

DAO-Agent: Zero Knowledge-Verified Incentives for Decentralized Multi-Agent Coordination

Yihan Xia

xiayihan2023@email.szu.edu.cn
Shenzhen University
Shenzhen, China

Wenxin Xu

xuwenxin2022@email.szu.edu.cn
Shenzhen University
Shenzhen, China

Taotao Wang*

ttwang@szu.edu.cn
Shenzhen University
Shenzhen, China

Shengli Zhang

zsl@szu.edu.cn
Shenzhen University
Shenzhen, China

Abstract

Autonomous Large Language Model (LLM)-based multi-agent systems have emerged as a promising paradigm for facilitating cross-application and cross-organization collaborations. These autonomous agents often operate in trustless environments, where centralized coordination faces significant challenges, such as the inability to ensure transparent contribution measurement and equitable incentive distribution. While blockchain is frequently proposed as a decentralized coordination platform, it inherently introduces high on-chain computation costs and risks exposing sensitive execution information of the agents. Consequently, the core challenge lies in enabling auditable task execution and fair incentive distribution for autonomous LLM agents in trustless environments, while simultaneously preserving their strategic privacy and minimizing on-chain costs. To address this challenge, we propose DAO-Agent, a novel framework that integrates three key technical innovations: (1) an on-chain decentralized autonomous organization (DAO) governance mechanism for transparent coordination and immutable logging; (2) a ZKP mechanism approach that enables Shapley-based contribution measurement off-chain, and (3) a hybrid on-chain/off-chain architecture that verifies ZKP-validated contribution measurements on-chain with minimal computational overhead. We implement DAO-Agent and conduct end-to-end experiments using a crypto trading task as a case study. Experimental results demonstrate that DAO-Agent achieves up to 99.9% reduction in verification gas costs compared to naive on-chain alternatives, with constant-time verification complexity that remains stable as coalition size increases, thereby establishing a scalable foundation for agent coordination in decentralized environments.

Keywords

Multi-Agent Systems, Blockchain, Zero-Knowledge Proofs, Shapley Value, Decentralized Autonomous Organizations

1 Introduction

Autonomous Large Language Model (LLM)-based multi-agent systems have emerged as a promising paradigm for cross-application collaborations [15, 30]. However, these agents often operate in trustless environments where centralized coordination faces significant

challenges: ensuring transparent contribution measurement, equitable incentive distribution, and preventing strategic manipulation by rational agents.

While blockchain offers decentralized coordination through smart contracts and Decentralized Autonomous Organizations (DAOs), it introduces prohibitive on-chain computation costs and risks exposing sensitive agent execution data [8, 22]. Existing solutions face fundamental limitations: permissioned blockchains sacrifice decentralization [3], oracle-based systems reintroduce centralized trust [10, 17], and current verifiable computation approaches lack practical scalability for dynamic multi-agent scenarios [14].

This analysis reveals a fundamental dilemma between trust and efficiency as Multi-Agent Systems (MAS) evolve towards DAOs. Traditional blockchain architectures adhere to “Code is Law,” offering maximal transparency but suffering from severe computational constraints that preclude complex LLM reasoning or game-theoretic calculations (e.g., $O(n!)$ complexity). Conversely, off-chain systems possess abundant compute but lack verifiable mechanisms to ensure task quality or fair reward distribution.

To resolve this, our research goal is to establish a “Compute Off-chain, Verify On-chain” paradigm. Specifically, we aim to achieve:

- **From Unstructured to Ordered:** Bridging the gap between natural language goals and executable logic by utilizing LLMs for dynamic task planning and DAG generation.
- **Fairness through Game Theory:** Ensuring equitable incentive distribution through Shapley values, which axiomatically quantify each agent’s marginal contribution to collaborative outcomes.
- **Proof as Justice:** Replacing reliance on centralized coordinators with Zero-Knowledge Proofs (ZKP), effectively transforming “trust in intermediaries” into “trust in mathematics.”

We propose **DAO-Agent**, a novel framework integrating these principles. DAO-Agent employs a hybrid architecture where agents collaborate off-chain while ensuring verifiable contribution measurement through cryptographic proofs.

Our main contributions are three key technical innovations:

- (1) **Hybrid On-chain/Off-chain Architecture:** We design a novel architecture that separates computationally intensive Shapley value calculation from lightweight on-chain verification, achieving constant $O(1)$ verification cost regardless of agent count.

*Corresponding author.

- (2) **Fair Contribution Measurement:** We implement a contribution measurement system based on Shapley values from cooperative game theory. This mechanism provides axiomatically fair reward allocation, making honest participation a dominant strategy for rational agents.
- (3) **Verifiable “Proof as Justice” Architecture:** We construct a ZKP-based verification pipeline (using recursive proof composition: STARK proofs wrapped in Groth16) that allows the blockchain to verify off-chain game-theoretic computations with $O(1)$ cost, ensuring that the incentive distribution is mathematically proven to be fair without exposing private strategies.

We implement DAO-Agent and demonstrate its effectiveness through crypto trading experiments, showing significant cost reduction while maintaining fairness and system robustness at scale. The remainder of this paper systematically develops our solution: Section 3 formalizes the system model and trustless coordination challenges that motivate our architectural design; Section 4 presents our hybrid on-chain/off-chain framework that transforms abstract design goals into concrete cryptographic protocols; and Section 5 validates our approach through comprehensive experiments demonstrating constant-cost verification and fair incentive distribution. Note that detailed ZKP construction is discussed in Section 4.3.

2 Related Work

Our work intersects three research domains: multi-agent collaboration systems, blockchain-based coordination mechanisms, and zero-knowledge proof technologies. We position DAO-Agent relative to prior work in each area and highlight our contributions.

2.1 Multi-Agent Collaboration

Recent advances in large language models have enabled sophisticated multi-agent collaboration systems capable of autonomous task decomposition and execution. MegaAgent [30] demonstrates that LLM-based systems can scale to hundreds of agents without predefined standard operating procedures, while production systems like Anthropic’s multi-agent research platform [2] leverage multiple Claude agents for parallel search and synthesis. Building on this foundation, HiveMind [31] introduces contribution-guided prompt optimization using Shapley value analysis, demonstrating principled agent evaluation in centralized environments. Surveys [16, 27] identify coordination, scalability, and autonomous decision-making as central challenges. However, existing approaches predominantly assume centralized coordination or trusted execution environments, with none addressing fair contribution measurement or equitable incentive distribution in competitive multi-agent scenarios. DAO-Agent extends this line of work by introducing decentralized coordination through blockchain governance, employing game-theoretic Shapley value computation for axiomatically fair reward allocation, and achieving privacy-preserving contribution measurement through zero-knowledge proofs.

2.2 Blockchain-Based Coordination

Decentralized Autonomous Organizations (DAOs) have emerged as a novel governance structure enabled by blockchain technology

[7, 22]. Recent work has begun exploring DAOs for AI coordination, though primarily focusing on human-in-the-loop governance rather than fully autonomous agent collaboration [6]. However, DAO governance faces persistent challenges including the whale problem and collusion issues [26]. The Shapley value [21, 23] provides a principled approach to fair allocation, but its exponential computational complexity renders direct on-chain computation prohibitively expensive. Recent advances in DAG-based approximations [31] have significantly reduced computational overhead while maintaining theoretical guarantees. DAO-Agent builds upon these techniques and further addresses the challenge of trustless verification through a hybrid architecture that separates computation from verification, achieving constant verification cost ($\sim 27k$ gas) independent of agent count while preserving computational privacy through zero-knowledge proofs.

