DIP Protocol

The Decentralised Intellectual Property

Peeramid Labs
The AI Futures Collective
T. Pecerskis, A. Smirnovs, et al.
Email: contact@peeramid.xyz

***Abstract*—The proliferation of advanced Artificial Intelligence (AI) demands high-quality, verifiable data, yet the digital economy lacks robust frameworks for valuing and protecting this foundational intellectual property (IP). This gap exacerbates the tension between proprietary IP (often siloed via patents, the "patent secret dilemma") and open-source innovation (often unremunerated, limiting sustainability). Simultaneously, decentralization faces challenges from infrastructure centralization and vulnerable governance. This paper presents the Decentralised Intellectual Property (DIP) Protocol as a visionary strategic roadmap, outlining a novel framework designed to bridge these divides. DIP envisions a secure, liquid market for digital IP by integrating four core conceptual pillars: (1) a meritocratic system (ACIP) for generating data with verifiable provenance; (2) a game-theoretically sound economic architecture enabling Meritocratic Autonomous Organizations (MAOs); (3) a flexible infrastructure leveraging advanced cryptography (MPC, ZKML, FHE) for privacy-preserving computation and verification without disclosure; and (4) a model incentivizing true geospatial decentralization through specialized, high-commitment Authority Nodes, capable representing self-sovereign communities, coupled with Reciprocal IP Escrow and a sustainable, burn-driven emission model. By proposing mechanisms to enable verification without disclosure and creating pathways for both proprietary and open value creation, this paper outlines foundational concepts for a scalable and sustainable future technology. It explicitly identifies areas requiring further research to realize a more equitable, efficient, and institutionally-viable ownership economy for the burgeoning knowledge noosphere.**

***Index Terms*—Decentralized Intellectual Property; Data Markets; Zero-Knowledge Proofs; ZKML; Multi-Party Computation; DAO; Tokenomics; AI; Machine Learning.**

I. Introduction: A Strategic Vision for Decentralised Intellectual Property

This paper presents a strategic vision and foundational architecture for the Decentralised Intellectual Property (DIP) Protocol, a system designed to address fundamental challenges at the intersection of Artificial Intelligence, intellectual property (IP) rights, and decentralized systems. Recognizing the complexity of building such a comprehensive protocol, this document serves as a visionary blueprint and strategic roadmap. It outlines the core principles, innovative mechanisms, and a potential path forward, while explicitly acknowledging areas that necessitate significant further research and development before full realization. Our aim is to lay the groundwork for a scalable and sustainable future technology capable of resolving the persistent tension between the need for proprietary IP protection (the "patent secret dilemma") and the desire for open innovation often hampered by inadequate remuneration models in the open-source world.

A. The AI/ML Revolution and the Insatiable Demand for Verifiable Data

The contemporary technological landscape is being fundamentally reshaped by advancements in Artificial Intelligence (AI) and Machine Learning (ML). The capabilities of these systems, from large language models to sophisticated predictive analytics, are directly contingent upon the volume, relevance, and, most critically, the quality of the data on which they are trained. The foundational principle of "Garbage In, Garbage Out" (GIGO) dictates that even the most advanced algorithms will produce inaccurate, biased, or unreliable outcomes if trained on flawed data. This dependency has created an insatiable demand not merely for data, but for high-fidelity, verifiable, and "fit for purpose" datasets [1], [2].

The economic and strategic risks associated with poor data quality are substantial. They manifest as inaccurate predictions, the amplification of societal biases, and significantly inflated project costs, as data scientists expend a majority of their efforts on data cleaning and preparation rather than model development [3]. With AI adoption accelerating—78% of organizations reported using AI in at least one business function in 2024, supported by record levels of private investment—the market for premium data is expanding at an unprecedented rate [4]–[6].

This explosion in AI has also surfaced a new, systemic threat: model collapse. Recent research indicates that generative models trained recursively on synthetic or AI-generated data risk degrading in quality, losing diversity, and amplifying biases over time [7]. A study from Meta highlighted that even 1% of synthetic data in a training set can lead to this degenerative phenomenon, where larger datasets no longer yield performance improvements. Similarly, research from Anthropic has demonstrated a phenomenon termed "subliminal learning," where AI models can covertly transmit hidden behaviors and biases to other models through seemingly random data, a risk that is magnified by the industry's increasing reliance on synthetic data to reduce costs [8]. These challenges underscore a critical market need: a reliable and scalable source of high-quality, verifiably human-generated data to serve as a "ground truth" for training, fine-tuning, and re-calibrating the next generation of AI systems.

B. The Web3 Dilemma: Open-Source Ideals vs. The Unsolved IP Problem

The Web3 ecosystem, built on the principles of decentralization and permissionless innovation, has operated primarily under an open-source ethos. While this has been a powerful catalyst for development, it has simultaneously created a structural inability to value, protect, and monetize intellectual property (IP). The prevailing paradigm encourages the creation of digital public goods but offers no native mechanism to compensate their creators, leading to an extractive dynamic where centralized commercial entities can freely capitalize on open-source code and public data without remuneration [7]. This represents a significant market failure; for Web3 to mature and capture value at the scale of the traditional economy, it must evolve beyond a purely open-source model and develop robust frameworks for managing IP [9].

The challenges of protecting IP in a decentralized environment are profound. Traditional legal frameworks rely on centralized authorities for enforcement, a model that is incompatible with the pseudonymous, borderless, and immutable nature of blockchains. Issues of anonymity, jurisdictional ambiguity, and the finality of on-chain transactions render conventional IP enforcement mechanisms largely ineffective. The market has begun to recognize the immense value in solving these deep, structural problems. The significant valuation of companies like Zama, which focuses on providing on-chain confidentiality through advanced cryptography, serves as a powerful market signal that verifiable privacy and data control are not peripheral features but core components of Web3's future value proposition [10]. The open-source ethos of Web3 can be understood not just as a philosophical choice, but as a direct technical consequence of its failure to solve the underlying data control problem. In the absence of a trusted central authority, verifying the value of a digital asset has historically required direct access to it. However, in a trustless environment, granting access is tantamount to relinquishing control. Faced with this paradox, the only viable path to permissionless collaboration was to make the IP—the code and the data—open by default. A technical solution that allows for verification without disclosure would fundamentally break this dependency, enabling a new paradigm for proprietary IP in decentralized ecosystems.

C. The Data Disclosure Challenge: Why Traditional IP Fails in Trustless Environments

The core technical barrier preventing the emergence of a robust market for digital IP is the data disclosure problem. This refers to the fundamental paradox that to prove the value or verify the properties of a piece of digital information, one has historically been required to disclose the information itself, thereby destroying its scarcity and commercial value as exclusive IP **wallarm˙info˙disclosure**, [11]. Any party who is granted a copy of a dataset for evaluation can subsequently redistribute that copy publicly, making the asset worthless. This problem has long been considered intractable in trustless systems, confining valuable data to centralized, walled-garden platforms where trust is enforced through legal agreements and platform-level controls rather than technical guarantees.

This challenge is precisely why a true, decentralized data economy has failed to materialize. Without a cryptographic solution, the exchange of valuable data requires trusting a counterparty or an intermediary, reintroducing the very centralization that Web3 seeks to eliminate. The problem is not merely one of preventing unauthorized copying (a task at which digital rights management has largely failed) but of enabling confident commercial exchange. A buyer needs to verify that a dataset meets their specifications before purchase, but the seller cannot provide the data for verification without losing control over it. This dilemma has been the primary impediment to the creation of liquid, open markets for proprietary data. The solution to this long-standing problem lies in advanced cryptographic primitives that can decouple verification from disclosure, allowing for computation and validation to be performed on encrypted or otherwise obscured data.

D. Thesis: Introducing DIP as a Foundational Layer for Verifiable Digital IP

This paper introduces the Decentralised Intellectual Property (DIP) Protocol, a novel framework designed to create a secure, transparent, and liquid market for digital IP by directly solving the data disclosure problem and the challenge of verifiable network decentralization. The protocol's architecture is built upon four integrated pillars:

1) **Meritocratic Provenance:** A system for generating data with a verifiable and auditable history, rooted in the demonstrated competence of its human and AI contributors. This ensures that data quality is not a subjective label but an emergent property of a rigorous, incentive-aligned process.
2) **Meritocratic Autonomous Organizations (MAOs):** A sophisticated economic model that evolves the DAO concept, enabling the creation of unified digital marketplaces governed by dynamic, competitive, and merit-based principles rather than static token-based voting.
3) **Privacy-Preserving Infrastructure:** A flexible, L2-native network of service nodes utilizing a spectrum of cryptographic techniques, including Multi-Party Computation (MPC) and Zero-Knowledge Machine Learning (ZKML), to solve the data disclosure problem.
4) **Geospatial Decentralization:** A node participation model that moves beyond simplistic token staking to incentivize tangible, real-world infrastructure investment, providing a systemic solution for on-chain institutional compliance and resilience.

The demand for high-quality data from the AI industry represents the practical for such a protocol. Unlike many previous Web3 use cases that created self-contained economies, the AI data market is a massive, external, and established economy that Web3 is currently ill-equipped to service. By providing the infrastructure for verifiable quality, secure access, and liquid exchange, DIP aims to act as a bridge, enabling the

decentralized world to capture a significant share of this multi-trillion dollar market. The following sections will provide a detailed exposition of the protocol's theoretical underpinnings, economic model, and technical infrastructure.

II. Literature Review and Related Work

The DIP protocol, draws upon and differentiates itself from several key areas in decentralized systems and applied cryptography.

