future internet

MDPI

Article

Leveraging the DAO for Edge-to-Cloud Data Sharing and Availability

Adnan Imeri [1,*], Uwe Roth [1], Michail Alexandros Kourtis [2], Andreas Oikonomakis [2], Achilleas Economopoulos [2], Lorenzo Fogli [3], Antonella Cadeddu [3], Alessandro Bianchini [4], Daniel Iglesias [5] and Wouter Tavernier [6]

1 Luxembourg Institute of Science and Technology (LIST), 5 Avenue des Hauts-Fourneaux, L-4362 Esch-sur-Alzette, Luxembourg; uwe.roth@list.lu
2 Institute of Informatics and Telecommunications, National Centre for Scientific Research "DEMOKRITOS" (NCSRD), Patr. Gregoriou E & 27 Neapoleos Str, 15341 Agia Paraskevi, Greece; akis.kourtis@iit.demokritos.gr (M.A.K.); a.oikonomakis@iit.demokritos.gr (A.O.); aeconomopoulos@iit.demokritos.gr (A.E.)
3 DSTech, Via Salaria 719, 00138 Rome, Italy; l.fogli@dstech.it (L.F.); a.cadeddu@dstech.it (A.C.)
4 SCM Group S.p.a., Via Emilia 77, 47900 Rimini, Italy; alessandro.bianchini@scmgroup.com
5 Capgemini (Spain), Calle Puerto de Somport 9, Edificio, OXXEO, 28050 Madrid, Spain; daniel.iglesias-canelo@capgemini.com
6 IMEC Research Group, Ghent University, iGent, Technologiepark Zwijnaarde 126, 9052 Ghent, Belgium; wouter.tavernier@ugent.be
* Correspondence: adnan.imeri@list.lu; Tel.: +352-275-888-2780

Abstract

Reliable data availability and transparent governance are fundamental requirements for distributed edge-to-cloud systems that must operate across multiple administrative domains. Conventional cloud-centric architectures centralize control and storage, creating bottlenecks and limiting autonomous collaboration at the network edge. This paper introduces a decentralized governance and service-management framework that leverages Decentralized Autonomous Organizations (DAOs) and Decentralized Applications (DApps) to to govern and orchestrate verifiable, tamper-resistant, and continuously accessible data exchange between heterogeneous edge and cloud components. By embedding blockchain-based smart contracts within swarm-enabled edge infrastructures, the approach enables automated decision-making, auditable coordination, and fault-tolerant data sharing without relying on trusted intermediaries. The proposed OASEES framework demonstrates how DAO-driven orchestration can enhance data availability and accountability in real-world scenarios, including energy grid balancing, structural safety monitoring, and predictive maintenance of wind turbines. Results highlight that decentralized governance mechanisms enhance transparency, resilience, and trust, offering a scalable foundation for next-generation edge-to-cloud data ecosystems.

Keywords: blockchain; smart contract; DAO; decentralized application; edge computing; swarm computing

Academic Editor: Qiang Qu

Received: 30 November 2025
Revised: 4 January 2026
Accepted: 5 January 2026
Published: 8 January 2026

1. Introduction

Data availability is critical for stakeholders who rely on accurate, real-time data to make their decisions and maintain trust in the system. This timely, reliable access to data is essential for operational efficiency and for ensuring participant transparency and accountability. Moreover, information sharing is crucial for maintaining and executing

various use cases, particularly when multiple stakeholders collaborate to achieve business or daily objectives. One challenging aspect of large-scale stakeholder collaboration is the decision-making process that governs processes and events. In addition, long-term collaboration requires trust and transparency in all decisions made by the communities managing such processes.

Data availability depends heavily on the software system architecture, data governance, and sharing aspects. Many information computing systems process data within a single computer system with extensive architectural capacities in memory, processors, and storage. Decisions regarding protection levels and authorized access typically fall within the system administrator's responsibility [1,2]. Currently, the most powerful data processing is centralized, primarily situated in the cloud [3]. This approach can bring significant benefits. It enables on-demand scaling and efficient resource allocation. Further, it reduces costs by eliminating the need for additional hardware, improves data security, and ensures that data and programs on each information system remain independent, thereby increasing security and trust [4]. At the same time, cloud hosting ensures the accessibility of applications and websites using dedicated cloud resources [5].

However, despite their widespread use, centralized processing and cloud-based infrastructures fundamentally limit how services and applications operate, as they depend on large single entities for authentication, storage, processing, and connectivity, and often enforce vendor-locked development and orchestration environments [6–11]. This substantially reduces users' ability to govern their own data, limits their visibility into who holds access rights, and hinders the implementation of controls needed to prevent inappropriate or risky access [12,13].