2.3 Verifiable Computation and Privacy

Zero-knowledge proofs (ZKPs) have evolved from theoretical cryptographic primitives to practical tools for blockchain scalability and privacy [24]. Comparative analyses [13] distinguish zkSNARKs from zkSTARKs in terms of proof size, verification cost, and trusted setup requirements. However, existing applications primarily focus on transaction validation and state transitions [1, 5, 11], with limited exploration of verifiable computation for multi-party coordination. Recent advances in multi-modal learning and semantic completion techniques [29] demonstrate sophisticated approaches to cross-modal data alignment and semantic understanding, which inform our approach to ensuring data integrity across heterogeneous agent outputs. DAO-Agent employs a STARK-to-SNARK proof aggregation pipeline to apply ZKPs to a novel domain: proving correctness of Shapley value computation over committed agent outputs, achieving $O(1)$ on-chain verification cost while supporting exponential off-chain computation complexity.

3 Problem Setup

This section establishes the system model, formalizes core challenges in trustless multi-agent coordination, and defines formal security properties that guide the architectural design in Section 4.

3.1 System and Threat Model

System Model. Consider a collaborative task T that involves n autonomous LLM agents, denoted as $\mathcal{N} = \{a_1, \dots, a_n\}$, each possessing specialized capabilities. Each agent a_i produces an output o_i during the task execution, where their outputs may be interdependent. We model this as a cooperative game $\Gamma = (\mathcal{N}, v)$, where the characteristic function $v : 2^{\mathcal{N}} \rightarrow \mathbb{R}$ maps each agent coalition $S \subseteq \mathcal{N}$ to a real value $v(S)$ quantifying the collaborative value created by that subset of agents [23]. Formally, $v(S) = f_{\text{eval}}(O_S)$ where $O_S = \{o_i : a_i \in S\}$ represents the collective outputs of coalition S , and $f_{\text{eval}}(\cdot)$ is a task-specific evaluation function. We instantiate this framework with a cryptocurrency trading task where agents collaboratively analyze market data, synthesize trading perspectives, and generate investment strategies. In this domain, $v(S)$ quantifies the trading performance achieved by coalition S based on their collective market analysis and decision-making accuracy. The marginal contribution of agent a_i to coalition S is quantified by

$v(S \cup \{a_i\}) - v(S)$. This formulation accommodates collaborative synergies through superadditivity:

$$v(\mathcal{N}) > \sum_{i \in \mathcal{N}} v(\{a_i\}) \quad (1)$$

where $v(\mathcal{N})$ denotes the grand coalition value and $v(\{a_i\})$ represents agent i 's standalone contribution. This inequality formalizes the collaborative synergy property where collective performance exceeds individual capabilities [19, 25].

Threat Model. Rational, self-interested agents may seek to maximize individual rewards through three primary attack vectors: (1) *Output Manipulation*, where an agent submits a modified output $o'_i \neq o_i$ after observing others' contributions to inflate its perceived value; (2) *Collusion*, where a coalition of agents $K \subseteq \mathcal{N}$ coordinates to unfairly redistribute rewards in their favor; and (3) *Strategic Withholding*, where an agent reduces its effort contribution e_i below an expected baseline \bar{e} while relying on others to compensate for the deficit.

Trust Model. Our model assumes a secure underlying blockchain and cryptographic primitives. Specifically: agents cannot compromise the blockchain infrastructure, as Byzantine fault tolerance ensures the probability of a successful network-level attack, $\epsilon_{\text{blockchain}}$, is a negligible function of the security parameter λ (i.e., $\epsilon_{\text{blockchain}} = \text{negl}(\lambda)$ where $\text{negl}(\lambda)$ denotes any function that decreases faster than the inverse of any polynomial in λ) [33]. All cryptographic primitives (e.g., hash functions) are assumed to be secure under standard computational assumptions. The off-chain Coordinator is trusted for *liveness* (i.e., it will eventually perform its computational tasks) but not for *correctness*; its computational integrity is enforced cryptographically through zero-knowledge proofs, which are verified on-chain.

3.2 Core Challenges

Given the threat model, we identify three fundamental challenges for trustless, fair, and scalable multi-agent collaboration:

Challenge C1 (Fair Contribution Measurement): How to quantify each agent's contribution when outputs are interdependent and collaborative value exhibits the superadditivity property (Eq. 1)? The measurement must satisfy axiomatic fairness—equal marginal contributions yield equal rewards, zero marginal contribution yields zero reward—while accounting for interaction effects.

Challenge C2 (Verifiable Output Authenticity): How to ensure inputs for contribution measurement are authentic and tamper-proof? The system must prevent retroactive output manipulation with negligible failure probability, even when agents observe others' contributions before finalizing their own.

Challenge C3 (Scalable Privacy-Preserving Verification): How to achieve verifiable fairness without prohibitive on-chain costs or revealing strategic information? Fair allocation mechanisms like Shapley values require $O(2^n)$ coalition evaluations, economically infeasible on-chain beyond $n > 6$ agents. Revealing individual outputs may expose competitive strategies.

Existing approaches face fundamental limitations: centralized coordinators lack transparency (violating C2); permissioned blockchains sacrifice decentralization; oracle-based systems reintroduce trust assumptions; direct on-chain Shapley computation violates C3's scalability requirement.

3.3 Design Goals and Formal Guarantees

We address challenges C1–C3 through three design goals, each paired with a verifiable guarantee that maps the identified risk to a concrete mitigation.

3.3.1 Goal G1: Fair and Incentive-Compatible Contribution Measurement. To resolve Challenge C1, DAO-Agent must discourage strategic deviation while preserving Shapley fairness across all coalitions.

Guarantee G1 (Incentive Compatibility and Collusion Resistance). DAO-Agent makes honest participation weakly dominant for each agent and suppresses coordinated manipulation as the population grows:

- (1) $\mathbb{E}[\text{reward}_i(\text{honest})] \geq \mathbb{E}[\text{reward}_i(\sigma'_i)]$ for every unilateral deviation σ'_i .
- (2) Coalition gain satisfies $\text{gain}_K \leq \frac{|K|}{n} \cdot v(\mathcal{N}) + O\left(\frac{|K|^2}{n}\right)$ for any colluding subset $K \subseteq \mathcal{N}$.

Here, $\text{reward}_i(\cdot)$ denotes the expected on-chain payout to agent a_i under the strategy profile supplied as an argument; σ'_i denotes any unilateral deviation from the honest policy; K labels a colluding coalition distinct from the generic coalition symbol S ; and gain_K captures the aggregate reward uplift that coalition K can realize relative to honest execution.

Shapley allocation (Section 4.2) enforces axiomatic fairness, eliminating profitable unilateral deviations when computation is faithful. Guarantee G2 (3.3.2) makes tampering detectable with overwhelming probability, so deviations yield no reward. The coalition bound follows from the Shapley efficiency axiom: total surplus remains $v(\mathcal{N})$, turning collusion into a zero-sum redistribution that vanishes as n increases.

THEOREM 3.1 (INCENTIVE COMPATIBILITY). *Under the Shapley allocation $\{\phi_i\}$ with cryptographic commitment binding (G2), honest participation is a weakly dominant strategy for each agent $a_i \in \mathcal{N}$.*

PROOF SKETCH. By the Shapley efficiency axiom, $\sum_{i \in \mathcal{N}} \phi_i = v(\mathcal{N})$. Any unilateral deviation σ'_i that attempts to increase μ_i must either (1) modify the committed output, which is detected with probability $1 - \text{negl}(\lambda)$ by G2, or (2) manipulate the Shapley computation, which is verified by the ZKP (G3). In both cases, the deviation triggers verification failure, resulting in zero payout. Thus, $\mathbb{E}[\text{reward}_i(\sigma'_i)] \leq \text{negl}(\lambda) \cdot v(\mathcal{N}) < \mathbb{E}[\phi_i]$. \square

3.3.2 Goal G2: Cryptographic Commitment for Output Authenticity. Challenge C2 demands a verifiable link between off-chain execution artifacts and on-chain settlement.