A. Decentralized Privacy and Computation Technologies

Numerous approaches aim to bring privacy and complex computation to blockchains:

- **Centralisation in blockchain:** Ethereum being one of industry and thought leaders protocol in distributed ledgers today still sufferst from substential centrlisation risk [12] [13]. It's inability to physically incentivize geo-spatial decentralization is confirmed and still is unresolved challenge [14], while proof-of-stake on it own as a system introduces a restrictive participation behavior, making it harder for new members to join the network in a non-permissioned way. Similarly, Bitcoin like proof-of-work is not believed to be sustainable due to it's environmental impact [15].
- **Lattices based Fully Homomorphic Encryption (FHE):** Schemes like those being developed by Zama [10] and FHEnix [16] [17] allow computation on encrypted data with substantial performance. This works proposes general-purpose FHE directly in EVM opcodes. The major challenge however stays in the re-encryption proxies required to communicate with FHE server stays to be a bottleneck, with both Zama and FHEnix employing centralised model that has not been fully resolved up to the date and requires to fallback in to trusted execution environment.
- **Threshold Cryptography and Multi-Party Computation (MPC):** Protocols like Lit Protocol [18] or general MPC [19] use threshold cryptography to manage distributed keys and access control. More advanced MPC protocols for cryptographic operations, such as DKLS23 for distributed key generation and signing [19], offer robust security models.
  Limitations: While powerful for specific use-cases (like decentralized custody or co-signing), many MPC protocols, especially for complex operations beyond signing, can exhibit high communication complexity (e.g., $O(n^2)$ or higher for n parties) for each operation. This makes them potentially less suitable as a universal, per-transaction solution for frequent, general-purpose data decryption/re-encryption tasks envisioned for all Cypher Nodes in a highly scalable L2, where efficiency is paramount.
- **Trusted Execution Environments (TEEs):** TEEs offer hardware-based isolation for secure computation. While providing practical privacy, they introduce specific trust assumptions about hardware manufacturers. Numerous of attack vectors has been proven to render TEEs generally vulnerable, beyond simple supply chain risks. [20] [21] [22]
- **ICP vetKeys:** The Internet Computer Protocol offers vetKeys (verifiably encrypted threshold keys) [23] for applications requiring decentralized key management and encryption services, yet creates a architecture vendor specific solution.
- **Zero knowledge cryptography:** Advancements in zero-knowledge cryptography are substentially acelerated thanks to distributed ledger advancements and show promising metrics for high intensity computation optimisation via privacy perserving proofs, with proof systems have experienced exponential performance improvements [24] [25]. Such proofing systems allow machine-learning on private datasets, proving private inputs against public models, or validating data integrity for black-box systems.

B. Decentralized Storage and Identity

- **Decentralized Storage Networks (DSNs):** Platforms like Filecoin [26], Arweave [27], and Swarm [28] provide robust solutions for data persistence. These protocols however do not focus on access control layers nor fully integrate existing blockchains as payment environment.
- **Decentralized Identity (DID) and Verifiable Credentials (VCs):** While DIDs [29] and VCs offer standards for identity and claims.

C. Electronic data privacy law regulations

Various jurisdictions issued strong personal identifiable information privacy policies over past decade that can all together be summed as fundamental rights of individuals for their data ownership, as well as requirement for personal data, generally to stay in the jurisdictions, without cross-border transfers, which puts substantial legal implications on modern cloud infrastructure [30]–[32]. Cases already present showing courts ready to rule against surveillance that does not provide adequate protection for their jurisdictional data [33].

III. A New Foundation: Decentralizing private key infrastructure

As can be noted from literature review section, the various solutions such as Trusted Execution Environments, Threshold and FHE Cryptography and even distributed ledgers such as Ethereum suffer from various risks which all have common property in common - they all require private key infrastructure that is intrinsically a physical, real-world asset that cannot be thought as purely mathematical object.

While many solutions overview take a mathematical approach in solving this trough complex cryptography [10], [23] they all in fact in closer review are falling back to trusted execution environment that is proven to be not secure [20]–[22] and with regulatory context in mind - not viable for large scale intellectual property and RWA management [30]–[32].

Progress in TSS encryption for FHE and zero knowledge cryptography however implies [16], [24] strong computational potential is possible, however is still limited. The bottleneck stays in trust assumptions for honest node majority. In protocols like Zama or FHEnix, the majority of nodes can decrypt all of the encrypted content and it is intrinsically hard to scale such multi-party-computation to large extends of nodes because of exponential networking complexity.

To address these problems, we propose to fallback to existing web2 experience, and formalize what already works - physical jurisdictional compliance enclaves, that are not just mathematically, but also legally and geo-spatially decentralized in their nature. Users should physically be able to chose where their PKI is stored by selecting a policy.

Instead of trying to define one-works-for-all solution for PKI, the DIP protocol offers a free market solution. FHEnix introduces precompiles for ethereum virtual machine such as *FHE.encrypt(data)* and *FHE.decrypt(data)*, we propose to extend it with *policy* pointers: *DIP.encrypt(data, policy)* and *DIP.decrypt(cipher, cipherId)* where *policy* is a set of rules defined by protocol that involve information about i) responsible node, ii) backup recovery policy iii) service level agreement and corresponding stakes and *cipherId* is resulting identifier of encrypted data associated with particular policy, representing a binding service-level agreement commitment.

A. Network node functions

The foundational infrastructure of the DIP Protocol is a decentralized network of independent node operators who provide the critical computational and storage resources required for the protocol to function. However, unlike validators in traditional Proof-of-Stake networks whose primary contribution is capital-based signing, DIP Nodes provide tangible, verifiable services. Their core responsibilities are:

- **Privacy-Preserving Computation:** Performing authorized encryption, decryption, and participating in the MPC schemes for key management.
- **Provenance Attestation:** Signing and attesting to the integrity of data generation processes.
- **General computation:** Any other computation can be built on top and extended with proofing system, creating decentralized cloud computing paradigm.

This service-oriented role provides a systemic solution to the challenge of blockchain decentralization. Because node operators must compete on the quality and security of their services, they are incentivized to make tangible investments in their infrastructure. This creates a market where nodes can differentiate themselves based on:

- **Jurisdictional Guarantees:** A node can operate within a specific legal jurisdiction (e.g., Switzerland, Singapore) to appeal to institutional clients with strict data residency requirements.
- **Verifiable Security:** Node operators are incentivized to obtain security certifications (e.g., SOC 2, ISO 27001) and even allow physical inspection of their data centers to attract high-value clients.
- **Specialized Hardware:** Nodes may offer specialized hardware, such as Trusted Execution Environments (TEEs) or high-performance GPUs for ZK proof generation, creating a tiered market for different levels of security and performance.
- **Decentralization:** While we speak of DIP node as singular entity, we assume that node can act as aggregated signature, acting as a gatekeeper for larger, underlying network of nodes such that could provide high redundancy and security by own design, examples of such could be Zama, Internet Computer, IEXEC or others.
- **Latency:** Offering services with lower latency or higher reliability for specific regions.

This transforms decentralization from an abstract metric into a verifiable, market-driven feature, solving a major adoption barrier for enterprise and institutional use of blockchain technology.

1) A Market for Privacy Technologies: This market-driven approach also extends to the underlying privacy technologies employed by the nodes. While cutting-edge solutions like Fully Homomorphic Encryption (FHE) offer the ability to compute on encrypted data, the DIP protocol does not mandate its exclusive use. A core design principle is to foster a competitive marketplace where different technological trade-offs can coexist. The security of any advanced cryptographic primitive is strongly dependent on its specific implementation, and for many use cases, the performance overhead of FHE may be unnecessary. Therefore, the protocol allows for a heterogeneous network where different nodes can offer different solutions:

- **FHE-based Nodes:** For high-assurance applications requiring complex computations directly on encrypted data, where performance is a secondary concern to absolute privacy.
- **Hardware-Isolated Nodes:** Utilizing Trusted Execution Environments (TEEs) like Intel SGX or AMD SEV to provide practical privacy with high performance for simpler tasks, appealing to users who accept hardware-based trust models.
- **MPC Nodes:** Focusing on robust key management and secure multi-party computation for access control without relying on specialized hardware or the computational intensity of FHE.

This flexibility allows users and data creators to select the node that provides the optimal balance of security, performance, and cost for their specific needs, rather than enforcing a one-size-fits-all cryptographic solution.

B. A Decentralized Key Management Scheme via Multi-Party Computation (MPC)

A critical security challenge for any system that manages encrypted data is the management of decryption keys. A centralized key holder would represent a single point of failure and a prime target for attack. The DIP Protocol addresses this challenge through a sophisticated, decentralized key management

architecture that utilizes Multi-Party Computation (MPC) [34]. MPC is a cryptographic subfield that allows multiple parties to jointly compute a function over their inputs while keeping those inputs private. In DIP, it is used to manage decryption keys without any single party ever holding a complete key.

The protocol employs a two-key MPC scheme to balance efficiency with security:

- **Key Share 1 (Node-Specific Key):** For any given RFD, the primary decryption key is secret-shared. A crucial share is held by the specific DIP Node selected by the Buyer. This allows for highly efficient and low-cost data access under normal operating conditions. The node operator is held accountable through a slashing mechanism; if they can be proven to have colluded in disclosing data to an unauthorized party, their stake is forfeited.
- **Key Share 2 (Network Consensus Key):** A second, complementary share of the decryption key is distributed among the broader consensus of DIP network participants (or a designated committee thereof). This network key is not used for routine data access. It serves as a high-reliability, decentralized backup mechanism. In the event that the primary DIP Node becomes unavailable or maliciously withholds data, the LAT holder can petition the network. If the request is validated by consensus, the network can use its key share to reconstruct the full key and grant the holder access to their data.

This dual-key architecture provides the best of both worlds: the efficiency of a single, designated operator for normal operations, and the robust security and liveness guarantees of a fully decentralized consensus mechanism for fault tolerance and recovery **coindesk˙mpc**, **wipro˙mpc**.