An alternative approach to addressing data availability and collaborative decision-making challenges involves using blockchain and smart contracts. They offer a new way of managing decentralized services and ensure that data remains accessible, secure, and verifiable across the network [12,13]. Integrating decentralized governance and decentralized applications via Decentralized Autonomous Organizations (DAOs) enables tamper-proof services and process management. Furthermore, the combination of on-chain and off-chain data enabled by oracles ensures comprehensive data availability for decision-making. This ensures that external or real-world data can be securely integrated into the decentralized system, thereby improving the reliability and performance of decentralized services [12,14].

This article investigates the potential of DAO-governed smart contracts and oracle-based data acquisition to support reliable data flows and availability. The proposed governance paradigm formalizes the policies, processes, standards, metrics, and stakeholder roles necessary for effective data utilization and for achieving organizational objectives [12].

It establishes responsibilities and processes that ensure the quality and security of the data used. We will focus on swarm-based use cases, which are good examples of collaborative systems that exchange data and make collective decisions. These use cases include a swarm of drones synchronized for mast inspection (5G antennas), a swarm of sensors to monitor the structural safety of infrastructures and buildings, and a swarm of sensors to support windmill maintenance.

While earlier OASEES publications introduced the project vision and individual enabling technologies, this work goes beyond them by formalizing DAO-driven governance as an operational service layer and by validating its impact on data availability and decision-making across multiple real-world edge-swarm use cases.

This paper is organized as follows: Section 2 introduces the key concepts of edge computing and swarm-based coordination. Section 3 defines the problem of information unavailability in edge and swarm environments. Section 4 reviews related work in decentralized systems, data availability, and swarm intelligence. Section 5 presents the OASEES

concept as a DAO-as-a-service framework and outlines its high-level architecture. Section 6 details how DAOs and DApps support secure data sharing across three use cases and reports experimental results, including smart contract performance. Section 7 describes the OASEES implementation, SDK stack, and deployment across core and edge resources. Section 8 offers a cross-cutting evaluation of the DAO–DApp swarm architecture. Finally, Section 9 concludes the paper and highlights future research directions.

2. Background: Edge-Swarm Computing and the Information Sharing

This section provides an overview of the evolution from centralized cloud infrastructure to distributed and cooperative paradigms, such as edge and swarm computing. It outlines how the convergence of these models supports intelligent, scalable, and adaptive information processing across heterogeneous environments.

2.1. From Cloud to Edge-Swarm Computing

Cloud Computing presents a computing paradigm that consists of a set of resources and services offered through the Internet [15]. The Cloud Computing model enables ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) [16].

Edge Computing is a new distributed computing paradigm enabling computation and data storage closer to the data sources, i.e., near happening, such as for IoT devices or local edge servers. The core advantages of edge computing are exploiting such proximity to reduce latency, conserve bandwidth, and enhance real-time data processing capabilities. Such technological characteristics offer many advantages, including enhanced security. Exploiting local processing capabilities enables risk mitigation when transmitting sensitive data over networks [17,18]. *Swarm Computing* is a distributed computing model inspired by the collective behavior of natural swarms, such as bees, ants, or birds. In such a model, many agents work together in a decentralized, autonomous way to achieve a common goal. This is achieved by sharing information and making collective decisions, resulting in emergent intelligence that exceeds the sum of individual capabilities [19]. Swarm Computing is characterized by: (i) *decentralization*, where the decisions are made collectively rather than via single-point of control; (ii) *self-organization*, allowing agents to organize themselves based on the local and timely environment; (iii) *adaptability*, allowing agents (and systems) to responds dynamic changes in the environment; (iv) *scalability* that allows adding new agents following system needs, and (v) *robustness* where swarm-based system allows failure of certain number of agent and still perform the common task [19,20].

Swarm intelligence powers computing systems by providing various concepts that are further computerized. Such concepts are related to *data processing* and aggregation by many agents simultaneously. Further, via the *decision-making*, the intelligence process is performed by agents who share observations and converge on optimal solutions through consensus. Additionally, swarm intelligence is implemented, i.e., computerized via *learning* processes, where agents exploit feedback loops to enable the system to improve and adapt over time [19–21].

In summary, the evolution from cloud to edge and swarm computing marks a shift from centralized resource provisioning toward decentralized, intelligent collaboration among distributed entities. This transition not only enhances computational efficiency and scalability but also enables new paradigms of information sharing. Data and intelligence are processed more closely to their sources. The following section explores components of the distributed architectures that facilitate secure and adaptive information exchange across interconnected systems.