Guarantee G2 (Commitment Binding). Once an agent output o_i is committed at time t , any modification $o'_i \neq o_i$ is detected and rejected with probability at least $1 - \text{negl}(\lambda)$. For any coalition $S \subseteq \mathcal{N}$ with the associated output set $O_S = \{o_i : a_i \in S\}$ (the collection of the outputs from the agents in S) and the corresponding output hash set $\mathcal{H}_{O_S} = \{H(o_i) : o_i \in O_S\}$ (the set of the cryptographic hashes of these outputs),

$$\Pr[\text{Accept}(O'_S) \mid \exists o'_i \in O'_S : H(o'_i) \notin \mathcal{H}_{O_S}] \leq \text{negl}(\lambda). \quad (2)$$

where O'_S is the submitted output set for coalition S , and $\text{Accept}(\cdot)$ is the verification predicate that returns true if the submitted outputs are consistent with the on-chain commitment [9, 18].

This guarantee is realized through a dual-commitment scheme that provides a trustless foundation for off-chain computation. First, agent outputs (o_i) are deterministically captured and hashed; the resulting hash set is stored on IPFS to generate a content identifier (CID), which is then anchored on-chain [4, 28]. Second, the evaluated coalition value ($v(S)$) is also hashed, and its hash ($H(v(S))$) is committed directly to the blockchain. This layered cryptographic binding ensures that any tampering with either the outputs or their evaluated value is detected when the Coordinator verifies the data against the immutable on-chain anchors (as detailed in Algorithm 1). Security relies on the collision resistance of the hash function H and the immutability of the blockchain.

THEOREM 3.2 (COMMITMENT BINDING). *For any adversary \mathcal{A} running in polynomial time, the probability of producing a valid output set O'_S inconsistent with the on-chain commitment is negligible: $\Pr[\text{Accept}(O'_S) \wedge \exists o'_i : H(o'_i) \notin \mathcal{H}_{O_S}] \leq \text{negl}(\lambda)$.*

PROOF SKETCH. Assume \mathcal{A} produces $o'_i \neq o_i$ such that $H(o'_i) = H(o_i)$. This implies a hash collision, which contradicts the collision resistance of H under standard assumptions. Since the hash set \mathcal{H}_{O_S} is anchored on the immutable blockchain, any modification to O_S after commitment requires finding a collision, occurring with probability at most $\text{negl}(\lambda)$. \square

3.3.3 Goal G3: Zero-Knowledge Proofs for Scalable Verification. Challenge C3 requires verifiable computation without transferring exponential costs to the blockchain.

Guarantee G3 (Computational Scalability). Verification cost remains $O(1)$ as agent count n grows, even when contribution measurement requires $O(2^n)$ coalition evaluations. This decouples on-chain verification from off-chain computational complexity, enabling practical deployment at scale.

The guarantee is realized through a hybrid proof pipeline: the off-chain prover executes the full Shapley computation off-chain, produces a STARK proof, and recursively compresses it into a constant-size Groth16 proof for on-chain verification (Section 4.3) [12]. Consequently, the blockchain only performs a fixed-cost pairing check while inheriting soundness from the underlying proof systems.

THEOREM 3.3 (VERIFICATION SOUNDNESS). *For any computationally bounded adversary, the probability of the on-chain verifier accepting an incorrect Shapley allocation is negligible: $\Pr[f_{\text{verify}}(\pi, \text{pub}) = 1 \wedge \exists i : \mu_i \neq \phi_i] \leq \text{negl}(\lambda)$.*

PROOF SKETCH. The ZKP circuit enforces constraint (iii): $\forall i : \mu_i = \phi_i(\{v(S)\})$. By the knowledge soundness of the Groth16 proof system, any accepting proof π implies the existence of a valid witness satisfying all constraints. If $\mu_i \neq \phi_i$, constraint (iii) is violated, and no valid proof exists. The probability of forging a proof without a valid witness is bounded by the soundness error of Groth16, which is $\text{negl}(\lambda)$ under the q -PKE assumption [12]. \square

Having established the system model, identified core challenges, and formalized design goals with security guarantees, we now present the concrete architectural mechanisms that realize these properties in Section 4.

4 DAO-Agent Framework Design

To address the challenges of fair contribution measurement (C1), output authenticity (C2), and scalable verification (C3), we propose the framework of DAO-Agent. As illustrated in Figure 1, our design is a hybrid on-chain/off-chain architecture that synergizes three core technical components: (1) an on-chain DAO for governance and settlement, (2) an off-chain workflow for agent execution and contribution measurement, and (3) a zero-knowledge proof (ZKP) mechanism cryptographically link the two. This separation of concerns allows computationally intensive tasks to execute off-chain while leveraging the blockchain for what it does best: providing a trustless source of truth for verification and settlement [20, 32].

The on-chain component serves three critical functions that distinguish DAO-Agent from traditional off-chain computation approaches: (1) **Governance Anchor**: immutable task lifecycle management and agent registration via smart contract state machine, ensuring transparent coordination with cryptographic certainty; (2) **Verification Layer**: constant-cost ZKP verification (approximately 27k gas) that remains independent of agent count n , enabling scalable trust without prohibitive on-chain expenses; (3) **Settlement Engine**: cryptographically certain incentive distribution with on-chain transparency, eliminating the need for trusted third parties while preserving execution privacy. This hybrid model represents a paradigm shift from direct on-chain computation—where Shapley value calculation would require $O(2^n)$ gas—to verification-centric architecture that inherits blockchain’s trust properties while avoiding its computational limitations.

4.1 Workflow-Based Commitments and Hybrid Trust Pipeline

The DAO-Agent framework implements a comprehensive hybrid workflow that orchestrates the entire lifecycle of decentralized multi-agent collaboration through cryptographically secure coordination between off-chain execution and on-chain verification. Algorithm 1 presents the complete four-phase protocol that systematically addresses the fundamental challenges of fair contribution measurement, output authenticity, and scalable verification identified in Section 3.2.

Hybrid Protocol Overview. Algorithm 1 orchestrates the complete workflow through four distinct phases that systematically address the challenges of fair contribution measurement (C1), output authenticity (C2), and scalable verification (C3). The protocol maintains a clear separation of concerns: computationally intensive tasks execute off-chain while the blockchain provides trustless verification and settlement with cryptographic certainty.