What if a specific node becomes unavailable, The data cannot be lost. With a robust recovery mechanism as opt-in policy, every piece of encrypted data can be rescued by policy settings.

We assume this is obvious that such protocol can be extended with nested policies, sub-jurisdictional recovery authorities and can support both on-chain active FHE encryption and more regular off-chain data gating.

C. On-Chain Computation on cross-policy encrypted data

In regular case of FHE encryption, there is just one FHE virtual server that is run as co-processor. This is a very key problem of both centralisation of TSS keystores and also breaking the privacy directives for compliance reason.

In case of DIP protocol, the computation becomes consensus driven SLA policy execution between two different nodes.

Calculation now takes form of multi-party FHE. Imagine you have Bob possess number *B* encrypted as *BCipher* with *BCipherId* and Alice with *A* encrypted as *ACipher* with *ACipherId* that command a smart contract logic to execute calculation of two numbers that they possess, and publish a public result on chain as public record.

To do that, instead of using global FHE server, Bob and Alice only need to decrypt their own shares and then either by doing turing-complete MPC, or setting up a shared FHE server, conduct a calculation:

$$x = MPC(ACipherId + BCipherId) \tag{1}$$

In order for this computation to be sound, Bob and Alice would need to provide shared zero-knowledge proof that their part of computation was done correctly to convince rest of network in their computation correctness. In fact, this architecture from network perspective already is well explored in zero-knowledge rollup space.

IV. A New Foundation: Meritocratic Provenance and Verifiable Competence

A. Redefining Data Quality: From Subjective Labels to Provable Merit

In the context of the data economy, the term ”data quality” is often ambiguous and subjective. The DIP Protocol posits that a more robust and useful concept is data provenance: a cryptographically verifiable and immutable record of a data asset’s entire lifecycle, from its origin and creation process to the demonstrated competence of the agents who contributed to it [35]. Within this framework, true quality is not an externally applied label but an emergent and intrinsic property of a well-defined, meritocratic, and transparent generation process. The protocol reframes the central question from ”How can we verify that this data is high-quality?” to ”How can we design a system that reliably produces high-quality data as its natural output?” The answer lies in establishing a verifiable measure of competence for the agents—both human and AI—who create and curate the data.

B. The Autonomous Competence Identification Protocol (ACIP) as the Engine of Provenance

The core mechanism for establishing data provenance in the DIP Protocol is the Autonomous Competence Identification Protocol (ACIP), a novel system for ranking agents in trustless environments based on verifiable merit [7], [36]. ACIP provides the foundational layer for ensuring that data is generated by agents with demonstrated expertise in a given domain.

ACIP formally defines competence as a quantifiable measure derived from the time and resource an agent is willing to commit to a specific domain, and peer-assessed recognition resulting from such an activity [7]. This protocol result is a dynamic ranking ladder where participants join tiered groups and engage in competitive interactions, or ”elections,” to choose a group delegate. Advancement to higher ranks requires succeeding in these time-locked, cost-based competitions.

The protocol’s design is inherently resistant to Sybil attacks. The cost to participate in a ranking event, X_{id}, is a function of the time commitment, T_{id}, and protocol-wide constants. To deterministically manipulate the system and achieve a high rank, an adversary would need to win multiple sequential ranking events. The total cost to achieve Rank R, $C_{TotalSybilToRankR}$, scales exponentially with the rank, as described by the equation (Eq. 1) .

$$C_{TotalSybilToRankR} \approx \sum_{k=0}^{R-1} N_{min}^{R-1-k} \cdot X_{avg\_group\_cost} = X_{avg\_group\_cost} \cdot \frac{N_{min}^{R} - 1}{N_{min} - 1} \tag{2}$$

where N_{min} is the minimum number of participants per group and $X_{avg\_group\_cost}$ is the average cost to control a single group instance [7]. This exponential cost structure makes sustained, high-rank Sybil attacks prohibitively expensive for a rational actor.

Furthermore, ACIP moves beyond a single, monolithic score by representing competence as a multi-dimensional vector, $P_r = (c_1, c_2, ..., c_m)$, where each component quantifies proficiency in a distinct domain (e.g., image annotation, code analysis, legal review). This allows for a nuanced and verifiable representation of an agent's specific expertise, forming the basis for a rich "competence multiverse" [7].

C. Collaborative Curation: Generating High-Fidelity Datasets with the Continuous Voting-Proposing Protocol (CVPP)

While ACIP provides the framework for identifying competent agents, the Continuous Voting-Proposing Protocol (CVPP) provides a practical methodology for these agents to engage in collaborative knowledge work, such as the creation of high-fidelity datasets [7], [37]. CVPP is a structured, gamified protocol that facilitates group consensus and ordering of information through iterative rounds of private proposals and voting.

The protocol operates in distinct stages:

1) **Proposing Stage:** Participants privately submit proposals (e.g., data points, labels, or other contributions) to a neutral facilitator or smart contract.
2) **Voting Stage:** The aggregated, anonymized proposals are presented to the group, and participants vote on their preferred submissions.
3) **Reveal Stage:** Scores are tallied, and the results, including proposer identities, are revealed.

This process, particularly the private nature of proposing and voting, is designed to mitigate common cognitive biases such as the halo effect or bandwagoning, encouraging participants to evaluate contributions on their intrinsic merit [7]. Empirical studies of a CVPP implementation for collaborative playlist curation demonstrated high participation rates (95% for active users) and high user satisfaction with the quality of the output (92% rating), validating its efficacy as a mechanism for generating community-vetted, high-quality ordered lists, which serve as a direct proxy for curated datasets [7].

The integration of ACIP and CVPP creates a powerful data generation engine. ACIP identifies and assembles groups of verifiably competent experts for a specific task, and CVPP provides them with a structured and incentive-aligned process to collaboratively produce a high-quality dataset. The entire process—the proposals, the votes, the evolution of consensus—is recorded on-chain, creating a rich, auditable trail of the dataset's provenance. This trail is the dataset's metadata, embedded at the moment of creation.

D. From Competence to Quality: A Formal Model ($q = f(x, t)$)

The synthesis of the ACIP and CVPP frameworks allows for a formal, quantifiable model of data quality. We can define the quality of a dataset, q, as a function of the energy and time invested in its creation:

$$q = f(x, t) \tag{3}$$

In this model:

- q represents the data quality, a verifiable and predictable output of the protocol. It is a measure of the dataset's fidelity, accuracy, and relevance, as determined by a meritocratic peer-review process.
- x represents the energy committed to the process. This is the irreversible financial stake, X_{id}, required for participation in an ACIP ranking group, which serves as a costly signal of commitment and a deterrent to low-effort or malicious contributions [7].
- t represents the time commitment, T_{id}, required to finalize a competitive interaction within a group. This ensures sustained engagement and prevents superficial participation [7].
- f represents the process function itself—the set of rules and interactions defined by the ACIP and CVPP protocols. It is the competitive, peer-validated mechanism that transforms the inputs of time and energy into the output of verifiable quality.

The core assertion of the DIP Protocol is that by precisely defining and controlling the inputs (x, t) and the process (f), the system can reliably produce data of a predictable and verifiable quality level, q. This allows the protocol to programmatically target and generate datasets that meet specific quality thresholds, such as the "top quartile" of all datasets within a given domain, and to provide cryptographic assurances of this quality to consumers. This model of meritocratic data generation offers a systemic defense against the threat of AI model collapse. By requiring verifiable commitments of time and economic stake, the protocol creates a high barrier to entry that is straightforward for motivated humans to meet but economically infeasible for automated agents to fake at scale. The output is a continuous stream of data with strong cryptographic and economic guarantees of its human-centric, high-effort origin. This stream can serve as a trusted "gold standard" for the AI industry, providing a crucial and verifiable source of ground-truth data to benchmark, fine-tune, and safeguard AI models against degradation.

V. Economic Architecture: Liquid Access and Aligned Incentives

A. Liquid Access Tokens (LATs): A Novel Primitive for Quantized Data Quality

The core economic primitive of the DIP Protocol is the **Liquid Access Token (LAT)**. A LAT is a fungible (e.g. ERC-20 [38]) or semi-fungible (ERC-1155 [39]) digital asset that represents a tokenized right to access a specific dataset or data stream at a defined quality level, q. Each LAT is a claim on a piece of intellectual property whose provenance and quality have been established through the ACIP and CVPP mechanisms.

The defining innovation of LATs is their liquidity. Unlike traditional, static access credentials or the non-transferable Soulbound Tokens (SBTs) proposed in other identity systems, LATs are designed to be freely tradable, creating a dynamic, open market for data access [7]. This transforms intellectual property from an illiquid, difficult-to-price asset into a standardized, composable, and liquid financial instrument.

The tokenomics of LATs are flexible and can be tailored to specific use cases, enabling a variety of access models:

- **One-Time Access:** A LAT can be designed to be burned upon use, granting a single, exclusive access to the underlying data. This model is ideal for buyers who require data exclusivity for training a proprietary AI model.
- **Subscription Access:** Holding a certain number of LATs could grant continuous access to a data stream for a defined period, functioning like a decentralized subscription service.
- **Tiered Access:** The quantity of LATs held could determine the level or granularity of data access, allowing for more sophisticated pricing and packaging of IP.

By quantizing data quality (q) and representing it as a liquid token, the DIP Protocol creates the necessary conditions for efficient price discovery and allocation of intellectual property in a decentralized market.

B. The Three-Party Escrow Model: An Advanced Use Case for High-Value IP

While the DIP protocol provides a flexible foundation for various data commerce models, its full power is demonstrated in a novel three-party escrow system designed for high-value, enterprise-grade IP exchange. This model is designed based on game-theoretic principles to align the incentives of three distinct, rational agents: the Buyer, the Expert Community, and the Expert Guild [40], [41].