2.2. Decentralized Technology Components for Enhancing Information Sharing and Security

Blockchain maintains a distributed, decentralized shared ledger that enables secure transaction exchange. The network of BC nodes follows a peer-to-peer communication protocol, and the involved nodes maintain an exact copy of the ledger. The transaction data is governed by a consensus protocol that ensures user trust in the system's reliability. Transactions are stored in blocks, which are subsequently chained. Chaining is a fundamental characteristic of blockchain, which supports the properties of immutability and integrity of data stored on the blockchain, as well as non-repudiation of the act of storing the data by any party [22].

Smart contracts are code that runs on the blockchain. All nodes contributing to the blockchain can prove that the outcome of an innovative contract execution is correct because all data and events used to execute the smart contract code are transparent to all nodes.

A *Decentralized Autonomous Organization (DAO)* represents the concepts of an organization that operates on a blockchain. A DAO is completely controlled or governed by smart contracts. It is designed to be autonomous and decentralized, with decision-making processes and operations carried out through consensus mechanisms among its participants [23].

A *Decentralized Application (DApp)* is a type of software that operates on a blockchain in a peer-to-peer manner. Unlike traditional applications that rely on a single central server, the back-end of a DApp runs across multiple blockchain nodes, enhancing transparency, security, and censorship resistance [24].

Decentralized Storage refers to storing data across multiple nodes in a distributed network rather than relying on a single central server. This approach enhances data availability, resilience, and security, as no single point of failure can compromise the system. One widely adopted protocol for decentralized storage is the InterPlanetary File System (IPFS; https://ipfs.tech/ (accessed on 4 January 2026)), which allows files to be stored and retrieved using a content-addressed system. In IPFS, each file is assigned a unique cryptographic hash, ensuring immutability and verifiable integrity, while the network enables efficient peer-to-peer data sharing.

3. Problem Definition: Information Unavailability in Edge-Swarm Computing

The Internet of Things (IoT), smartphones, drones, and other mobile devices have recently enhanced global connectivity, allowing people, devices, and systems to stay interconnected seamlessly [25,26]. The exponential growth in device connectivity and data generation has led to the proliferation of intelligent processing services, enabling the creation of insights and the exploitation of data in a multi-modal manner. Further, the emergence of technologies, such as artificial intelligence, machine learning, data analysis, and trusted digital governance, that process large amounts of data, enables the extraction of valuable and creative insights. Exploiting such technologies enables organizations to leverage their established systems for more efficient data analysis and interpretation, leading to faster and more accurate data-driven decisions [27].

The most computationally powerful data processing is performed within centralized cloud infrastructures, enabling scalability and efficient resource allocation to respond to market demands. However, centralized processing and cloud hosting impose resource restrictions on their services and applications. That underscores the urgent need for decentralized solutions in edge-cloud computing [28,29].

In edge-cloud computing architectures, centralized processing and cloud hosting are tightly coupled, limiting the ability of services and applications to operate in resource-restricted environments, especially in data management [30]. These centralized systems

often rely on single, large entities to provide core services, including (i) **authentication**, (ii) **data storage**, (iii) **data processing**, (iv) **network connectivity**, and (v) **vendor-specific environments** for application development and orchestration [31]. As a result, centralized structures restrict data accessibility and autonomy in the edge-cloud architecture. This dependence creates significant challenges for real-time data governance, availability, and authentication, which are critical requirements for edge-native applications [32,33]. Consequently, there is a pressing need for decentralized approaches to data processing, storage, and authentication to ensure resilience, efficiency, and trust at the network edge.

3.1. Motivation to Use DAO in Swarm-Edge Computing

OASEES aims to create an open, decentralized, intelligent, programmable edge framework for Swarm architectures and applications. It leverages the DAO paradigm and integrates Human-in-the-Loop (HITL) processes for efficient decision-making. The OASEES vision is to provide open tools and secure environments for swarm programming and orchestration for numerous fields in a completely decentralized manner [13].

Decentralized swarm-based systems add complexity to decision-making. To manage this, an advanced yet transparent rules-based process is needed for sustainable collaboration. DAOs have the properties to behave as rule-based systems within an organization, assuming that decision-making processes are predetermined and encoded in advance [34]. DAOs have inherent transparency and self-explanatory properties. They impose strict access controls and end-to-end management processes. That certainly enhances the trustless properties in various business processes.