Cryptographic Infrastructure. The algorithmic realization of our hybrid architecture relies on a carefully orchestrated set of cryptographic primitives and smart contract interfaces that bridge the gap between off-chain computation and on-chain verification. The IPFS decentralized storage system serves as our content-addressed persistence layer, where $f_{\text{IPFS}}(\cdot)$ atomically stores hash sets and returns content identifiers (CIDs) that serve as tamper-proof references to agent outputs. These CIDs are subsequently anchored on-chain through the smart contract’s commitment interface $\mathcal{E}_{\text{commit}}(\cdot)$, which generates immutable timestamps t_{block} and transaction hashes txHash that provide cryptographic binding

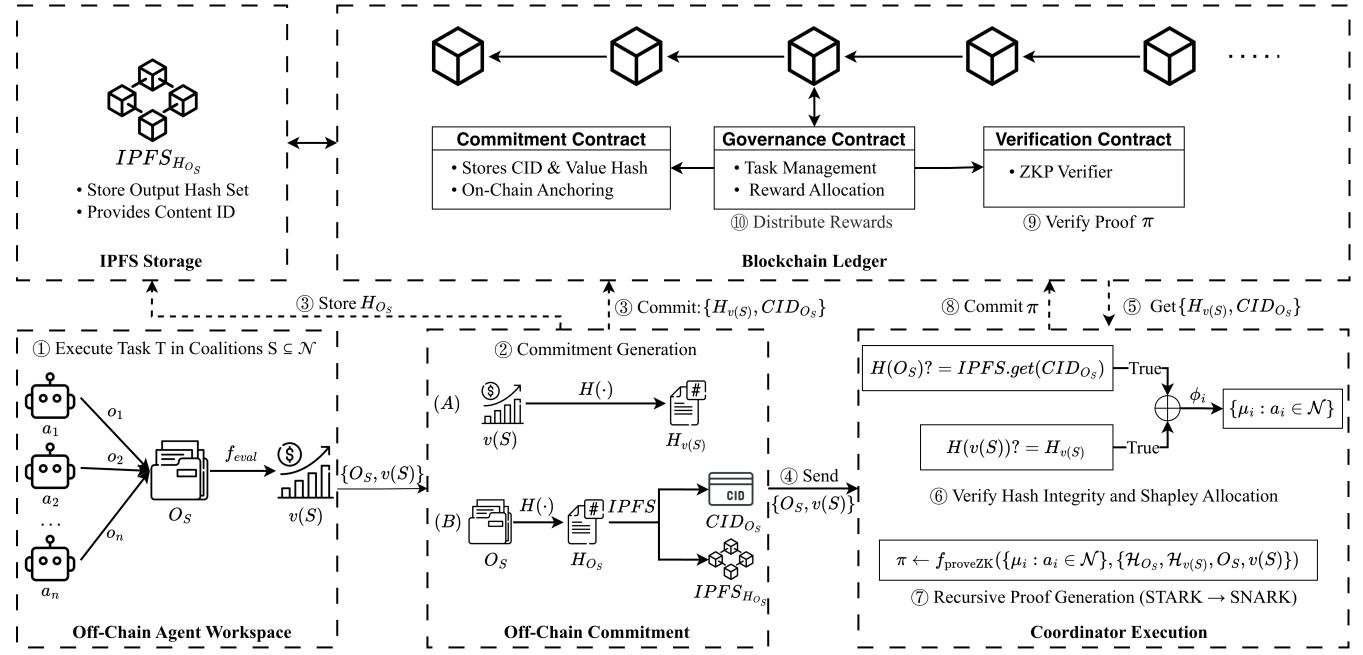


Figure 1: The DAO-Agent hybrid architecture, integrating off-chain collaborative execution with on-chain cryptographic verification. The framework bridges the trust gap through a four-phase workflow: (1) Off-Chain Execution and Multi-Tier Commitment, where agent outputs O_S and coalition values $v(S)$ are hashed ($H_{O_S}, H_{v(S)}$) and anchored on-chain via IPFS CIDs; (2) Coordinator Integrity Verification, where the Coordinator trustlessly validates hash integrity and evaluates axiomatically fair rewards using the Shapley value ϕ_i while enforcing the Efficiency Axiom ($\sum \mu_i = v(\mathcal{N})$); (3) Recursive Proof Composition, involving the generation of a STARK proof for the $O(2^n)$ Shapley computation, subsequently compressed into a constant-size Groth16 proof for blockchain compatibility; and (4) On-Chain Settlement, where the verification contract performs a single $O(1)$ pairing check to trigger automated reward distribution.

for all off-chain artifacts. The dual-retrieval mechanism $\mathcal{E}_{getCID}(S)$ and $\mathcal{E}_{getValueHash}(S)$ enables the Coordinator to trustlessly reconstruct the complete commitment state, while $IPFS.get(\cdot)$ resolves CIDs to their corresponding hash sets for integrity verification. Zero-knowledge proof generation through $f_{proveZK}(\cdot)$ transforms the exponentially complex Shapley computation into succinct cryptographic arguments, and the verification function $f_{verify}(\cdot)$ provides constant-cost on-chain validation that remains independent of the underlying computational complexity. Finally, the incentive distribution mechanism $f_{allocate}(\cdot)$ atomically transfers rewards according to the proven-fair allocation, completing the trustless coordination cycle while maintaining execution privacy and computational efficiency.

Phase 1: Subset Execution and Hash Commitment. Every possible agent coalition $S \subseteq \mathcal{N}$ executes the collaborative task off-chain, producing outputs that are immediately cryptographically secured. This phase implements the Commitment Binding guarantee (G2) through a dual-commitment scheme that prevents output manipulation without relying on agent self-reporting.

Phase 2: Coordinator Verification and Shapley Computation. The Coordinator acts as a trustless computation node that

verifies the integrity of all committed data and computes axiomatically fair Shapley value allocations. This phase realizes the Incentive Compatibility guarantee (G1) by ensuring that contribution measurements are both cryptographically verifiable and game-theoretically sound.

Phase 3: Zero-Knowledge Proof Generation. Zero-knowledge proofs are generated to attest to the correctness of the entire off-chain computation without revealing sensitive execution details. This phase provides the Computational Scalability guarantee (G3) by converting exponential off-chain computation into constant-size cryptographic proofs.

Phase 4: On-Chain Verification and Settlement. The smart contract performs efficient on-chain verification and atomically distributes incentives according to the proven-fair allocation. This final phase ensures that all previous computations are cryptographically validated before any value transfer occurs.

The framework's operation is orchestrated by the smart contract \mathcal{E} , which implements a hybrid trust model combining off-chain computational efficiency with on-chain verification integrity. On-chain verification consumes approximately 27k gas regardless of agent count n , achieving constant $O(1)$ complexity through succinct non-interactive argument verification. This represents a paradigm shift from traditional on-chain computation—where exact Shapley

Algorithm 1: DAO-Agent Hybrid Workflow

```

Input: Task  $T$ , Agent Set  $\mathcal{N} = \{a_1, \dots, a_n\}$ , Coordinator  $C$ 
// Phase 1: Subset Execution and Hash Commitment
1 foreach coalition  $S \subseteq \mathcal{N}$  do
2   Agents in  $S$  execute  $T$  in workflow environment;
3    $O_S \leftarrow \{o_i : a_i \in S\}$  // Coalition  $S$  output set
4    $\mathcal{H}_{O_S} \leftarrow \{H(o_i) : o_i \in O_S\}$  // Hash set of outputs
5    $CID_{O_S} \leftarrow f_{IPFS}(\mathcal{H}_{O_S})$ 
      $E_{commit}(CID_{O_S}) \rightarrow (t_{block}, txHash)$ 
      $v(S) \leftarrow f_{eval}(O_S)$  // Coalition value evaluation
6    $\mathcal{H}_{v(S)} \leftarrow H(v(S))$  // Hash of coalition value
7    $\mathcal{E}_{commitValue}(\mathcal{H}_{v(S)}) \rightarrow (t'_{block}, txHash')$ 

// Phase 2: Coordinator Verification and Shapley Computation
8 foreach received  $O_S$  do
9    $CID_{O_S} \leftarrow \mathcal{E}_{getCID}(S)$  assert
      $\{H(o_i) : o_i \in O_S\} = IPFS.get(CID_{O_S});$ 
10 foreach received  $v(S)$  do
11    $\mathcal{H}_{v(S)} \leftarrow \mathcal{E}_{getValueHash}(S)$  assert  $H(v(S)) = \mathcal{H}_{v(S)}$ 
12    $\{\mu_i : a_i \in \mathcal{N}\} \leftarrow \frac{1}{n} \sum_{S \subseteq \mathcal{N} \setminus \{a_i\}} \binom{n-1}{|S|}^{-1} (v(S \cup \{a_i\}) - v(S))$ 
     // Shapley allocation
13 // Phase 3: Zero-Knowledge Proof Generation
14  $\pi \leftarrow f_{proveZK}(\{\mu_i : a_i \in \mathcal{N}\}, \{\mathcal{H}_{O_S}, \mathcal{H}_{v(S)}, O_S, v(S)\});$ 
15 // Phase 4: On-Chain Verification and Settlement
16  $pub\_inputs \leftarrow (\{\mu_i : a_i \in \mathcal{N}\}, v(\mathcal{N}), \{\mathcal{H}_{O_S} : S \subseteq \mathcal{N}\}, \{\mathcal{H}_{v(S)} : S \subseteq \mathcal{N}\});$ 
17 if  $f_{verify}(\pi, pub\_inputs, \mathcal{E}) = true$  then
18    $f_{allocate}(\{\mu_i : a_i \in \mathcal{N}\}) \rightarrow \mathcal{E};$ 
19   return  $\{\mu_i : a_i \in \mathcal{N}\};$ 
20 return abort;