- **The Buyer (Purchaser):** An entity (e.g., an AI company) seeking to acquire high-quality data. The Buyer initiates a transaction by issuing a Request-for-Data (RFD). This RFD is a smart contract that specifies the desired data type (or generally - knowledge work), the required quality level (q), and any other parameters (such as the ZKML verification model, detailed in Section 4). The Buyer funds this contract with the payment, which is held in escrow. Their primary objective is to acquire verifiably clean data with minimal counterparty risk.
- **The Expert Community (Workers):** A decentralized network of individuals or AI agents who participate in the ACIP/CVPP framework to generate data. By contributing their time and expertise, they earn LATs corresponding to the quality of the data they produce. Their primary objective is to monetize their skills by selling their earned LATs to fulfill a Buyer's RFD.
- **The Expert Guild (DAO as Steward):** A Decentralized Autonomous Organization (DAO) that serves as the trusted third-party escrow agent, arbitrator, and long-term *steward* of the intellectual property. Guilds are formed by high-ranking experts who have achieved a significant level of competence within a specific domain and have chosen to transition from active data creation to a governance and curation role. The Guild's primary objective is to maintain the long-term value of its ecosystem. This includes not only facilitating transactions but also ensuring the ongoing availability and monetization of the data assets created by its community. As such, the Guild is the recipient of **Data Retention Fees** from Buyers, and it is the Guild's responsibility to use these fees to contract with and incentivize DIP Nodes for secure, long-term data hosting. This aligns the Guild's incentives with the perpetual value of the IP, rather than just the initial sale.

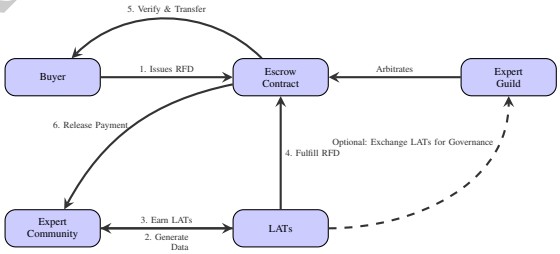

Fig. 1. The Three-Party Escrow Model. The Buyer issues an RFD, Workers provide data for LATs, and the Guild acts as a reputation-based arbiter, creating a game-theoretically balanced system.

This three-party model creates a system of checks and balances where each participant is incentivized to act honestly to maximize their own utility, leading to a stable and self-regulating market equilibrium.

C. Tokenomics of LATs: Governance, Staking, and Liquidation Dynamics

The incentive alignment at the heart of the escrow model is driven by a unique tokenomic mechanism centered on the relationship between LATs and the governance of the Expert Guild.

A fundamental feature of the protocol is that experts who earn LATs have the option to convert them into the Guild's native governance tokens. This provides a valuable "exit" opportunity for experts, allowing them to transition from being active workers to becoming stakeholders in the governance and

long-term success of the ecosystem. However, this conversion right creates a central economic tension, which can be termed the **Dilution Dilemma**. From the perspective of the existing governance token holders of the Guild, every LAT conversion represents a dilution of their voting power and their claim on the Guild's future revenue. Therefore, while the Guild is broadly incentivized to foster a vibrant ecosystem to attract more business, its incumbent governors are specifically incentivized to minimize the rate at which new governance tokens are minted via LAT conversion.

The Buyer's RFD is strategically designed to leverage this tension. A key condition of the RFD smart contract is that any LATs purchased to fulfill the request must be permanently locked or burned. This clause makes the transaction highly attractive to the Expert Guild. By agreeing to act as the escrow and arbitrator for the RFD, the Guild not only facilitates economic activity (from which it may derive fees) but also ensures that this specific transaction eliminates a quantum of potential governance dilution.

This dynamic establishes a robust game-theoretic equilibrium:

- The Guild is strongly motivated to provide fair and rigorous escrow services to attract more Buyers. Each successful transaction reinforces its reputation and, through the LAT burn mechanism, protects its governance from dilution.
- The Buyer is motivated to use the Guild's escrow service because the Guild's self-interest in maintaining its reputation and preventing dilution makes it a credible and aligned arbiter of data quality.
- The Experts are motivated to produce high-quality data to earn LATs, confident that they have two viable paths to monetization: selling directly to a Buyer's RFD or converting their LATs into a long-term governance stake.

In the event of a dispute where a Buyer deems the provided data to be inappropriate, the resolution is governed by this incentive structure:

- If the Guild sides with the Buyer against the Workers: The Workers' staked LATs are slashed or burned, and the payment is returned to the Buyer. This outcome is favorable to the Guild's governance holders (as it prevents dilution) and reinforces its reputation for upholding high standards with Buyers. However, if this power is used unfairly, it will damage the Guild's reputation with the Expert Community, potentially causing them to migrate to a competing Guild.
- If the Guild sides with the Workers against the Buyer: The payment is released to the Workers. This maintains the trust of the expert base but risks damaging the Guild's reputation among Buyers, who may see the Guild as insufficiently rigorous.
- If the Workers and Buyer agree to bypass the Guild: This scenario is disincentivized by the protocol design, as the Guild provides the foundational trust, security, and dispute resolution framework that makes the permissionless transaction viable in the first place.

This system creates a self-regulating market for trust. A Guild that arbitrates poorly will either lose market share as both Buyers and Experts migrate to Guilds with a more balanced and reputable track record or will experience governance quorum rebalancing with time, according to ACIP protocol time-invariant properties. This competitive pressure forces Guilds to optimize for long-term fairness and sustainability, effectively creating a decentralized, market-driven judicial system for intellectual property.

D. From DAOs to MAOs: A Paradigm of Competitive Governance

The protocol's architecture enables a profound evolution of decentralized governance, from the standard Decentralized Autonomous Organization (DAO) to a **Meritocratic Autonomous Organization (MAO)**. In a traditional DAO, a 51% governance capture is often seen as a catastrophic failure. In an MAO, powered by the principles of ACIP, temporary quorum capture is an expected and acceptable part of a dynamic, competitive system.

This paradigm shift is possible because ACIP's time-financial constraint, $q = f(x, t)$, makes permanent, centralized control economically irrational. Any party wishing to seize governance control faces a clear trade-off: the faster they wish to acquire power (reducing time, t), the exponentially higher the energy and capital cost they must expend (x). This creates a system where governance control is likely to be in a constant state of flux, oscillating between competing parties who are judged by the merit of their decisions, rather than being captured permanently by a single, entrenched entity.

E. Mitigating Collusion and Ensuring Rational Agency

The primary threat to any multi-party system is collusion. The DIP Protocol incorporates several layers of defense, inherited primarily from the design of ACIP, to ensure that collusion between any two parties against the third is economically irrational or technically infeasible over the long term.

The first line of defense is the cost of participation. As established in ACIP, achieving a high rank and the ability to generate valuable LATs requires a significant and irreversible investment of time and capital [7]. This "skin in the game" disincentivizes short-term, extractive behavior.

The second layer of defense is transparency and randomization. All core interactions—group formation, voting, and escrow transactions—are recorded on-chain. This transparency allows for the application of collusion clustering analysis, where voting patterns and social graphs can be monitored to identify and flag coordinated, non-meritocratic behavior [7]. Furthermore, ACIP can incorporate randomized participation in ranking events, making it difficult for colluding groups to guarantee they are placed in the same competitive instance [7].

Finally, the economic model itself provides a strong defense. For example, if a Guild and a group of Workers were to collude to defraud a Buyer with low-quality data, the public and immutable nature of the blockchain record would

permanently damage the Guild's reputation. The short-term gain from the single fraudulent transaction would likely be outweighed by the long-term loss of future business from other Buyers, who would shun the now-untrustworthy Guild. This aligns with research on collusion-resistant mechanisms, which demonstrates that well-designed incentive structures can make joint deviation from honest behavior unprofitable [42]–[44]. The protocol is designed such that the dominant strategy for all participants is long-term, honest cooperation.

VI. Protocol Infrastructure: Verifiable Decentralization and Privacy

1) Node Economic Model and LAT Requirements: To ensure a sustainable and reliable network of service providers, DIP Nodes are compensated through a clear economic model. Nodes register their capabilities and pricing structures on-chain, allowing for a transparent service marketplace. The primary revenue streams are:

- **Service Fees:** Direct payments for computational work, such as processing a decryption request or generating a proof.
- **Data Hosting Fees:** Long-term revenue, paid by Expert Guilds from their collected Data Retention Fees, to ensure the ongoing, persistent, and secure storage of data assets. This provides a stable, recurring revenue stream that incentivizes node reliability and longevity.

For certain high-value use cases, particularly within the RFD framework, an additional economic requirement may be imposed on the service-providing node. A Buyer or Guild issuing an RFD can specify that the chosen DIP Node must itself hold the relevant LATs to be eligible to service the request. This creates a powerful, skin-in-the-game dynamic: to be entrusted with managing a specific class of high-value data, a node must first be an economic stakeholder in that same data. This requirement can be programmatically enforced by the RFD smart contract.

A. Security and Consensus: An L2-Native Approach

The DIP Protocol is designed to be architecturally agnostic and deployable on any sufficiently advanced EVM-compatible Layer 2 (L2) network. It inherits the security and consensus mechanism of its host chain. The network's core security is not maintained by the DIP Nodes themselves, but rather by the standard validators of the L2, who stake the host chain's native asset (e.g., ETH).

This deliberately decouples the role of network security from the role of specialized service provision. DIP Nodes are economic actors who compete in a free market to provide privacy and data management services, while network validators are responsible for the integrity of the underlying ledger.