3.2. OASEES Scientific Objectives and Research Focus

This research addresses the overarching challenge of enabling data governance, security, and availability for edge–cloud applications by leveraging DAO. It explores how these emerging technologies can enhance decentralized decision-making. Further, how they establish trustless mechanisms for managing and securing data across distributed environments and for automating regulatory compliance. By exploiting the inherent properties of DAOs, i.e., transparency, immutability, and collective consensus, this study proposes solutions to overcome the limitations of traditional, centralized cloud systems, particularly in maintaining consistent, auditable, and low-latency data access. The paper emphasizes the use of "near-happening" data in edge-swarm scenarios, where governance and decision-making are distributed across multiple autonomous nodes. Within the OASEES framework, this work advances the scientific understanding of how decentralized governance and self-sovereign identity can enable resilient, auditable, and privacy-preserving data ecosystems. The scientific contributions of this research are summarized as follows:

A novel, auditable, and decentralized governance model for edge-swarm computing. This model advances beyond traditional centralized approaches by introducing a tamper-proof, transparent mechanism for coordinating swarm operations and collective decision-making. It directly addresses the key challenges of trust, transparency, and accountability in multi-stakeholder collaborations.

A secure, identity-based access control mechanism grounded in Self-Sovereign Identity (SSI). The research implements SSI-based identity management to regulate participation and data access within decentralized environments. Through verifiable credentials and on-chain identity proofs, this mechanism minimizes unauthorized access and enables trustless authentication across the swarm without relying on central authorities.

A validated architecture for real-time data availability within the OASEES framework. The study not only theorizes but also provides a practical implementation of a decentralized architecture that ensures data remains available, secure, and verifiable, overcoming the

inherent limitations of centralizing data in a single repository. It introduces a mechanism that enables the logical integration of data from heterogeneous edge devices without requiring physical consolidation, thereby improving scalability and reducing latency.

An empirical assessment of blockchain limitations in resource-constrained environments. Through performance evaluation and benchmarking, the paper identifies how traditional DLT constraints—such as latency, throughput, and energy consumption—can be mitigated via optimized consensus protocols and hybrid off-chain computation models suitable for edge-swarm ecosystems.

4. Related Works Studies, and Scientific Contributions

This section covers related studies on swarm computing and decentralized technologies in the context of varying data availability for swarm-edge systems. Furthermore, we present a scientific contribution that serves as a synthesis of progress beyond the state of the art.

4.1. Related Studies

Data availability is a critical requirement for ensuring the proper functioning and execution of intended operations within a system. Distributed Ledger Technology (DLT) and blockchain systems are no exception, as they also rely on data availability to maintain functionality. This ensures that all transactional data within associated systems remains accessible to relevant participants, thereby supporting consistent system performance and facilitating data verification.

In swarm-edge computing, where distributed nodes must autonomously coordinate, data availability and decentralized decision-making are particularly vital, as they enable real-time responsiveness, fault tolerance, and scalable collaboration among edge devices [35]. Swarm computing leverages the collective intelligence of distributed nodes to allow scalable, resilient operations. Recent studies have increasingly focused on integrating blockchain and distributed ledger technologies to enhance trust, traceability, and auditability within such systems.

For instance, Strobel et al. [36] demonstrate how blockchain-based consensus protocols can secure robot swarms against Byzantine behavior, ensuring transparent, tamper-resistant coordination. Their work establishes that even in adversarial conditions where up to 33% of agents may be compromised, blockchain-anchored voting mechanisms maintain swarm integrity. Similarly, Pacheco et al. [37] employ smart contracts for real-time swarm coordination, demonstrating how decentralized ledgers can automate decision-making and improve system robustness through experimental validation of foraging tasks. Tran et al. [38] introduce SwarmDAG, a partition-tolerant distributed ledger protocol designed for swarm networks that effectively addresses the limitations of traditional blockchains under intermittent connectivity. By employing a directed acyclic graph structure rather than linear chains, SwarmDAG achieves higher throughput and lower latency in network-partitioned environments, a critical requirement for mobile swarm robotics. Extending to other domains, Ibrahim et al. [39] apply blockchain mechanisms to nanosatellite swarms, achieving higher reliability and data integrity across distributed systems operating in resource-constrained space environments.

From a scalability perspective, Bulgakov et al. [40] and Wu et al. [41] evaluate sharding-based mechanisms that partition blockchain data to reduce latency and improve throughput, which are essential for large-scale swarm-edge infrastructures. Bulgakov's analysis demonstrates that horizontal sharding can increase transaction throughput by up to 64x in controlled environments, though at the cost of increased cross-shard communication complexity. Wu's protocol introduces dynamic shard reconfiguration based on transac-

tion patterns, showing particular promise for heterogeneous swarm systems with uneven workload distribution. Complementary approaches also leverage token economies and distributed trust models to neutralize malicious entities and maintain system integrity [42]. Strobel et al. demonstrate that economic incentive mechanisms can effectively discourage Byzantine behavior by making attacks financially non-viable, even without perfect knowledge of agent identities. These advances illustrate how decentralized coordination can mitigate the issues of central dependency, limited transparency, and probabilistic synchronization observed in conventional, centralized, or agenda-based coordination schemes.

