can benefit from a decentralized ecosystem. Like healthcare, data and insights are isolated in silos due to regulation. Through privacy-preserving analytics over decentralized data, financial institutions can collaborate on fraud detection, credit scoring, and risk assessment without sharing customer data. This allows for robust models while maintaining regulatory compliance and privacy. Peer-to-peer lending platforms can use verifiability mechanisms to assess creditworthiness without centralizing sensitive information.

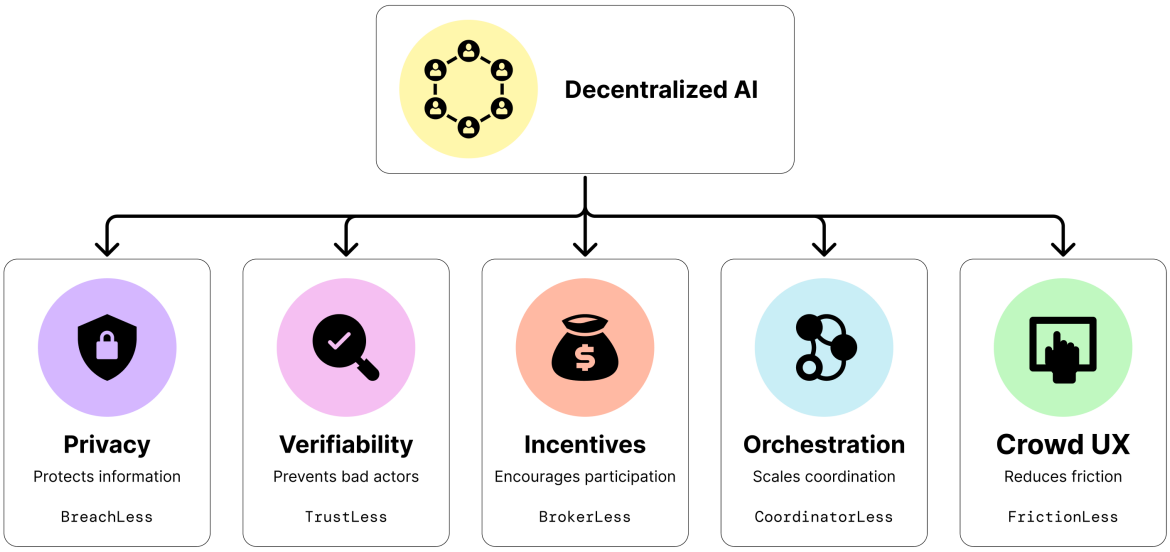

Figure 7: **Five building blocks to enable decentralized AI:** Privacy (BreachLess) protects sensitive information, Verifiability (TrustLess) ensures system integrity, Incentives (BrokerLess) drive participation, Orchestration (CoordinatorLess) enables scalable collaboration, and Crowd UX (FrictionLess) simplifies user interaction. Each pillar addresses a critical challenge in decentralized systems while eliminating traditional intermediaries (reflected in their "Less" designations).

Supply Chain can be improved through collaboration between competitors while protecting proprietary information. End-to-end visibility can be improved if companies 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 without centralizing manufacturing data. Organizations can collectively optimize sustainability metrics through route optimization and capacity planning without exposing operational information. Decentralized orchestration platforms can coordinate just-in-time production and logistics across factories and carriers. Crowd UX innovations can allow small suppliers and consumers to benefit from these complex supply chains through user-friendly interfaces.

Mobility can be improved by integrating data at scale. Cities can collaborate on traffic prediction and management without centralizing data on individual movements. Data markets can be used to create incentives for people to participate and contribute movement data. Similarly, car manufacturers and tech companies can pool data to improve autonomous driving algorithms while protecting proprietary technologies. Verifiability mechanisms can ensure integrity and provenance of shared data, critical for safe autonomous systems. Transit agencies can work together using orchestration algorithms to optimize routes and schedules across regions without centralizing operational data. Energy companies and automotive manufacturers can collaborate on charging station placement and usage without sharing market data.

5 Risks of Decentralization

This paper advocates for decentralizing the entire machine learning pipeline, citing numerous advantages this confers over centralized systems. However, there remain challenges. Decentralizing AI does not solve several problems that AI systems face, such as hallucination, bias, etc. Furthermore, decentralization introduces new problems that the community must navigate. Fig. 8 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. By scrutinizing these drawbacks and self-correcting course accordingly, we can realize the many benefits of Decentralized AI while containing its risks.