B. Solving the Disclosure Problem: A Verifiable Quality Function Interface

The technical core of the DIP Protocol, and its solution to the data disclosure problem, lies in establishing a standardized interface for a **verifiable quality function**. This is a smart contract interface that allows a Buyer to programmatically define the conditions a dataset must meet. The protocol remains agnostic to the specific verification method, allowing for a spectrum of trust models to coexist in a competitive marketplace. The interface is designed to support two primary modes of verification:

- **Pre-Purchase (Trustless) Verification:** This model solves the data disclosure problem completely by allowing for verification before the data is revealed to the Buyer. This is the most secure method, ideal for high-value IP exchange in fully trustless environments. The primary implementation for this is Zero-Knowledge Machine Learning (ZKML), as detailed below.
- **Post-Purchase (Dispute-Based) Verification:** For lower-stakes transactions or in cases where the Buyer and Seller have a pre-existing degree of trust, a simpler model can be used. The data is delivered to the Buyer upon payment, but the funds are held in escrow for a defined period. The Buyer can then run their own quality checks. If the data is found to be deficient, the Buyer can submit proof of this deficiency to the escrow contract to initiate a dispute, which is then arbitrated by the Expert Guild.

This flexibility allows participants to choose the appropriate trade-off between cryptographic security and transactional simplicity for their specific needs.

1) Advanced Implementation: Zero-Knowledge Machine Learning (ZKML):

C. Native Opcodes for Efficient Privacy Services

If the DIP protocol is implemented as a sovereign Layer 1 or Layer 2, it can introduce novel, precompiled contracts or native EVM opcodes to dramatically improve the efficiency and developer experience of interacting with its privacy infrastructure. These opcodes would serve as a standardized, gas-efficient interface for smart contracts to request services from the network of DIP Nodes.

For example, the protocol could include:

- `DIP_ENCRYPT_POLICY`: A precompile that allows a smart contract to submit a data payload, specify an access policy (e.g., requiring ownership of a specific LAT), and request its encryption and storage by a designated DIP Node. The precompile would handle the routing of the request to the node and the on-chain registration of the access policy.
- `DIP_DECRYPT_REQUEST`: A precompile that allows a smart contract, on behalf of a user, to verify the necessary on-chain conditions (e.g., burning a LAT) and then formally request the decryption of the corresponding data from the responsible DIP Node.

By embedding these functions at the protocol level, the cost and complexity of calling these services are significantly reduced. It abstracts away the need for developers to manage complex off-chain communication with nodes, making the integration of advanced privacy features as simple as a standard smart contract call. This deep integration makes the

TABLE I
COMPARISON OF IP MANAGEMENT PARADIGMS

Feature	Traditional Legal System	NFT Licensing (e.g., CC0)	DIP Protocol
Proof of Origin	Relies on registration with centralized authorities (e.g., patent offices). Can be slow, expensive, and geographically limited.	On-chain token minting provides a timestamped proof of creation, but does not verify the creator's identity or originality.	Cryptographically signed actions within ACIP/CVPP create an immutable, on-chain record of contribution tied to a meritocratic identity.
Proof of Quality	Relies on subjective, ex-post evaluation (e.g., market success, expert reviews). No objective, a priori guarantee.	None. The quality of the underlying asset is completely divorced from the NFT that represents it.	Quality (q) is a quantifiable, verifiable output of the meritocratic generation process. Can be objectively proven using ZKML.
Access Control	Enforced through legal agreements and technological restrictions (DRM), which are often brittle and centralized.	Generally none. Access is often public, with the NFT representing a social claim of ownership rather than technical control.	Access is cryptographically enforced via LATs. The protocol allows for granular, programmable access logic (e.g., one-time, subscription).
Liquidity	Highly illiquid. IP transactions are bespoke, high-friction legal processes that can take months or years.	Liquid market for the NFT "wrapper," but not necessarily for the underlying IP rights, which are often ambiguous.	High. LATs are designed as liquid, fungible/semi-fungible assets, creating a dynamic, low-friction market for IP access rights.
Dispute Resolution	Centralized, expensive, and slow court systems. Access to justice can be prohibitive for smaller creators.	Rudimentary and often off-chain. Relies on platform-level moderation or social consensus, with no binding enforcement mechanism.	Decentralized, game-theoretically balanced arbitration provided by Expert Guilds. Incentives are aligned for fast, fair, and low-cost resolution.
Scalability	Low. Each transaction requires significant manual legal and administrative overhead.	High scalability for token transfers, but lacks scalable mechanisms for quality control or rights enforcement.	High. The use of ZKML for automated quality verification and smart contracts for escrow allows the system to scale efficiently.

DIP network a uniquely powerful environment for building privacy-preserving applications.

1) Advanced Implementation: Zero-Knowledge Machine Learning (ZKML): For the highest level of assurance, the protocol's verifiable quality interface is best implemented using Zero-Knowledge Machine Learning (ZKML). This technology enables the verification of data properties without revealing the underlying data itself, making trustless commercial exchange of IP possible.

A Zero-Knowledge Proof (ZKP) is a cryptographic protocol in which one party (the Prover) can prove to another party (the Verifier) that a given statement is true, without conveying any information apart from the fact that the statement is indeed true **circularise˙zkp**, **identitycom2025zkp**, [45]. ZKPs are characterized by three properties:

- **Completeness:** If the statement is true, an honest Prover can always convince an honest Verifier.
- **Soundness:** If the statement is false, a dishonest Prover cannot convince an honest Verifier (except with a negligible probability).
- **Zero-Knowledge:** The Verifier learns nothing other than the validity of the statement.

ZKML extends this concept to the domain of machine learning **sharma˙zkml**, [46]–[48]. It allows a party to prove that they have correctly executed a specific ML model on a specific input to produce a specific output, all without revealing the input, the model's internal parameters (weights), or the intermediate computational steps. This is achieved by representing the ML model's operations as an arithmetic circuit and using a ZKP system, such as a zk-SNARK (Zero-Knowledge Succinct Non-Interactive Argument of Knowledge), to generate a compact, efficiently verifiable proof of the computation's integrity **nitulescu˙zksnark**, [49], [50].

Within the DIP Protocol, ZKML is the mechanism for objective and automated quality assurance. In an RFD, a Buyer can specify not just a subjective description of the data they want, but a precise, computational "quality function." This function can be an algorithm, a set of logical rules, or, most powerfully, an ML model designed to detect specific properties (e.g., a model that classifies images for content, a model that checks text for toxic language, or a statistical model that verifies a dataset's distribution and lack of bias).

A data contributor (Worker) can then take their private dataset, run it through the Buyer's public quality model, and generate a ZK proof. This proof cryptographically attests to the statement: "When my private dataset is used as input to the specified public quality model, it produces the claimed output (e.g., 'passes quality check' with a score of 99%)." The Worker can submit this proof to the escrow smart contract. The contract, and the Buyer, can efficiently verify the proof on-chain without ever gaining access to the Worker's proprietary dataset. This process makes the arbitration role of the Expert Guild objective and scalable. Instead of mediating subjective disputes, the Guild's primary function becomes the verification of cryptographic proofs, transforming a complex social problem into a straightforward computational one. This verifiable computation model replaces reputation-based trust with mathematical certainty, a paradigm shift that is essential for building a truly trustless data economy [51], [52].

For large scale mathematical proofs obviously the challenge

still persists, with ZKML industry requiring substantial computational powers to deliver on the promise. Nevertheless, there are substantial efforts already by collectives doing research such as [25], [48], [53], [54]

D. The Request-for-Data (RFD) Lifecycle: A Technical Walkthrough

The integration of these components can be illustrated by a step-by-step walkthrough of a complete transaction on the DIP Protocol:

1) **RFD Issuance:** An AI company (the Buyer) wishes to acquire a dataset of 10,000 expertly annotated medical images for training a diagnostic model. The Buyer creates an RFD smart contract with the following parameters:
   - Data Specification: "10,000 chest X-ray images, annotated for pneumonia."
   - Quality Level: Requires LATs of quality level $q \geq 0.9$.
   - Trusted Node: Specifies the address of a reputable DIP Node for data hosting and decryption.
   - ZKML Verifier: Specifies the address of a smart contract containing a pre-trained ML model that verifies the accuracy of annotations and flags images with artifacts.
   - Escrow: The Buyer deposits payment (e.g., in USDC) into the RFD contract.
2) **Data Generation and Proof Creation:** A community of radiologists (the Experts) collaborates via a CVPP instance to annotate a large pool of X-ray images. Through this meritocratic process, they earn LATs representing their contributions at various quality levels. An expert who has earned a sufficient number of LATs at $q \geq 0.9$ compiles a dataset of 10,000 images. They then use the Buyer's specified ZKML verifier model to generate a zk-SNARK proof, demonstrating that their dataset passes the quality check.
3) **Escrow Fulfillment:** The Expert submits their LATs and the generated ZK proof to the Buyer's RFD contract.
4) **Verification and Access Grant:** The RFD smart contract executes the verifier function on-chain, which confirms the validity of the ZK proof. This action is computationally inexpensive. Upon successful verification, the contract transfers ownership of the LATs to the Buyer.
5) **Decryption and Data Delivery:** The Buyer presents their ownership of the LATs to the trusted DIP Node specified in the RFD. The node verifies the on-chain ownership record and, using its MPC key share, decrypts the underlying image dataset and delivers it securely to the Buyer.
6) **Settlement:** The RFD contract, having confirmed the successful verification and token transfer, automatically releases the USDC payment to the Expert. Per the contract's terms, the transferred LATs are then sent to a burn address, permanently removing them from circulation and eliminating any risk of governance dilution for the Expert Guild.