The integration of blockchain with edge intelligence has gained attention for enabling secure distributed learning. Li et al. [43] propose blockchain-based frameworks for federated learning that address privacy preservation and model poisoning attacks through cryptographic verification of model updates. Their approach demonstrates that distributed trust mechanisms can reduce attack success rates by over 80% while maintaining acceptable training convergence, a critical consideration for swarm systems that must learn and adapt collectively. Building on this, Nguyen et al. [44] investigate hybrid storage architectures for edge-cloud systems, proposing tiered models where frequently accessed data is cached at edge nodes, intermediate data is stored in IPFS with blockchain anchoring, and archival data resides in incentivized storage networks. Their evaluation shows that such architectures can reduce data retrieval latency by 73% compared to pure blockchain storage while maintaining cryptographic verification, directly addressing the data availability challenges inherent in swarm-edge computing.

The governance dimension of decentralized systems has been examined through DAO frameworks. Wang et al. [23] provide a comprehensive taxonomy that distinguishes among token-weighted, reputation-based, and hybrid governance models, suggesting that reputation-based mechanisms may offer advantages for swarm systems that require rapid adaptation. Beck et al. [45] extend this analysis by examining hybrid human-machine voting protocols and find that human oversight in critical decision paths can increase system reliability by 34% without significantly impacting response times. However, applying DAO principles to cyber-physical systems spanning multiple domains, such as energy management, structural monitoring, and predictive maintenance, remains relatively underexplored in the literature. More recent research has further examined decentralized autonomous organizations as governance mechanisms for complex socio-technical and cyber-physical systems. Lustenberger [46] provides an up-to-date synthesis of DAO research trends, identifying key challenges related to governance scalability, participation incentives, and integration with real-world systems. Complementing this perspective, Bonnet [47] presents a systematic literature review of DAO research, highlighting governance automation, accountability, and coordination as dominant themes, and notes the limited number of studies addressing operational cyber-physical deployments.

Beyond purely digital ecosystems, Ly and Shojaei [48] investigate the application of DAOs in built and infrastructure environments, demonstrating the potential of decentralized governance for managing physical assets while emphasizing unresolved challenges related to latency, regulatory compliance, and stakeholder heterogeneity. In parallel, broader surveys on blockchain-enabled decentralized intelligence [49] highlight the convergence of governance mechanisms, edge intelligence, and autonomous system coordination, reinforcing the relevance of DAO-based approaches for next-generation cyber-physical and swarm-edge systems. However, these works generally focus on single-domain scenarios or conceptual governance models and do not explicitly address cross-domain data availability, SSI-based access control, or integrated DAO–DApp orchestration as proposed in OASEES.

Security considerations in blockchain-enabled swarms present unique challenges. Ferrag et al. [50] conduct a comprehensive survey identifying oracle manipulation, smart

contract vulnerabilities, and consensus attacks as primary threat vectors in IoT and edge environments. They propose multilayered defense strategies combining formal verification, secure oracle protocols, and edge-layer anomaly detection. In the context of swarm robotics specifically, Dorigo et al. [51] examine trade-offs between decentralization and security, demonstrating that purely distributed consensus without trusted components may be vulnerable to eclipse attacks in sparse network topologies. These findings underscore the need for hybrid architectures that balance trustlessness with practical security requirements.

Data storage solutions for decentralized systems have evolved beyond simple blockchain anchoring. Benet [52] introduces IPFS as a content-addressed, peer-to-peer protocol that has become foundational for decentralized storage. However, IPFS alone does not guarantee persistence, leading to complementary solutions such as Filecoin [53], which adds economic incentives for long-term data availability. For real-time swarm applications, these storage paradigms must be adapted to support both the immutability requirements of governance decisions and the ephemeral nature of sensor streams.

At a broader architectural level, recent surveys highlight the convergence of blockchain, edge computing, and AI for building trustworthy, low-latency, and autonomous distributed systems [54–56]. Collectively, these works reinforce the paradigm shift toward secure, transparent, and adaptive swarm-edge infrastructures, where decentralized ledgers not only record transactions but also facilitate coordination, governance, and fault resilience across heterogeneous and dynamic environments.

Recent work has explored blockchain-enabled security and scalability mechanisms in edge-cloud and cyber–physical environments. Khodjamov et al. [57] propose a blockchain-based trusted clustering framework for multi-tier Social IoT systems, focusing on secure inter-cluster communication and trust establishment across edge and cloud layers. While effective for hierarchical IoT security, their approach remains protocol-centric and does not address decentralized governance, identity sovereignty, or multi-stakeholder coordination.

Similarly, Li et al. [58] introduce AssociateChain, a scalable blockchain architecture for cloud–edge systems based on associative sharding, primarily targeting throughput and data consistency in large-scale deployments. However, this work focuses on infrastructure-level scalability rather than governance-as-a-service, policy-driven access control, or Human-in-the-Loop decision-making, which are central to OASEES.