Lack of Traceability: Decentralized AI minimizes dependence on centralized institutions. This facili-

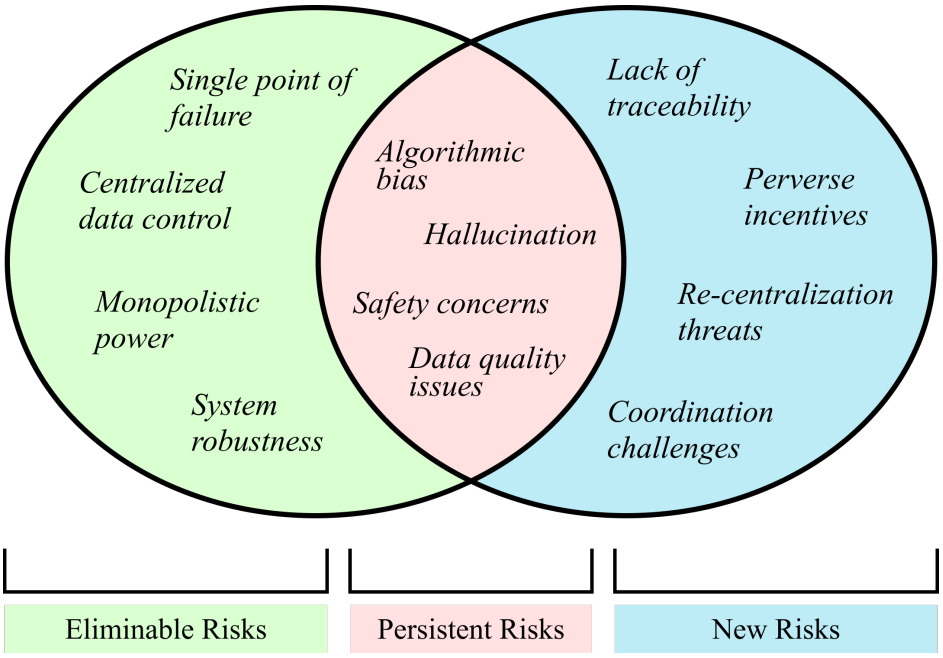

Figure 8: **Risks of Decentralized AI**: There are several risks associated with AI. A subset of them can be eliminated by introducing decentralization in the system. However, decentralization itself introduces new risks. We discussed technical challenges to address some of these risks, but a subset of the risks are expected to creep into any Decentralized AI system. Do the benefits outweigh the risks? This is a question that requires discussion between various stakeholders.

tates collaboration among entities that otherwise lack mutual trust, incentive, or coordination. However, it becomes less clear where the fault lies if things go awry. Without a central authority, the system lacks an accountable linchpin. For a decentralized system to remain reliably self-correcting, it must incorporate safeguards and accountability chains that trace culpability. Enabling anonymity and confidentiality while embedding auditability is an open research challenge. The solutions will likely involve cryptographic schemes to certify origin and intent without compromising privacy, and game-theoretic interactions that incentivize good behavior.

Perverse Incentives: Several individuals and organizations host open datasets and volunteer compute for altruistic reasons. Explicit incentive structures for contributing to decentralized systems can risk crowding out altruism and diminishing participation from those seeking to help rather than to profit. It has been observed that extrinsic rewards can override intrinsic motivations over time [DKR99]. When we compensate people for activities they once did voluntarily, they tend to lose intrinsic interest in those activities. Therefore, designing effective incentive programs requires careful consideration of community norms, social motivations, and human psychology as well. The goal should be to complement extant altruism without supplanting it. Hybrid approaches that balance incentives with opportunities for voluntary participation could help (i.e. combining economic and reputation-based incentives).

Consolidation by Re-centralization: Decentralized systems can re-centralize over time without safeguards. Dominant centralized institutions can emerge organically, which is not inherently problematic. However, this risks bringing back the issues of freedom and competition that decentralization aims to resolve. For example, cryptocurrency exchanges have become centers of immense centralized control, and services such as FreeBasics have threatened to bypass net neutrality [Bay+21]. Recentralizing forces can increase efficiency, but simultaneously undermine openness. Therefore, decentralized networks should institute mechanisms that allow dominant players to operate while maintaining ease of entry and participation for individuals and startups. As certain centralized institutions gain prominence, decentralized systems must facilitate alternative providers challenging them. 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 intermediaries, recentralization can be prevented.

The intent is not to artificially promote decentralization when centralization is better. Both should co-exist in balance. If decentralized participation remains simple, open, and impartial, dominant institutions will rise and fall based on merit. This dynamism also provides the right incentives for innovation within centralized players, creating a vibrant, evolving ecosystem. Short-term gains from centralization must be weighed against long-term ecosystem health and innovation.