```

value calculation would require exponential $O(2^n)$ gas consumption—to a verification-centric approach that inherits blockchain's trust properties while avoiding its computational limitations. Our hybrid architecture reduces on-chain verification complexity from exponential to constant, enabling practical deployment for large-scale multi-agent coordination while maintaining cryptographic certainty.

From Protocol to Mechanisms. While Algorithm 1 presents the complete workflow coordination, three fundamental technical mechanisms enable this hybrid architecture to achieve its security and efficiency guarantees. First, the protocol requires **fair contribution measurement** that can withstand strategic manipulation by rational agents—this necessitates a rigorous game-theoretic foundation that we develop in Section 4.2. Second, the Coordinator must generate **cryptographic proofs** that convincingly demonstrate computation integrity without revealing sensitive execution data—this demands sophisticated zero-knowledge proof integration detailed in Section 4.3. Third, the entire system must maintain **computational scalability** as the number of agents grows, requiring

careful architectural decisions that separate expensive off-chain computation from lightweight on-chain verification.

The following sections dissect these three critical mechanisms. Section 4.2 establishes the game-theoretic foundation by demonstrating how Shapley values provide axiomatically fair contribution measurement that makes honest participation a dominant strategy for agents. Section 4.3 then shows how zero-knowledge proofs cryptographically link the off-chain Shapley computation to on-chain verification, ensuring that fairness guarantees are preserved while maintaining execution privacy. Together, these mechanisms transform the high-level workflow presented above into a concrete, implementable system that resolves the tension between decentralization, privacy, and computational efficiency in multi-agent coordination.

4.2 Shapley-Based Contribution Measurement

To achieve fair contribution measurement (C1) and realize the Incentive Compatibility guarantee (G1), we ground our reward mechanism in the Shapley value from cooperative game theory. The Shapley value, $\phi_i(v)$, provides an axiomatically fair allocation by quantifying each agent a_i 's contribution as its average marginal value across all possible coalition permutations.

Formally, for each agent $a_i \in \mathcal{N}$, the Shapley value is:

$$\phi_i(\{v(S) : S \subseteq \mathcal{N}\}) = \frac{1}{n} \sum_{S \subseteq \mathcal{N} \setminus \{a_i\}} \binom{n-1}{|S|}^{-1} (v(S \cup \{a_i\}) - v(S)) \quad (3)$$

The weight term ensures that all agent joining orders are equally likely, eliminating order bias. This method yields a unique allocation satisfying four axioms: **Efficiency** ($\sum_{i \in \mathcal{N}} \phi_i = v(\mathcal{N})$), **Symmetry**, **Dummy**, and **Additivity**. The uniqueness of this allocation provides an indisputable foundation for fair rewards, making honest participation a dominant strategy when combined with the cryptographic guarantees that follow. The efficiency axiom is particularly central to our design, serving as: (1) a theoretical guarantee of complete value distribution, (2) a computational constraint verified within the ZKP, and (3) a final on-chain check using public inputs. To formalize this verification, we distinguish between the true Shapley value, defined by the function ϕ_i , and the concrete allocation vector computed by the Coordinator, which we denote as $\{\mu_i\}$. The core of the ZKP is to prove that the submitted $\{\mu_i\}$ correctly corresponds to the output of the ϕ_i function for all agents (i.e., that $\mu_i = \phi_i$).

Within our hybrid architecture, Shapley computation is performed off-chain by the Coordinator, leveraging the computational efficiency of traditional computing environments while maintaining verifiability through on-chain commitments. The on-chain smart contract \mathcal{E} does not perform the expensive $O(2^n)$ coalition evaluations directly; instead, it verifies that the off-chain computation was performed correctly on the committed data through zero-knowledge proof verification. This separation enables the system to achieve both computational scalability and cryptographic verifiability without compromising either property.

4.3 Zero-Knowledge Proof Integration

To address scalable, privacy-preserving verification (C3) and provide the Computational Scalability guarantee (G3), DAO-Agent

Algorithm 2: ZKP Construction: Witness Generation and Constraint Enforcement

Input: Coalition Outputs $\{O_S\}$, Coalition Values $\{v(S)\}$, Shapley Allocation $\{\mu_i\}$, Commitments $\{\mathcal{H}_{O_S}, \mathcal{H}_{v(S)}\}$

Output: Proof π and public inputs

// Phase I: Off-Chain Witness Computation

// Generates the execution trace \mathcal{W} for the arithmetic circuit

```

1  $\mathcal{W} \leftarrow \text{InitTrace}();$ 
2 foreach  $S \subseteq \mathcal{N}$  do
3    $\mathcal{W}.\text{AppendInput}(O_S, v(S));$ 
4 foreach agent  $a_i \in \mathcal{N}$  do
5    $\phi_i \leftarrow \text{ComputeShapley}(i, \{v(S)\})$  // Execute Eq. 3
6    $\mathcal{W}.\text{RecordComputation}(i, \phi_i);$ 

// Phase II: In-Circuit Constraint Enforcement
// Arithmetic constraints verified within the ZK circuit

7 Circuit Logic:
8   // C1: Input Consistency Check
9   foreach  $S \subseteq \mathcal{N}$  do
10    constrain
11      PoseidonHash( $\mathcal{W}.O_S$ )  $\equiv$  public_input. $\mathcal{H}_{O_S}$ ;
12    constrain
13      PoseidonHash( $\mathcal{W}.v(S)$ )  $\equiv$  public_input. $\mathcal{H}_{v(S)}$ ;
14   // C2: Shapley Arithmetization
15   foreach agent  $a_i \in \mathcal{N}$  do
16     // Polynomial constraints for Eq. 3
17     sum  $\leftarrow 0;$ 
18     foreach  $S \subseteq \mathcal{N} \setminus \{a_i\}$  do
19       coeff  $\leftarrow \text{Lookup}\left(\binom{n-1}{|S|}^{-1}\right);$ 
20       marginal  $\leftarrow \mathcal{W}.o(S \cup \{a_i\}) - \mathcal{W}.o(S);$ 
21       sum  $\leftarrow sum + (coeff \times marginal);$ 
22     constrain  $\mathcal{W}.\mu_i \equiv sum \times n^{-1};$ 
23   // C3: Efficiency Axiom Check
24   constrain  $\sum \mathcal{W}.\mu_i \equiv \mathcal{W}.v(\mathcal{N});$ 

// Phase III: Recursive Proof Generation
25  $\pi \leftarrow \text{STARK.Prove}(\text{Circuit}, \mathcal{W}, \text{public\_inputs});$ 
26 return ( $\pi, \text{public\_inputs}$ );

```

integrates zero-knowledge proofs. This allows the off-chain Coordinator to prove the correctness of the computationally expensive Shapley value calculation without revealing any private data (e.g., agent strategies embedded in outputs) and without imposing exponential costs on the blockchain. The on-chain verification component consumes approximately 27k gas regardless of agent count, achieving the $O(1)$ complexity required for practical deployment at scale.