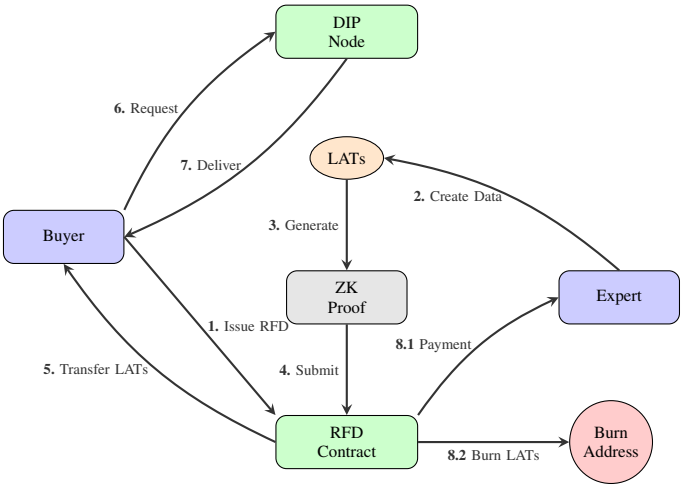

Fig. 2. The Request-for-Data (RFD) Lifecycle within the DIP Protocol, from issuance to final settlement.

VII. Applications and Ecosystem

A. Powering the Next Generation of AI Models with Verifiable Data

The primary and most immediate application of the DIP Protocol is to serve the burgeoning AI and ML industry. AI development companies can leverage DIP as a decentralized marketplace to source bespoke, high-quality datasets with unprecedented guarantees. Through the RFD process, a company can commission the creation of training data that is cryptographically verified to meet specific criteria, such as:

- **Bias Mitigation:** Using a ZKML model to prove that a dataset has a balanced demographic distribution, helping to create fairer and more equitable AI systems.
- **Content Filtering:** Ensuring a dataset is free of harmful, toxic, or copyrighted content by requiring it to pass a ZKML classifier model.
- **Provenance Verification:** Guaranteeing that a dataset is composed entirely of verifiably human-generated data, providing a crucial defense against model collapse and subliminal learning from synthetic data [54].

This moves the industry beyond relying on the reputation of data vendors to a new standard of mathematically verifiable data integrity, fundamentally de-risking the AI development lifecycle.

B. Creating Sustainable Markets for Knowledge Work

The framework established by the DIP Protocol extends far beyond datasets. It can be applied to any form of digital knowledge work where quality can be objectively or semi-objectively assessed. This transforms the "Knowledge work as a service" concept from a theoretical model into a practical reality [7]. Potential applications include:

- **Decentralized Security Audits:** A DAO could issue an RFD for a security audit of its smart contracts, specifying a ZKML verifier that runs a suite of automated analysis tools. Auditing firms could compete to find vulnerabilities and submit their findings, with payment escrowed and released upon successful verification.
- **Verifiable Academic Research:** A research foundation could fund studies by requiring researchers to submit their results along with ZK proofs demonstrating that their statistical analysis was performed correctly on a private dataset, enhancing reproducibility and trust in scientific findings.
- **Creative Content Generation:** A gaming company could commission the creation of in-game assets (e.g., character designs, lore) through a CVPP process, with the community of players and artists voting on the best submissions, ensuring the final content is aligned with player preferences.

C. The Meritocratic Flywheel: Unifying Digital Marketplaces

The principles underpinning the DIP Protocol can be generalized beyond the data economy to create a powerful new model for any digital marketplace, from ride-sharing and food delivery to freelance services. This is achieved by abstracting ACIP's "energy input" from a direct financial stake to any verifiable, value-additive contribution to the network.

Consider a ride-sharing service built as an MAO on the DIP framework. The core "energy input" (x) required to earn governance rights is no longer just a stake, but the platform's primary revenue metric: the fare. Both the driver who provides the service and the rider who pays the fare are making verifiable contributions. The protocol can be configured to mint governance tokens proportional to this revenue generated, allocating them to both the service provider and the consumer.

This creates a powerful economic flywheel:

1) **Ownership attracts providers:** Drivers are strongly incentivized to join the platform that grants them a share of ownership and a say in its governance, a benefit no traditional, centralized competitor can offer.
2) **More providers improve service:** A larger pool of drivers leads to shorter wait times and better service, attracting more riders.
3) **More users create more value:** Increased platform usage generates more revenue, which in turn mints more governance rights, reinforcing the ownership stake of all active participants.

This flywheel effect, where usage directly translates into ownership, creates a network effect that is fundamentally more defensible than the purely capital-based moats of Web2 marketplaces.

D. The End of App Monopolies: A Unified User Experience

This MAO-based model has a profound implication for the end-user: the unification of competing services into a single, seamless user experience.

Even if multiple competing teams or companies build different front-end applications for the same service (e.g., three different ride-sharing apps), they would all operate on the shared DIP back-end. Service providers (the drivers) would naturally gravitate to the application that offers them the best terms and the most governance, but their services would be available across the entire network.

This leads to a paradigm shift:

- **For Users:** Instead of needing multiple apps for the same service, a user can access all providers through a single interface. Competition shifts from building walled-garden monopolies to providing the best user interface, discovery algorithms, or customer service on top of a shared, open protocol.
- **For Businesses:** The opportunity for entrepreneurs is preserved, but the model changes from platform monopolies to what can be described as "time-duplexed" competition. Different teams can compete for market share at different times, but they cannot lock in users or providers permanently. The underlying protocol and its pool of providers and users remain a shared public good.

This creates a market that is simultaneously more competitive for businesses and simpler and more efficient for consumers, aligning incentives to prevent the extractive monopolies that characterize the current digital landscape.

E. Enhancing DAO Governance and R&D through Meritocratic Tooling

The core primitives of the DIP Protocol, particularly ACIP and CVPP, are powerful governance tools in their own right and can be adopted by other DAOs to address common challenges. Many DAOs suffer from plutocratic governance models (1-token-1-vote) and low participation rates. By integrating ACIP, a DAO can identify and empower members with demonstrated expertise and contribution, moving beyond simple token-based voting towards a more meritocratic and effective governance system [7]. For instance, a protocol DAO could use ACIP to create a "Core Developer" guild, where only members who have achieved a certain competence rank in software development can vote on technical upgrade proposals. This ensures that critical decisions are made by the most qualified participants, rather than just the wealthiest.

F. On-Chain Compliance and Verifiable Decentralization

A critical, often unacknowledged, weakness of major blockchain ecosystems is the illusion of decentralization. While protocol rules are decentralized, the physical node infrastructure is often highly centralized. A majority of nodes for networks like Ethereum and Solana are hosted in a small number of data centers within a single jurisdiction (primarily the United States). This geographic concentration creates a systemic risk, making the network vulnerable to nation-state level regulation, censorship, or physical disruption, and severely limits its appeal for global institutional use cases that require jurisdictional guarantees.

The DIP Protocol is designed to solve this problem by treating decentralization not just as a software property, but as a verifiable, physical, and jurisdictional attribute. As described in Section 4.1, the protocol's service-oriented model inherently incentivizes the creation of a globally distributed network of nodes that compete on security, performance, and jurisdictional compliance.

Building on this foundation, the protocol can be implemented as a sovereign L1 or L2 that provides a native solution for on-chain compliance. This is achieved through an additional, optional field in the protocol's transaction structure designed for **aggregated compliance attestations**. This field allows a transaction to be co-signed by a specific quorum of registered DIP Nodes.

This seemingly simple feature unlocks a powerful new paradigm for regulated institutions:

- **Built-in Compliance Primitives:** Monetary authorities and financial institutions no longer need to build private blockchains. They can simply run a registered and verified DIP Node (or a quorum of nodes) within their jurisdiction. Their signature in the attestation field becomes a verifiable, on-chain "stamp of approval" for any transaction.
- **Enforceable Smart Assets:** A smart wallet or a specific token contract (e.g., a regulated stablecoin) can be programmed to require that all its transactions include a valid signature from a designated jurisdictional node. This allows for the creation of assets that are, by design, compliant with specific regulatory regimes, without compromising the public and permissionless nature of the broader network.

This architecture provides a direct path for bridging the gap between the decentralized world and institutional finance. It moves beyond the false dichotomy of permissionless versus permissioned systems, offering a network that is publicly accessible but allows for the creation of verifiable, opt-in "compliant enclaves" for specific assets and applications.

G. A Semi-Open Source Paradigm for Digital Public Goods

The DIP Protocol enables a novel and sustainable economic model for digital public goods, formalizing the "semi-open source" paradigm [7]. The current Web3 landscape is dominated by a binary choice: either a project is fully open-source and struggles with monetization, or it is fully proprietary and centralized. DIP creates a middle ground.

Using LATs, the creators of a valuable piece of IP (e.g., a dataset, a software library, a research paper) can implement tiered and programmable access. Commercial entities wishing to use the IP for profit can be required to purchase LATs on the open market, providing a direct and sustainable revenue stream to the creators. Simultaneously, the creators can grant free or heavily discounted access to non-commercial users, such as academics, students, or hobbyists. This model can be enforced through smart contracts, creating a fair and transparent system where those who derive commercial value from public goods contribute to their upkeep. This provides a robust solution to the chronic underfunding of open-source infrastructure and contrasts sharply with the often ambiguous and legally complex licensing models currently used for NFTs and other Web3 assets **solana˙ip**, **neptune˙ip**, **blockapps˙ip**, [55].

VIII. Protocol Bootstrapping and Sustainable Emission

Sections above discussed overall implementations and various mechanisms, however while critically addressing Proof-of-Stake in Ethereum or Proof-of-Work in Bitcoin.

In order to provision long term, sustainable and inclusive, decentralized by nature protocol, the incentive flywheel itself must fundamentally represent natural asset. Since we already have discussed jurisdictional federated architecture of protocol, the ideal decentralized protocol is fully ephemeral, simply describes metadata, however in order to empower truly liquid and market driven economy for information finance, the common denominator is needed.