4.2. Comparative Analysis and Research Positioning

Existing blockchain-based swarm and edge computing approaches share common goals with OASEES, including decentralization, trust establishment, and fault tolerance. However, most prior work focuses on coordination or consensus among agents (e.g., blockchain- secured voting or task allocation), treating governance, data availability, and access control as secondary concerns. In contrast, OASEES explicitly elevates governance to a first-class service through DAO-as-a-Service, integrating identity (SSI), data access policies, and execution logic within a unified framework.

Moreover, while several studies validate their approaches in simulations or single-domain scenarios, OASEES demonstrates cross-domain applicability through multiple real-world use cases, highlighting both strengths (auditability, stakeholder accountability, flexible onboarding) and limitations (latency overheads and reliance on permissioned participation). This positioning allows OASEES to address practical governance and data-availability challenges that are insufficiently covered by existing swarm-edge solutions. Table 1, highlighting similarities, differences, advantages, and limitations of the proposed approach with respect to representative related works.

Table 1. Comparison with Representative Related Works.

Evaluation Metric	Blockchain-Based Swarm Coordination [36–38,57,58]	DAO-Enabled Edge/CPS Systems [23,45]	OASEES (This Research Paper)
Primary objective	Secure coordination and consensus among swarm agents	Automation of selected cyber–physical processes	Governance-driven data availability and decision-making across edge-cloud swarms
Governance model	Implicit or protocol-level coordination	Partial DAO usage, often limited to voting	DAO-as-a-Service with explicit proposal, voting, execution, and treasury mechanisms
Data availability handling	Assumed through ledger replication	Application-specific and limited	Explicit design combining on-chain governance, off-chain storage, and oracle-based ingestion
Identity and access control	Typically absent or centralized	Basic role-based or token-based mechanisms	SSI-based identity with verifiable credentials and policy-driven access control
Human-in-the-Loop support	Generally not considered	Occasionally included for exceptional decisions	Native HITL integration for critical governance and operational actions
Validation scope	Simulations or single-domain experiments	Single use-case deployments	Multiple real-world use cases across energy, infrastructure, and industrial domains
Known limitations	Limited governance and data lifecycle management	Participation and scalability challenges	Governance latency and reliance on permissioned stakeholders as a trade-off for auditability

Despite these advances, several critical gaps remain (summarized in Table 1). In contrast to previous OASEES-related studies that primarily focused on architectural concepts or isolated blockchain components, this paper provides an integrated DAO–DApp–SSI framework and a cross-domain empirical evaluation, thereby extending the state of the art from conceptual design to operational governance in edge-swarm systems.

First, while existing work demonstrates blockchain-based coordination for small-to-medium swarms (typically fewer than 100 agents), governance mechanisms for large-scale deployments exceeding 1000 agents remain underexplored, particularly with respect to voting efficiency, proposal management, and spam prevention. Second, most blockchain-enabled swarm studies focus on scenarios where sub-second response times are not critical. In contrast, applications such as structural safety monitoring or energy grid balancing require near-instantaneous coordination, creating inherent tension between blockchain consensus latency and operational requirements. Third, the seamless integration of human decision-makers into DAO-governed swarms while preserving decentralization properties has received limited attention—existing Human-in-the-Loop (HITL) approaches often reintroduce central control points or operational bottlenecks. Fourth, most studies focus on homogeneous swarms rather than heterogeneous, multi-stakeholder environments with fundamentally different governance, incentive, and data-sharing requirements. Finally, real-world validations of DAO-based swarm governance across multiple application domains remain scarce, with most existing work limited to simulations or single-domain pilots.

By addressing these gaps, this work advances the state-of-the-art through: (1) demonstrating DAO-governed coordination across heterogeneous, multi-domain swarm-edge systems spanning energy, infrastructure, and industrial applications; (2) integrating SSI-based access control with blockchain governance to enable trustless authentication without central authorities; (3) providing empirical insights into scalability and performance trade-offs through parallel validation across multiple real-world use cases and (4) establishing a replicable architectural framework for decentralized edge-cloud data ecosystems that balances the immutability requirements of governance with the real-time demands of swarm coordination.

5. OASEES: The DAO as a Service for Decentralized Edge-Cloud Use Cases

In this section, we discuss the OASEES project and how its framework addresses the problems and challenges presented in Section 3. We present project use cases built on that framework.