4.3.1 Proof of Correct Computation. The Coordinator uses a proving function of ZKP to generate a proof π attesting to the integrity

of the entire off-chain collaboration process. The proving function of ZKP takes public input and private witness as the inputs and produces a proof for the computation correctness. The verification function of ZKP requires only the proof and public inputs to confirm the correctness of the computation, achieving this with significantly lower complexity compared to re-executing the entire computation process.

Specifically, the ZKP protocol is defined over a relation \mathcal{R} comprising a private witness Ω_{private} and public input Ω_{public} :

$$\begin{cases} \Omega_{\text{private}} = (\{O_S\}_{S \subseteq \mathcal{N}}, \{v(S)\}_{S \subseteq \mathcal{N}}), \\ \Omega_{\text{public}} = (\{\mu_i\}, v(\mathcal{N}), \{\mathcal{H}_{O_S}\}, \{\mathcal{H}_{v(S)}\}) \end{cases} \quad (4)$$

Here, Ω_{private} encapsulates the complete execution trace, including all coalition outputs O_S and their corresponding evaluations $v(S)$. The public input Ω_{public} serves as the on-chain anchor, containing the proposed Shapley allocation $\{\mu_i\}$, the grand coalition value $v(\mathcal{N})$, and the set of committed cryptographic hashes. The validity of the proof π is contingent upon satisfying the following arithmetic constraints:

$$\begin{cases} \text{(i) } \forall S \subseteq \mathcal{N} : \{H(o_i) : o_i \in O_S\} = \mathcal{H}_{O_S}, \\ \text{(ii) } \forall S \subseteq \mathcal{N} : H(v(S)) = \mathcal{H}_{v(S)}, \\ \text{(iii) } \forall i : \mu_i = \phi_i(\{v(S) : S \subseteq \mathcal{N}\}), \\ \text{(iv) } \sum_{i \in \mathcal{N}} \mu_i = v(\mathcal{N}) \end{cases} \quad (5)$$

These constraints enforce the system's core integrity properties:

- (i) **Input Consistency:** guarantees that the private witness values correspond exactly to the immutable on-chain commitments, preventing retroactive data manipulation.
- (ii) **Value Authenticity:** ensures the coalition evaluations used in the circuit match the committed values.
- (iii) **Computational Correctness (Shapley Arithmetization):** validates that the allocation $\{\mu_i\}$ is derived via the exact Shapley formula (Eq. (3)). We arithmetize the iterative summation and combinatorial weighting logic into polynomial constraints (see Algorithm 2, Lines 13-20), thereby proving that the $O(2^n)$ factorials and marginal contributions were computed correctly.
- (iv) **Conservation of Value:** enforces the Efficiency Axiom, ensuring the total distributed reward strictly equals the generated value.

These cryptographic assertions form the basis of our "Code is Law" implementation, distinguishing DAO-Agent from systems relying on optimistic assumptions or centralized verifiers. Algorithm 2 delineates the formal separation between off-chain trace generation and in-circuit constraint enforcement.

4.3.2 Recursive Proof Composition and On-Chain Verification. To reconcile the computational complexity of Shapley value derivation with the strict gas limits of blockchain execution, we employ a recursive proof composition strategy. The pipeline initiates with the generation of STARK proofs (Scalable Transparent Arguments of Knowledge), which provide the necessary computational capacity for checking $O(2^n)$ coalition values without trusted setup. However, the resulting proofs are typically large (tens of kilobytes), rendering direct on-chain verification economically infeasible.

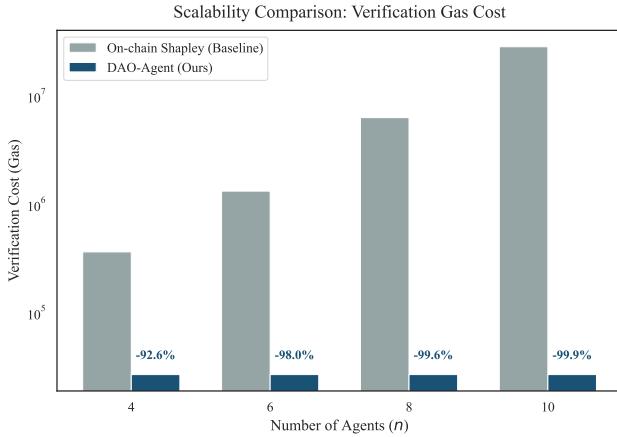


Figure 2: Scalability Comparison: Verification Gas Cost (Log Scale). The bar chart demonstrates a massive cost reduction of up to 99.9% for larger agent coalition ($n = 10$), contrasting the exponential growth of the baseline with the constant cost of our hybrid approach.

To address this, we utilize a proof-carrying data (PCD) approach where the STARK proof π_{STARK} is recursively verified within a secondary circuit. This circuit generates a succinct Groth16 proof π_{SNARK} , compressing the verification complexity to constant size. This STARK-to-SNARK recursion leverages the transparency and scalability of STARKs for the heavy arithmetic lifting (Shapley computation) while utilizing the compactness of pairing-based SNARKS for final on-chain settlement. Consequently, the smart contract performs a single $O(1)$ pairing check ($\approx 27\text{k}$ gas), decoupling the on-chain verification cost from the exponential off-chain workload.

5 Experimental Evaluation

5.1 Experimental Setup

We implement a multi-agent cryptocurrency trading system with a fixed architecture (2 data analysis agents, 1 decision-making agent, and a variable number of market perspective agents, where $x \in \{1, 3, 5, 7\}$) deployed on an Ethereum testnet. For each coalition $S \subseteq \mathcal{N}$, we quantify its value $v(S)$ using Sharpe ratio-based trading performance metrics over ETH/USDT historical data from 2022–2024. The experiments evaluate agent sets of size $n \in \{4, 6, 8, 10\}$, requiring 2^n coalition evaluations each.

Our performance assessment is structured into two key areas: the off-chain computational overhead required for proof generation and the on-chain resource consumption for verification. We evaluate DAO-Agent against an *On-chain Shapley* baseline, which performs all computations directly in a smart contract. The coalition value function $v(S)$ is computed using Sharpe ratio-based trading performance metrics, validated against historical ground-truth data. The results validate our hybrid model’s ability to achieve constant-cost on-chain scalability while managing exponential complexity off-chain.