6 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

[Arr72] Kenneth Joseph Arrow. *Economic welfare and the allocation of resources for invention*. Springer, 1972.

[DKR99] Edward L Deci, Richard Koestner, and Richard M Ryan. "A meta-analytic review of experiments examining the effects of extrinsic rewards on intrinsic motivation." In: *Psychological bulletin* 125.6 (1999), p. 627.

[Bac+02] Adam Back et al. "Hashcash-a denial of service counter-measure". In: (2002).

[Kah+07] Charles E Kahn et al. "DICOM and radiology: past, present, and future". In: *Journal of the American College of Radiology* 4.9 (2007), pp. 652–657.

[Nak08] Satoshi Nakamoto. "Bitcoin: A peer-to-peer electronic cash system". In: (2008).

[Ros11] Jeffrey Rosen. "The right to be forgotten". In: *Stan. L. Rev. Online* 64 (2011), p. 88.

[Dea+12] Jeffrey Dean et al. "Large scale distributed deep networks". In: *Advances in neural information processing systems* 25 (2012).

[Yu+13] Han Yu et al. "A Survey of Multi-Agent Trust Management Systems". In: *IEEE Access* 1 (2013), pp. 35–50. DOI: 10.1109/ACCESS.2013.2259892.

[FJR15] 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. Denver, Colorado, USA, 2015, pp. 1322–1333. ISBN: 9781450338325. DOI: 10.1145/2810103.2813677. URL: https://doi.org/10.1145/2810103.2813677.

[PH17] 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". In: *BMC medical ethics* 18 (2017), pp. 1–8.

[Sho+17] Reza Shokri et al. "Membership inference attacks against machine learning models". In: *2017 IEEE symposium on security and privacy (SP)*. IEEE. 2017, pp. 3–18.

[Bha+19] Arjun Nitin Bhagoji et al. *Analyzing Federated Learning through an Adversarial Lens*. 2019. arXiv: 1811.12470 [cs.LG].

[DL19] Sylvie Delacroix and Neil D Lawrence. "Bottom-up data trusts: Disturbing the 'one size fits all' approach to data governance". In: *International data privacy law* 9.4 (2019), pp. 236–252.

[GZ19] Amirata Ghorbani and James Zou. "Data shapley: Equitable valuation of data for machine learning". In: *International Conference on Machine Learning*. PMLR. 2019, pp. 2242–2251.

[Kim+19] Hyesung Kim et al. "Blockchained on-device federated learning". In: *IEEE Communications Letters* 24.6 (2019), pp. 1279–1283.

[LSP19] Leslie Lamport, Robert Shostak, and Marshall Pease. "The Byzantine generals problem". In: *Concurrency: the works of leslie lamport*. 2019, pp. 203–226.

[Roy+19] Abhijit Guha Roy et al. *BrainTorrent: A Peer-to-Peer Environment for Decentralized Federated Learning*. 2019. arXiv: 1905.06731 [cs.LG].

[Ud +19] Ikram Ud Din et al. "Trust Management Techniques for the Internet of Things: A Survey". In: *IEEE Access* 7 (2019), pp. 29763–29787. DOI: 10.1109/ACCESS.2018.2880838.

[Xu+19] Guowen Xu et al. "Verifynet: Secure and verifiable federated learning". In: *IEEE Transactions on Information Forensics and Security* 15 (2019), pp. 911–926.

[Zha+19] Yang Zhao et al. "Mobile edge computing, blockchain and reputation-based crowdsourcing iot federated learning: A secure, decentralized and privacy-preserving system". In: *arXiv preprint arXiv:1906.10893* (2019), pp. 2327–4662.

[Cao+20] Xiaoyu Cao et al. "Fltrust: Byzantine-robust federated learning via trust bootstrapping". In: *arXiv preprint arXiv:2012.13995* (2020).

[Kar+20] Sai Praneeth Karimireddy et al. "Scaffold: Stochastic controlled averaging for federated learning". In: *International conference on machine learning*. PMLR. 2020, pp. 5132–5143.

[LYY20] Lingjuan Lyu, Han Yu, and Qiang Yang. "Threats to federated learning: A survey". In: *arXiv preprint arXiv:2003.02133* (2020).

[Lyu+20] Lingjuan Lyu et al. "Towards fair and privacy-preserving federated deep models". In: *IEEE Transactions on Parallel and Distributed Systems* 31.11 (2020), pp. 2524–2541.

[Mat+20] Peter Mattson et al. "MLPerf: An industry standard benchmark suite for machine learning performance". In: *IEEE Micro* 40.2 (2020), pp. 8–16.