The OASEES project (OASEES: Open autonomous programmable cloud apps & smart sensors; https://oasees-project.eu/ (accessed on 4 January 2026)) introduces a decentralized and swarm intelligence-based computing framework built on Distributed Ledger Technology (DLT) (see Figure 1 on the following page) [12,14]. The foundational elements of DLT enable trustworthy data exchange and collaboration, fostering transparency and trust by creating an auditable trail. This system ensures that every participant within the swarm agrees on the state of the data in the ledger, leading to consensus.

OASEES deploys Decentralized Autonomous Organization (DAO) to inherent trust within swarms, where an OASEES swarm organizes its operations and intelligence via a DAO. Each device within the swarm can participate in the DAO, voting automatically on decision-making based on different parameters and conditions. This self-governance model, in conjunction with the cloud-native approach of OASEES, forms a flexible, agile framework for swarm architectures.

Swarm collaboration within OASEES is a robust process that brings together a collective of edge devices and human experts. It leverages decentralized technology for involvement, synchronization, and oversight. A significant aspect of this process is the execution of collaboration within the Gaia-X (Gaia-X: Federated Secure Data Infrastructure; https://gaia-x.eu/ (accessed on 4 January 2026)) data federation, which enhances data sharing, interoperability, and sovereign data services. It enables federated learning by coupling DAO with Human-in-the-Loop (HITL) mechanisms across disparate edge devices.

These technological components offer several benefits: Participants can interact with the DAO through digital wallets, which allow them to stake tokens, vote on proposals, and receive rewards. The DAO paradigm's underlying automation works in harmony with human intelligence, driving toward the fulfillment of intricate objectives and the resolution of complex challenges.

In line with its decentralized architecture, data will remain distributed across multiple databases while providing a unified view of data access. Data federation enables data integration across different data sources or edge devices without requiring physical data consolidation. The data will remain under the control of the respective source, maintaining data ownership and security. It will improve scalability, as new data sources can be added/removed in real time, minimizing data movement and reducing latency. In this context, OASEES serves as a "First-Level Data Space" because it operates very close to where the data is generated. Here, the data can be correlated, stored, and integrated.

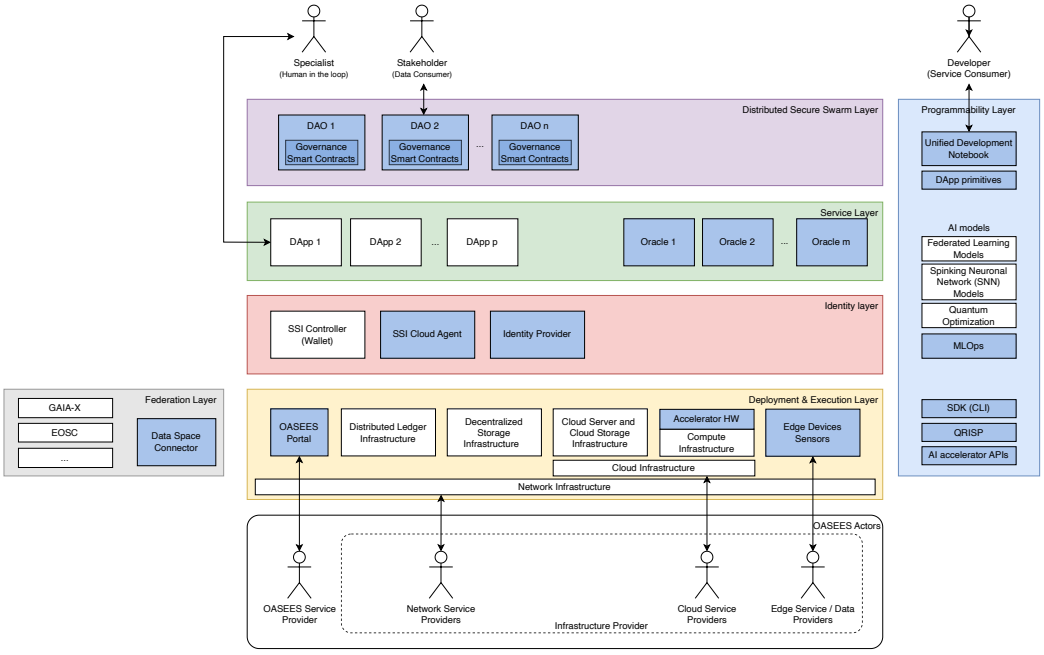

Figure 1. OASEES high-level architecture.

5.1. OASEES High-Level Architecture

The OASEES high-level architecture involves various actors and components that interact across different layers. Figure 1 highlights these components and their positions inside one of the following layers. The blue boxes represent the OASEES core components.