A core challenge for any decentralized protocol, particularly one employing a "Burn-and-Mint" tokenomic engine like LATs describe, is the initial bootstrapping phase and long-term inclusivity. How does the native asset, enter circulation sustainably, and how can new communities with existing value join over time without facing prohibitive capital barriers? Naive solutions like pre-mines or uncontrolled Initial Coin Offerings (ICOs) inherently compromise decentralization and meritocracy.

In the meantime, the very meaning of DIP protocol assets is poised to fundamentally represent the knowledge space of humanity and hence it market relationship of capital towards what philosophers and scientists of 20th century described as Noosphere [56].

The DIP Protocol achieves this through distinct pathways for network participation, a governance mechanism for recognizing established value, and a dynamic emission model tied to productive network activity and market driven incentives.

A. Pathways for Node Participation

The DIP network accommodates two primary modes for operating nodes, catering to different levels of commitment and capability:

- **Standard Nodes (Proof-of-Service):** This is the baseline, non-permissioned pathway for participating in network security and general service provision. Operators can simply acquire the native protocol asset, on the open market and stake it to become validators. Standard Nodes contribute to consensus, participate in basic computations, and earn rewards (ongoing emission and transaction fees) proportional to their stake and performance. This pathway ensures that anyone with sufficient capital can contribute to and benefit from network security.
- **Authority Nodes (Proof-of-Commitment & Issuance):** Authority Nodes act as trusted anchors within the ecosystem, often aligning with specific jurisdictions, knowledge domains, or established communities. Critically, Authority Nodes gain the exclusive right to issue Decentralized

Identifiers (DIDs) compatible with the protocol's identity framework that allows redistribution of base asset across node aligned community members with clear protocol wide visibility. This allows them to:

- **Nurture Local Economies:** Bootstrap and manage internal economies for their communities, potentially issuing a UBI-equivalent or time-based credits to account for member contributions and facilitate local exchange.
- **Onboard Users:** Act as the primary gateway for their members to interact with the broader DIP ecosystem.
- **Develop Specialized IP:** Foster the creation of domain-specific knowledge goods (LATs) within their community.

1) The Burn Commitment:: Achieving Authority Node status requires a significant, demonstrable commitment to the network and is a scarce resource similar for domain-name space. It is achievable through burning a substantial, predefined amount of base asset according to authorities issuance bonding curve. This irreversible act serves as a significant economic commitment, signaling long-term alignment and providing a capital backing the Authority's privileged role as a DID issuer. The burned base asset conceptually represents the capitalization underpinning the security and value shared within the Authority's managed community, enabling the traceable flow of value from base asset to individual contribution track of record.

2) Governance Vetting (Equivalence Mechanism):: For already established, high-value entities (e.g., reputable institutions, consortia with significant existing IP or user bases) that the network wishes to incentivize joining, an alternative pathway exists. Such entities can submit a governance proposal providing verifiable credentials and detailed data on-ramp policy, which involves LAT, data quality measures, samples and guarantees. If approved by the existing stakeholders, the protocol mints a staked Consensus Grant of directly to the entity, equivalent in commitment value to the burn requirement. This grant is non-liquid initially, ensuring immediate skin-in-the-game. This mechanism allows the network to strategically onboard major players by recognizing their existing value, effectively acquiring their integration through a capital grant rather than requiring an initial market purchase and burn.

B. Reciprocal IP Escrow: The Authority Quid Pro Quo

Regardless of the path taken (Burn or Vetting), achieving Authority Node status entails a Reciprocal IP Escrow commitment by publishing DIP policy staking with recovery mechanisms in place. The Authority must encrypt a designated, valuable portion of its own or its community's IP using a threshold scheme where majority node network consensus holds recovery key shares. These keys are strictly governed by protocol rules, usable only under verifiable conditions like node failure or malice.

This quid pro quo — Authority privileges and capital (grant/license via burn) in exchange for IP redundancy — deeply aligns incentives and establishes the network as a secure custodian for globally relevant knowledge.

Contrary to usual keys in protocols such as Zama or FHEnix [10], [16] these keys are emergency and hence can accommodate exponential networking complexity as under normal condition nodes do not go offline, but if they ever will, the recovery process may take high networking effect but acts as humanities last resort to prevent entropy and knowledge loss.

C. Rewarding Security via Stake-Weighting and Burn-Driving

The protocol ensures long-term security funding through its perpetual emission model, rewarding all staked nodes (Standard and Authority):

- **Burn-Driven Trigger:** New emission scales with the total knowledge creation usage by protocol cipher services while deflated by LAT production.
- **Decaying Subsidy:** The Minted vs Burned ratio (R_{mm}) decays programmatically over time.
- **Data quality-Weighted Distribution**: Emission is paid pro-rata to all staked, rewarding security provision based on capital commitment and network activity.

Authority Nodes, having made a significant commitment (via burn or receiving a grant), are well-positioned to earn substantial ongoing rewards through this mechanism, alongside fees from specialized services (like DID issuance or privacy computations). This ensures their high initial investment is coupled with the potential for significant long-term returns, funded sustainably by the network's productive core.

In summary, DIP offers a flexible participation model. Standard Nodes provide baseline security through capital staking. Authority Nodes make a higher commitment (burning or undergoing vetting) to gain the power to issue DIDs and foster sovereign local economies (potentially with UBI), receiving staked capital in return for IP escrow. A perpetual, burn-driven emission rewards all security providers, ensuring a sustainable, meritocratic, and economically vibrant ecosystem for the decentralized knowledge noosphere.

IX. Conclusion: A Strategic Vision for a Decentralised Knowledge Economy and Future Directions

The digital revolution's paradoxical effect—unprecedented information access coupled with the devaluation of intellectual property due to costless replication—has created a critical market failure, particularly acute in the era of data-hungry AI [7]. The traditional frameworks of patents often lead to siloed innovation, while the open-source ethos struggles with sustainable creator remuneration. This paper has presented the Decentralised Intellectual Property (DIP) Protocol not as a final specification, but as a visionary strategic roadmap outlining a foundational architecture to address these complex challenges.

We propose a novel integration of several core concepts: a meritocratic system for verifiable knowledge provenance (ACIP/CVPP) [7], [36]; a game-theoretically sound economic

engine built on Liquid Access Tokens (LATs) and Meritocratic Autonomous Organizations (MAOs); a flexible, privacy-preserving infrastructure leveraging advanced cryptography (MPC, ZKML, FHE) to solve the data disclosure problem [10], [24]; and critically, a sophisticated model for network bootstrapping and sustainable decentralization featuring Authority Nodes, Consensus Grants, Reciprocal IP Escrow, and a perpetual, burn-driven emission model [56]. This architecture aims to re-establish verifiable scarcity for digital assets, offer a potential bridge between proprietary and open-source value creation, and provide a framework for institutionally viable, geospatially decentralized infrastructure.

While DIP offers a comprehensive vision, the immediate next steps involve focused research and development to solidify its foundations. Key areas for further work include:

- **Leveraging Cryptographic Advancements:** The fields of ZKML, FHE, and MPC are advancing rapidly, with performance and scalability projected to improve significantly [24], [25]. Further research should focus on optimizing the integration of these primitives within the DIP architecture, potentially leveraging specialized protocols or hardware [10], [16]. Rather than viewing dedicated privacy solutions as competitors, they can be integrated as highly valuable, specialized nodes or services within the broader DIP network, enhancing its capabilities through composition. The pragmatic use of MPC for immediate needs, with FHE as a long-term goal or backup, remains a core strategy.
- **Formal Validation of the MAO Escrow Model:** While the ACIP/CVPP mechanisms provide a basis for meritocratic ranking and collaboration, the proposed three-party escrow system involving Buyers, Experts, and MAOs (governed by the "Dilution Dilemma") requires rigorous validation. A dedicated study, potentially employing formal game-theoretic analysis and agent-based modeling, is necessary to prove the equilibrium stability, incentive compatibility, and collusion resistance of this core economic engine under various market conditions.
- **Consensus Layer and Protocol Specification:** The successful implementation of the governance-gated onboarding (Consensus Grants), automated emission rules, and Reciprocal IP Escrow triggers necessitates a robust and efficient underlying consensus mechanism. Further investigation into high-throughput, low-latency consensus protocols, potentially including DAG-based BFT algorithms (e.g., Bullshark [57]), is warranted to ensure the base layer can support the protocol's complex state transitions and governance functions with substantial federation and parallelization. The next crucial step is the development of a detailed protocol specification ("Yellow Paper") formalizing these consensus rules, state machine logic, cryptographic interfaces, and economic parameters.
- **Reciprocal IP Escrow Security Analysis:** The specification, implementation, and formal security analysis of the threshold encryption schemes and the objective, manipulation-resistant triggers governing the network's IP recovery capabilities are paramount. Building verifiable trust in this mechanism is essential for onboarding Authority Nodes and securing high-value IP.

DIP, as outlined in this strategic document, represents more than a technical proposal; it is a hypothesis for a foundational economic and social layer suited to a future increasingly defined by intellectual contributions. By providing potential tools for fair compensation, verifiable quality, and secure, liquid exchange of knowledge assets, the DIP Protocol endeavors to lay the groundwork for a more equitable, efficient, and innovative digital ownership economy – the knowledge noosphere [56]. Successfully navigating the focused research and engineering challenges outlined above will be key to transforming this vision into a scalable and sustainable reality.

REFERENCES

[1] Helios Solutions, *The data foundation: Why data quality is crucial for ai/ml success*, n.d. [Online]. Available: https : / / www . heliossolutions . co / blog / the - data - foundation - why - data - quality - is - crucial - for - ai - ml - success/.