[Bay+21] Niloofar Bayat et al. “Zero-rating and net neutrality: Who wins, who loses?” In: *ACM SIGMETRICS Performance Evaluation Review* 48.3 (2021), pp. 130–135.

[Bou+21] Lucas Bourtoule et al. “Machine unlearning”. In: *2021 IEEE Symposium on Security and Privacy (SP)*. IEEE. 2021, pp. 141–159.

[Fan+21] Shiqing Fan 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*. 2021, pp. 431–445.

[FVL21] Yann Fraboni, Richard Vidal, and Marco Lorenzi. “Free-rider attacks on model aggregation in federated learning”. In: *International Conference on Artificial Intelligence and Statistics*. PMLR. 2021, pp. 1846–1854.

[Jia+21] Hengrui Jia et al. “Proof-of-learning: Definitions and practice”. In: *2021 IEEE Symposium on Security and Privacy (SP)*. IEEE. 2021, pp. 1039–1056.

[Kai+21] Peter Kairouz et al. “Advances and open problems in federated learning”. In: *Foundations and Trends® in Machine Learning* 14.1–2 (2021), pp. 1–210.

[MCK21] Hajar Moudoud, Soumaya Cherkaoui, and Lyes Khoukhi. “Towards a secure and reliable federated learning using blockchain”. In: *2021 IEEE Global Communications Conference (GLOBECOM)*. IEEE. 2021, pp. 01–06.

[Nar+21a] Deepak Narayanan 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*. 2021, pp. 1–15.

[Nar+21b] Deepak Narayanan et al. “Memory-efficient pipeline-parallel dnn training”. In: *International Conference on Machine Learning*. PMLR. 2021, pp. 7937–7947.

[Nic+21] Daniel Nichols et al. “A survey and empirical evaluation of parallel deep learning frameworks”. In: *arXiv preprint arXiv:2111.04949* (2021).

[Par+21] Jungwuk Park et al. “Sageflow: Robust federated learning against both stragglers and adversaries”. In: *Advances in neural information processing systems* 34 (2021), pp. 840–851.

[Thw+21] Chu Myaet Thwal et al. “Attention on personalized clinical decision support system: Federated learning approach”. In: *2021 IEEE International conference on big data and smart computing (BigComp)*. IEEE. 2021, pp. 141–147.

[Zha+21] Yufeng Zhan et al. “A survey of incentive mechanism design for federated learning”. In: *IEEE Transactions on Emerging Topics in Computing* 10.2 (2021), pp. 1035–1044.

[Li+22] Shuangtong Li et al. “Learning to collaborate in decentralized learning of personalized models”. In: *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*. 2022, pp. 9766–9775.

[Maz+22] Mark Mazumder et al. “Dataperf: Benchmarks for data-centric ai development”. In: *arXiv preprint arXiv:2207.10062* (2022).

[Sui+22] Yi Sui et al. “Find Your Friends: Personalized Federated Learning with the Right Collaborators”. In: *arXiv preprint arXiv:2210.06597* (2022).

[Yua+22] Binhang Yuan et al. “Decentralized training of foundation models in heterogeneous environments”. In: *Advances in Neural Information Processing Systems* 35 (2022), pp. 25464–25477.

[Aac+23] Marcel Aach et al. “Large scale performance analysis of distributed deep learning frameworks for convolutional neural networks”. In: *Journal of Big Data* 10.1 (2023), p. 96.

[AXS23] Dana Alsagheer, Lei Xu, and Weidong Shi. “Decentralized Machine Learning Governance: Overview, Opportunities, and Challenges”. In: *IEEE Access* 11 (2023), pp. 96718–96732. DOI: 10.1109/ACCESS.2023.3311713.

[Bia+23] Tian Bian et al. “Decision Support System for Chronic Diseases Based on Drug-Drug Interactions”. In: *2023 IEEE 39th International Conference on Data Engineering (ICDE)*. IEEE. 2023, pp. 3467–3480.

[Che+23] Lingjiao Chen et al. “Data Acquisition: A New Frontier in Data-centric AI”. In: *arXiv preprint arXiv:2311.13712* (2023).

[Dun23] Jamie Duncan. “Data protection beyond data rights: Governing data production through collective intermediaries”. In: *Internet Policy Review* 12.3 (2023), pp. 1–22.

[Gra23] Mackenzie Graham. “Data for sale: trust, confidence and sharing health data with commercial companies”. In: *Journal of Medical Ethics* 49.7 (2023), pp. 515–522.

[Lan23] Luke Lango. “Why AI Will Drive Major PC Market Growth in 2024”. In: *InvestorPlace* (2023).