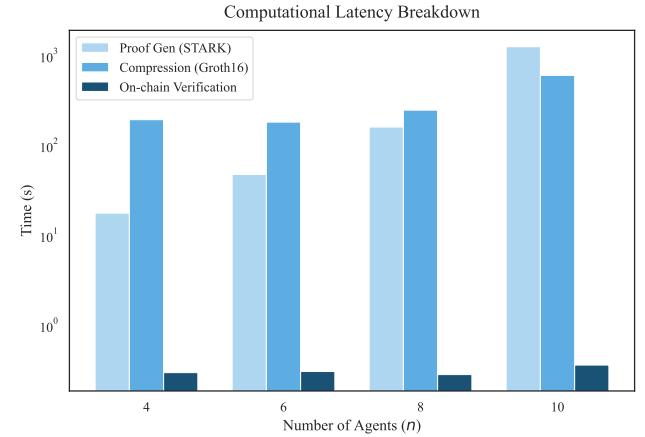


Figure 3: Computational Latency Breakdown (Log Scale). The grouped bar chart reveals the trade-off: while off-chain proof generation (STARK) scales exponentially, the on-chain verification time remains negligible and constant (< 0.4s).

5.2 Off-Chain Computational Performance

The primary computational workload of DAO-Agent resides in the off-chain proof generation pipeline (Phase 3). As detailed in Table 1 and Figure 3, the STARK proof generation time is the main bottleneck, scaling exponentially with the number of agents. This duration increases from 21.22 seconds for 4 agents to 425.60 seconds for 10 agents, reflecting the $O(2^n)$ complexity of the underlying Shapley value computation.

In contrast, the subsequent proof conversion to Groth16 remains highly efficient and does not exhibit exponential growth. Furthermore, the final proof size increases only marginally, from 1,417 bytes to 1,802 bytes, ensuring that the cryptographic artifacts remain compact and manageable. These results pinpoint the STARK generation as the key scalability constraint of the off-chain process.

Table 1: ZKP Performance: Proof Generation and Verification Metrics

Agents	STARK (s)	Groth16 (s)	Size (B)	Verify (s)
4	21.22	233.41	1,417	0.358
6	56.46	217.19	1,545	0.368
8	201.36	310.27	1,673	0.354
10	425.60	298.15	1,802	0.362

5.3 On-Chain Cost and Scalability

The central advantage of the DAO-Agent framework is its ability to achieve constant-cost on-chain scalability. Figure 2 illustrates the dramatic difference between our hybrid approach and the on-chain baseline. While the baseline’s gas cost explodes exponentially, DAO-Agent’s verification cost remains flat at approximately 27k gas, regardless of the number of agents.

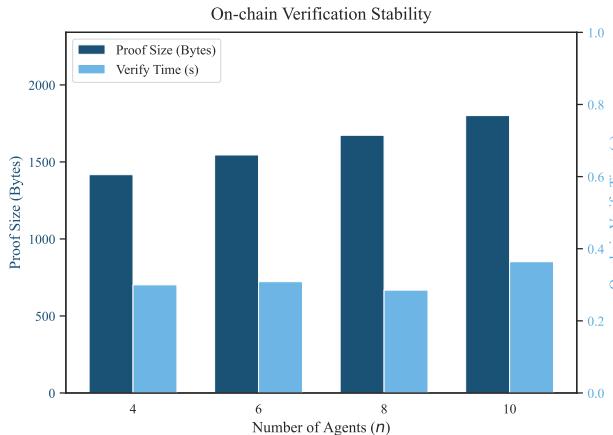


Figure 4: On-chain Verification Stability. The dual-axis bar chart illustrates that both Proof Size (Left Axis) and Verification Time (Right Axis) remain stable and low despite the increasing complexity of the multi-agent task.

As shown in Table 2, this translates to a gas reduction of 99.9% for a 10-agent system (27k vs. 28.6M gas). This efficiency transforms an intractable $O(2^n)$ on-chain problem into a lightweight $O(1)$ verification. The on-chain verification itself is consistently fast, taking approximately 0.36 seconds (see Table 1). This low, predictable gas cost, comparable to a standard ERC-20 transfer, confirms that DAO-Agent is economically viable for practical deployment at scale.

Table 2: Gas Cost Comparison: On-chain vs. DAO-Agent Verification

Agents	On-chain Gas	DAO-Agent Gas	Reduction
4	367K	27K	92.6%
6	1.33M	27K	98.0%
8	6.35M	27K	99.6%
10	28.6M	27K	99.9%

6 Conclusion

This paper addressed the core challenge of achieving fair, scalable, and privacy-preserving coordination in decentralized multi-agent systems, which is hindered by prohibitive on-chain computation costs and the lack of verifiable contribution measurement. We introduced DAO-Agent, a novel hybrid on-chain/off-chain framework that leverages the blockchain as a trust anchor while offloading computationally intensive tasks. Our approach cryptographically links Shapley value-based contribution measurements to a constant-cost on-chain verification mechanism using zero-knowledge proofs.

Our experimental evaluation demonstrates the practicality and efficiency of DAO-Agent. By transforming the exponential $O(2^n)$ on-chain complexity into a constant $O(1)$ verification process, our method reduces gas costs by up to 99.9% for 10 agents compared to a purely on-chain implementation. This breakthrough makes fair,

trustless multi-agent coordination economically viable in decentralized environments.

While our experiments validate efficiency for up to 10 agents, the architecture is designed for extensibility. The off-chain proof generation complexity ($O(2^n)$ for exact Shapley) can be addressed through approximation techniques such as Monte Carlo Shapley estimation, enabling larger-scale deployments with minimal precision trade-offs. Furthermore, the system's security model, which currently assumes coordinator liveness, could be strengthened by introducing redundant coordinators or decentralized challenge-response mechanisms. The security framework relies on standard cryptographic assumptions and is adaptable to post-quantum hash functions for future-proofing.

In summary, DAO-Agent provides a robust and efficient blueprint for building trustless, incentive-compatible multi-agent systems. By offering substantial cost savings for frequent coordination tasks, it paves the way for more sophisticated and secure decentralized collaborations. Future work could further enhance performance by exploring layer-2 deployment and proof batching techniques.