[2] AIMultiple, *Data quality in ai: Challenges, importance & best practices*, n.d. [Online]. Available: https : / / research.aimultiple.com/data-quality-ai/.

[3] Keymakr, *Future trends in data quality: Ai and machine learning*, Sep. 2024. [Online]. Available: https://keymakr.com/future-trends-in-data-quality-ai-and-machine-learning/.

[4] Stanford HAI, *The 2025 ai index report*, 2025. [Online]. Available: https://aiindex.stanford.edu/.

[5] McKinsey, *The state of ai: How organizations are rewiring to capture value*, n.d. [Online]. Available: https://www.mckinsey.com/capabilities/quantumblack/our-insights/the-state-of-ai-in-2023-generative-ais-breakout-year.

[6] Northwest Executive Education, *Increasing demand for artificial intelligence – 5 key factors*, May 2025.

[7] T. Pecherskis, A. Smirnovs, and A. Soboleva, *Continuous voting-proposing protocol for ordering group intents*, 2024.

[8] The Times of India, *Ai models may secretly pass on hidden behaviours, warns study*, Jul. 2025.

[9] HackerNoon, *To hit $1t tvl, ethereum must play the ace*, n.d. [Online]. Available: https://hackernoon.com/to-hit-dollar1t-tvl-ethereum-must-play-the-ace-that-is-data-sovereignty-l94z37a5.

[10] Zama, *Announcing the zama confidential blockchain protocol*, 2025. [Online]. Available: https://www.zama.ai/post/announcing-the-zama-confidential-blockchain-protocol.

[11] Wikipedia, *Full disclosure (computer security)*. [Online]. Available: https : / / en . wikipedia . org / wiki / Full_disclosure_(computer_security).

[12] C. Fracassi, M. Khoja, and F. Schär, *Decentralized crypto governance? transparency and concentration in ethereum decision-making*. 2024. [Online]. Available: https://ssrn.com/abstract=4691000.

[13] e. JÁNOS TAPOLCAI, *Slot à la carte: Centralization issues in ethereum's proof-of-stake protocol*, 2025.

[14] S. Yang and et.al, *Designing ethereum's geographical (de)centralization beyond the atlantic*, 2025.

[15] T. Forrest, *What is the environmental impact of cryptocurrency?* 2025. [Online]. Available: https://www.cigionline.org/static/documents/Emerging_Digital_Assets_Forrest.pdf.

[16] G. Zyskind, D. Zarchy, M. Leibovich, and C. Peikert, *High-throughput universally composable threshold FHE decryption*, Cryptology ePrint Archive, Paper 2025/1781, 2025. DOI: 10.1145/3719027.3744884. [Online]. Available: https://eprint.iacr.org/2025/1781.

[17] G. Zyskind, Y. Erez, T. Langer, I. Grossman, and L. Bondarevsky, "Fhe-rollups: Scaling confidential smart contracts on ethereum and beyond," ser. BSCI '24, New York, NY, USA: Association for Computing Machinery, 2025, ISBN: 9798400706387. DOI: 10.1145/3659463.3660031. [Online]. Available: https://doi.org/10.1145/3659463.3660031.

[18] *Lit protocol whitepaper*, 2024. [Online]. Available: https://github.com/LIT-Protocol/whitepaper/blob/3630c917e27b7037169678dd5e5089325d51274c/Lit%20Protocol%20Whitepaper%20(2024).pdf.

[19] J. Doerner and et al, *Threshold ecdsa in three rounds*, 2023.

[20] A. Seto, O. K. Duran, S. Amer, *et al.*, "Wiretap: Breaking server sgx via dram bus interposition," in *2025 SIGSAC Conference on Computer and Communications Security (CCS '25)*, Association for Computing Machinery, 2025. [Online]. Available: https://wiretap.fail.

[21] P. Kocher, J. Horn, A. Fogh, *et al.*, "Spectre attacks: Exploiting speculative execution," in *2019 IEEE Symposium on Security and Privacy (SP)*, 2019, pp. 1–19. DOI: 10.1109/SP.2019.00002.

[22] J. Van Bulck, M. Minkin, O. Weisse, *et al.*, "Breaking virtual memory protection and the sgx ecosystem with foreshadow," *IEEE Micro*, vol. 39, no. 3, pp. 66–74, May 2019, ISSN: 0272-1732. DOI: 10.1109/MM.2019.2910104. [Online]. Available: https://doi.org/10.1109/MM.2019.2910104.

[23] A. Cerulli and et.al, *Vetkeys: How a blockchain can keep many secrets*, 2023. [Online]. Available: https://eprint.iacr.org/2023/616.

[24] S. Chaliasos and et.al, *Analyzing and benchmarking zk-rollups*, 2024.

[25] U. Roy and et.al, *Succinct network: Prove the world's software*, 2024.

[26] P. Labs, *Filecoin: A decentralized storage network*, 2017.

[27] S. A. Williams, V. Diordiiev, and L. Berman, "Arweave: A protocol for economically sustainable information permanence," 2019. [Online]. Available: https://api.semanticscholar.org/CorpusID:234789646.

[28] S. team, *Storage and communication infrastructure for a self-sovereign digital society*, 2021.

[29] M. Sporny and et.al, *Decentralized identifiers (dids) v1.1 - core architecture, data model, and representations*. [Online]. Available: https://www.w3.org/TR/did-1.1/.

[30] *Consolidated text: Directive 2002/58/ec of the european parliament and of the council of 12 july 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (directive on privacy and electronic communications)*, 2009. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02002L0058-20091219.

[31] P. of the People's Republic of China Xi Jinping, *Personal information protection law of the people's republic of china*, 2021.

[32] *Personal data (privacy) (amendment) bill 2021*. [Online]. Available: https://www.pcpd.org.hk/english/complaints/doxxing/files/b202107161_Eng.pdf.

[33] *The cjeu judgment in the schrems ii case*, 2020. [Online]. Available: https://www.europarl.europa.eu/RegData/etudes/ATAG/2020/652073/EPRS_ATA(2020)652073_EN.pdf.

[34] Wikipedia, *Secure multi-party computation*. [Online]. Available: https://en.wikipedia.org/wiki/Secure_multi-party_computation.

[35] K. Werder, B. Ramesh, and R. (Zhang, "Establishing data provenance for responsible artificial intelligence systems," *ACM Trans. Manage. Inf. Syst.*, vol. 13, no. 2, Mar. 2022, ISSN: 2158-656X. DOI: 10.1145/3503488. [Online]. Available: https://doi.org/10.1145/3503488.

[36] T. Pechersky and A. Smirnovs, *Autonomous competence identification protocol: A dynamic ranking ladder system for blockchain applications*, 2025.

[37] T. Pecerskis and A. Smirnovs, *Continuous voting proposing protocol (cvpp) description*, 2024. [Online]. Available: https://peeramid.infura-ipfs.io/ipfs/QmVY86rL3Y5bJfLDkbeb2EUa4TfcEiZbHe186DquDmJXQJ.

[38] *Token standard*. [Online]. Available: https://ercs.ethereum.org/ERCS/erc-20.

[39] *Multi token standard*. [Online]. Available: https://ercs.ethereum.org/ERCS/erc-1155.

[40] CiteSeerX, *A game-theoretic model of third-party agents for enforcing obligations in transactions*, 2002.

[41] H. Zhang, *Hope or hype: On the viability of escrow services as trusted third parties in online auction environments*, 2004. [Online]. Available: https://doi.org/10.1287/ISRE.1040.0027.

[42] Y. Gafni and A. Yaish, *Barriers to collusion-resistant transaction fee mechanisms*, 2024. [Online]. Available: https://arxiv.org/abs/2402.08564.

[43] Frontiers in Blockchain, *Collusion resistance of voting systems in decentralized autonomous organizations*, 2024.
[44] Forbes Business Development Council, *Game theory in blockchain: The invisible hand of decentralized trust*, 2025.
[45] Wikipedia, *Zero-knowledge proof*. [Online]. Available: https://en.wikipedia.org/wiki/Zero-knowledge_proof.
[46] OSL, *How to verify on-chain machine learning algorithms using zero-knowledge*, n.d.
[47] Meegle, *Zero-knowledge proof in machine learning*, n.d.
[48] Cloud Security Alliance, *Leveraging zero-knowledge proofs in machine learning and llms: Enhancing privacy and security*, Sep. 2024.
[49] D. Kang, *Trustless machine learning inference*, Oct. 2022.
[50] S. Thakur and J. Breslin, *Efficient deep neural network verification with qap-based zksnark*, 2024. [Online]. Available: https : / / www . researchgate . net / publication / 380533825_Efficient_Deep_Neural_Network_Verification_with_QAP-based_zkSNARK.
[51] S. Simunic, D. Bernaca, and K. Lenac, "Verifiable computing applications in blockchain," vol. 9, pp. 156 729–156 745, 2021. DOI: 10.1109/ACCESS.2021.3129314.
[52] I. Chillotti, M. Joye, and P. Paillier, *Programmable bootstrapping enables efficient homomorphic inference of deep neural networks*, 2021.
[53] T. South, A. Camuto, and et.al, *Verifiable evaluations of machine learning models using zksnarks*, 2024.
[54] *Programmable bootstrapping enables efficient homomorphic inference of deep neural networks*.
[55] ICON Partners, *Strategies for web3 intellectual property management*, n.d.
[56] P. R. Samson and D. Pitt, *The biosphere and noosphere reader: Global environment, society and change*. 1999. DOI: ISBN0-415-16644-6.
[57] A. Spiegelman, N. Giridharan, A. Sonnino, and L. Kokoris-Kogias, *Bullshark: Dag bft protocols made practical*, 2022. arXiv: 2201.05677 [cs.CR]. [Online]. Available: https://arxiv.org/abs/2201.05677.