[Man+23] Zoltán Ádám Mann et al. “Towards practical secure neural network inference: the journey so far and the road ahead”. In: *ACM Computing Surveys* 56.5 (2023), pp. 1–37.

[Muñ+23] Antonio Muñoz et al. “A survey on the (in) security of trusted execution environments”. In: *Computers & Security* 129 (2023), p. 103180.

[Sin+23] Abhishek Singh et al. “Co-Dream: Collaborative data synthesis with decentralized models”. In: *ICML Workshop on Localized Learning (LLW)*. 2023.

[Was23] Noam Wasserman. “OpenAI’s Failed Experiment in Governance”. In: *Harvard Business Review* (2023). URL: https://hbr.org/2023/11/openais-failed-experiment-in-governance.

[Yua+23] Liangqi Yuan et al. “Decentralized federated learning: A survey and perspective”. In: *arXiv preprint arXiv:2306.01603* (2023).

[ZBL23] Mengxiao Zhang, Fernando Beltrán, and Jiamou Liu. “A survey of data pricing for data marketplaces”. In: *IEEE Transactions on Big Data* (2023).

[BOV24] Felix Brakel, Uraz Odyurt, and Ana-Lucia Varbanescu. “Model Parallelism on Distributed Infrastructure: A Literature Review from Theory to LLM Case-Studies”. In: *arXiv preprint arXiv:2403.03699* (2024).

[But24] Vitalik Buterin. *The promise and challenges of crypto + AI applications*. https://vitalik.eth.limo/general/2024/01/30/cryptoai.html. 2024.

[24] “COSMOS Protocol”. In: (2024). URL: https://cosmos.network/.

[DeG24] 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.

[Dix24] Chris Dixon. *Read Write Own. Building the Next Era of the Internet*. https://readwriteown.com/. 2024.

[Hua+24] Qiuyuan Huang et al. “Position Paper: Agent AI Towards a Holistic Intelligence”. In: *arXiv preprint arXiv:2403.00833* (2024).

[Kin24] Adrian Kingsley-Hughes. “What is an AI PC? (And should you buy one?)” In: *ZDNet* (2024). URL: https://www.zdnet.com/article/what-is-an-ai-pc-and-should-you-buy-one/.

[LAR24] Charles Lu, Mohammad Mohammadi Amiri, and Ramesh Raskar. “Data Measurements for Decentralized Data Markets”. In: *arXiv preprint arXiv:2406.04257* (2024).

[McA24] Megan McArdle. “Female popes? Google’s amusing AI bias underscores a serious problem”. In: *Washington Post* (2024). URL: https://www.washingtonpost.com/opinions/2024/02/27/google-gemini-bias-race-politics/.

[SB24a] Joseph Saveri and Matthew Butterick. *GitHub Copilot Litigation*. https://githubcopilotlitigation.com. Accessed: 2024-06-03. 2024.

[SB24b] Joseph Saveri and Matthew Butterick. *Stable Diffusion Litigation*. https://stablediffusionlitigation.com. Accessed: 2024-06-03. 2024.

[Zah+24] Matei Zaharia et al. *The Shift from Models to Compound AI Systems*. https://bair.berkeley.edu/blog/2024/02/18/compound-ai-systems/. 2024.

[Bau+] André Bauer et al. “Comprehensive exploration of synthetic data generation: A survey”. In: *arXiv preprint arXiv:2401.02524* ().

[BS] 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*. IEEE, pp. 326–331.

[FMJ] Dongyang Fan, Celestine Mendler-Dünner, and Martin Jaggi. *Collaborative Learning via Prediction Consensus*. arXiv: 2305.18497 [cs.LG].

[Jel+] Márk Jelasity et al. “Gossip-based peer sampling”. In: *ACM Trans. Comput. Syst.* 25.3 (), 8–es. ISSN: 0734-2071. DOI: 10.1145/1275517.1275520. URL: https://doi.org/10.1145/1275517.1275520.

[Liu+] Zelei Liu et al. “Contribution-aware federated learning for smart healthcare”. In: *Proceedings of the AAAI Conference on Artificial Intelligence*. Vol. 36. 11, pp. 12396–12404.

[Moo+] Michael Moor et al. “Foundation models for generalist medical artificial intelligence”. In: *Nature* 616.7956 (), pp. 259–265.

[Sin+] Abhishek Singh et al. “Posthoc privacy guarantees for collaborative inference with modified Propose-Test-Release”. In: *Advances in Neural Information Processing Systems* 36 ().

[XL] Xinyi Xu and Lingjuan Lyu. “A reputation mechanism is all you need: Collaborative fairness and adversarial robustness in federated learning”. In: *arXiv preprint arXiv:2011.10464* ().