References

- [1] M.J. Amiri, D. Basu, M. Canini, L. E. S. Rosa, and S. Schmid. 2024. The Bedrock of Byzantine Fault Tolerance: A Unified Framework. In *Proceedings of the 21st USENIX Symposium on Networked Systems Design and Implementation (NSDI 2024)*. <https://www.usenix.org/system/files/nsdi24-amiri.pdf>
- [2] Anthropic. 2025. How we built our multi-agent research system. <https://www.anthropic.com/index/how-we-built-our-multi-agent-research-system> Engineering Blog.
- [3] Yannis Bakos and Hanna Halaburda. 2022. Permissioned vs Permissionless Blockchain Platforms: Tradeoffs in Trust and Performance. *NYU Stern School of Business Working Paper* (March 2022).
- [4] Juan Benet. 2014. *IPFS - Content Addressed, Versioned, P2P File System*. Technical Report. InterPlanetary File System. Original IPFS white paper.
- [5] Tariq Bontekoe, Dimka Karastoyanova, and Fatih Turkmen. 2024. Verifiable Privacy-Preserving Computing. <https://arxiv.org/abs/2309.08248> arXiv preprint arXiv:2309.08248.
- [6] Agostino Capponi, Mohamed Amine Larachi, Qingqing Jia, Jayakrishnan Sethuraman, Hongkai Yan, and Jingyue Zhu. 2025. Decentralized Autonomous Organizations for Artificial Intelligence. <https://arxiv.org/abs/2510.21117> arXiv preprint arXiv:2510.21117.
- [7] André Guskow Cardoso. 2023. Decentralized Autonomous Organizations - DAOs: the Convergence of Technology, Law, Governance, and Behavioral Economics. *MIT Computational Law Report* (November 2023). <https://law.mit.edu/pub/decentralizedautonomousorganizations>
- [8] Cyril Chambefort and Magali Chaudey. 2024. Blockchain, tokens, smart contracts, and “decentralized autonomous organizations”: A governance theory perspective. *European Management Review* 44, 4 (August 2024), 1–15. doi:10.1111/emre.12677
- [9] Alex Coventry, Siam Hussain, Dahlia Malkhi, Alexandru Topiceanu, Xiao Wang, Chenkai Weng, and Fan Zhang. 2023. Commit-and-Prove ZKs. <https://blog.chain.link/commit-and-prove-zks/> Chainlink Labs Research Blog.
- [10] Chanelle Duley, Leonardo Gambacorta, Rodney Garratt, and Priscilla Koo Wilkens. 2023. The oracle problem and the future of DeFi. *BIS Bulletin* 76 (September 2023).
- [11] Ethereum.org. 2025. Zero-knowledge proofs. Official Documentation.
- [12] Jens Groth. 2016. On the Size of Pairing-based Non-interactive Arguments?. In *Advances in Cryptology - EUROCRYPT 2016*. Springer Berlin Heidelberg, 216–243. doi:10.1007/978-3-662-49896-5_8
- [13] Hacken. 2023. Comparing ZK-SNARKs & ZK-STARKs: Key Distinctions in Blockchain Privacy Protocols. <https://hacken.io/discover/zk-snark-vs-zk-stark/>
- [14] Xiang Huo, Hao Huang, Katherine R. Davis, H. Vincent Poor, and Mingxi Liu. 2024. A Review of Scalable and Privacy-Preserving Multi-Agent Frameworks for Distributed Energy Resource Control. *arXiv preprint arXiv:2409.14499* (September 2024).
- [15] Cristian Jimenez-Romero, Alper Yegenoglu, and Christian Blum. 2025. Multi-agent systems powered by large language models: applications in swarm intelligence. *Frontiers in Artificial Intelligence* 8 (May 2025), 1593017. doi:10.3389/frai.2025.1593017
- [16] Adam Kostka and Jarosław A. Chudziak. 2025. Towards Cognitive Synergy in LLM-Based Multi-Agent Systems: Integrating Theory of Mind and Critical Evaluation. <https://arxiv.org/abs/2507.21969> arXiv preprint arXiv:2507.21969.

- [17] Imran Makhdoom, Mehran Abolhasan, Justin Lipman, Wei Ni, and Lei Zhang. 2023. From trust to truth: Advancements in mitigating the Blockchain Oracle problem. *Journal of Network and Computer Applications* 217 (June 2023), 103672. doi:10.1016/j.jnca.2023.103672
- [18] Roxandra F. Olimid. 2025. Commitment Schemes for Multi-Party Computation. <https://arxiv.org/abs/2506.10721>
- [19] Bezalel Peleg and Peter Sudhölter. 2007. *Introduction to the Theory of Cooperative Games*. Theory and Decision Library C, Vol. 34. Springer Science & Business Media, Berlin, Heidelberg. doi:10.1007/978-3-540-77845-1
- [20] Minfeng Qi, Tianqing Zhu, Lefeng Zhang, Ningran Li, and Wanlei Zhou. 2025. Towards Transparent and Incentive-Compatible Collaboration in Decentralized LLM Multi-Agent Systems: A Blockchain-Driven Approach. <https://arxiv.org/abs/2509.16736> arXiv preprint arXiv:2509.16736
- [21] Lei Qin, Yingqiu Zhu, Shaonan Liu, Xingjian Zhang, and Yining Zhao. 2025. The Shapley Value in Data Science: Advances in Computation, Extensions, and Applications. *Mathematics* 13, 10 (May 2025), 1581. doi:10.3390/math13101581
- [22] Rui Qin, Wenwen Ding, Juanjuan Li, Sangtian Guan, Ge Wang, Yuhai Ren, and Zhiyou Qu. 2023. Web3-Based Decentralized Autonomous Organizations and Operations: Architectures, Models, and Mechanisms. *IEEE Transactions on Systems, Man, and Cybernetics: Systems* 53, 4 (April 2023), 2073–2084. doi:10.1109/TSMC.2022.3228530
- [23] Lloyd S. Shapley. 1953. *A Value for n-Person Games*. Vol. 2. Princeton University Press, Princeton, NJ. 307–317 pages.
- [24] Nojan Sheybani, Anees Ahmed, Michel A. Kinsky, and Farinaz Koushanfar. 2025. Zero-Knowledge Proof Frameworks: A Survey. *arXiv preprint arXiv:2502.07063* (February 2025).
- [25] Jeroen Suijs, Peter Borm, Anja De Waegenaere, and Stef Tijs. 1999. Stochastic Cooperative Games: Superadditivity, Convexity, and Certainty Equivalents. *Games and Economic Behavior* 27, 2 (1999), 331–345. doi:10.1006/game.1998.0656
- [26] Shunya Tamai and Shoji Kasahara. 2024. DAO voting mechanism resistant to whale and collusion problems. *Frontiers in Blockchain* 7 (June 2024). doi:10.3389/fbloc.2024.1405516
- [27] Khanh-Tung Tran, Dung Dao, Minh-Duong Nguyen, Quoc-Viet Pham, Barry O'Sullivan, and Hoang D. Nguyen. 2025. Multi-Agent Collaboration Mechanisms: A Survey of LLMs. *arXiv preprint arXiv:2501.06322* (2025). <https://arxiv.org/abs/2501.06322>
- [28] Dennis Trautwein, Aravindh Raman, Gareth Tyson, Ignacio Castro, Will Scott, Moritz Schubotz, Bela Gipp, and Yiannis Psarlas. 2022. Design and Evaluation of IPFS: A Storage Layer for the Decentralized Web. In *Proceedings of the ACM SIGCOMM 2022 Conference*. 1459–1471. doi:10.1145/3544216.3544232
- [29] Rong-Cheng Tu, Yatai Ji, Jie Jiang, Weijie Kong, Chengfei Cai, Wenzhe Zhao, Hongfa Wang, Yujia Yang, and Wei Liu. 2025. Global and local semantic completion learning for vision-language pre-training. *IEEE Transactions on Pattern Analysis and Machine Intelligence* 47 (2025), 11065–11079. doi:10.1109/TPAMI.2025.3596394
- [30] Qian Wang, Tianyu Wang, Zeyu Tang, Qi Li, Nuo Chen, Jing Liang, and Bingsheng He. 2025. MegaAgent: A Large-Scale Autonomous LLM-based Multi-Agent System Without Predefined SOPs. In *Findings of the Association for Computational Linguistics: ACL 2025*. Association for Computational Linguistics, Vienna, Austria, 4998–5036. doi:10.18653/v1/2025.findings-acl.259
- [31] Yihan Xia, Taotao Wang, Shengli Zhang, Zhangyuhua Weng, Bin Cao, and Soung Chang Liew. 2026. HiveMind: Contribution-Guided Online Prompt Optimization of LLM Multi-Agent Systems. In *Proceedings of the AAAI Conference on Artificial Intelligence (AAAI 2026)*. <https://arxiv.org/abs/2512.06432> To appear.
- [32] Huawei Yang. 2024. Swarm Contract: A Multi-Sovereign Agent Consensus Mechanism. <https://arxiv.org/abs/2412.19256> arXiv preprint arXiv:2412.19256.
- [33] Weiyu Zhong, Ce Yang, Wei Liang, Jiahong Cai, Lin Chen, and Jing Liao. 2023. Byzantine Fault-Tolerant Consensus Algorithms: A Survey. *Electronics* 12, 18 (2023), 3801. doi:10.3390/electronics12183801