The entire framework is built on top of a **Deployment and Execution Layer**. This layer includes different types of infrastructure with related management elements, such as network and cloud infrastructure, distributed ledger and decentralized storage infrastructures, and cloud server and cloud storage infrastructures. The data from the physical edge devices, including their sensors, might be processed in the compute infrastructure, which may use accelerator hardware to offload CPU-intensive calculations. Finally, it includes the OASEES portal, which serves as the central access point for provisioning swarm services.

The **(Data) Federation Layer** in OASEES enables seamless operation in multi-instance configurations within federation frameworks for cloud services and data spaces. OASEES aligns with Gaia-X concepts to connect infrastructure and data ecosystems, promoting compliance, federation, and data exchange. It acts as both an infrastructure service provider and a data provider, leveraging innovative edge-aware brokerage to facilitate collaboration and resource sharing. By registering its resources and services in the European Open Science Cloud (EOSC) (EOCS: European Open Science Cloud; https://open-science-cloud.ec.europa.eu/ (accessed on 4 January 2026)) ecosystem, OASEES becomes a provider within EOSC, thus offering various services and adding value through monitoring and helpdesk support.

The **Identity Layer** integrates Self Sovereign Identity technology, enabling the creation of portable digital identities based on Decentralized Identifiers (DIDs) and Verifiable Credentials (VCs). DIDs provide control over digital identity without relying on centralized intermediaries, while VCs offer tamper-evident credentials with enhanced trustworthiness. This layer consists of the SSI controller, which enables secure authentication to the OASEES portal; the SSI cloud agent, which stores and fetches certificates and DIDs in the distributed ledger; and the identity provider, which enables secure interactions and the identification of DAO participants.

The **Service Layer** provides the components for building and deploying Decentralized Applications (DApps). DApps are composed of micro-services and smart contracts.

The former are based on (traditional) cloud and edge infrastructure and associated services, the latter are based on smart contracts registered in a decentralized ledger. To bridge the gap between these two worlds, the service layer also involves oracles to enable interaction between smart contracts and the external world.

The **Distributed Secure Swarm Layer** focuses on the key OASEES concept of the DAO as a framework for regulating interactions among multiple parties, including humans and/or swarms of devices. The DAO is implemented as a set of smart contracts and includes Human-in-the-Loop (HITL) mechanisms that facilitate resource management, incentives, and decision-making for swarm collaboration. It includes **Governance Smart Contracts** that handle all smart contract logic for managing, collecting, and following up on proposal generation and voting. Users interact with the DAO through digital wallets, token staking, voting on proposals, and receiving incentives.

The **Programmability Layer** of the OASEES architecture provides the necessary tools and interfaces for developing, deploying, and managing decentralized applications (DApps) and DAOs on the Cloud-Edge continuum. It encompasses the OASEES SDK, which includes the CLI and DApp primitives for developing and deploying decentralized applications across the Cloud-Edge continuum. The unified development notebook serves as the central focal point for developing DAOs, smart contracts, and DApps. MLOps is a set of practices and tools designed to streamline the deployment, monitoring, and continuous improvement of machine learning models in production environments, and it supports several AI models, as well as external APIs. Additionally, the Eclipse QRISP quantum development kit is envisaged for deployment within DApps accessible through the OASEES portal.

5.2. Actors

Multiple stakeholders have roles in the OASEES paradigm. Each stakeholder plays a crucial role in the operation and management of OASEES services, ranging from infrastructure (cloud) management to service design, consumption, and provision.

An **Infrastructure Provider** provides devices and associated control/orchestration framework managing the devices to be used by OASEES to build services on top of them. We distinguish between Cloud Service Providers, Edge Service Providers (or, more general, Data Providers) and Network Service Providers.

Cloud Service Providers are responsible for managing and maintaining the cloud infrastructure, such as the cloud servers, cloud storage, and cloud networking equipment. They are responsible for ensuring that the cloud infrastructure is secure, reliable and performant, and they provide the tools and APIs that developers need to build and deploy applications on the cloud. Cloud Service Providers may also provide additional compute infrastructure, such as data processing, and machine learning, including accelerator hardware, that developers can use to build more advanced applications.

Sensors or data-generating devices (e.g., drones), such as those used to monitor wind turbines, may be owned by various parties, referred to as **Edge Service Providers** or **Data Providers**, depending on the context and application. In some cases, the equipment manufacturers may provide sensors as part of their products or offer them as optional additional features.

Network Service Providers provide the underlying network infrastructure to which Cloud Service Providers and Edge Services Providers connect. They are responsible for ensuring that the network is secure, reliable, and performant, managing the underlying network infrastructure, including the edge computing devices, routers, and switches. Network Service Providers also provide the necessary Distributed Ledger and the Decentralized Storage Infrastructure (e.g., IPFS).

Specialists (e.g., doctors) might act upon data as produced by the OASEES services or interact with OASEES DApps to make decisions as part of or interacting with a smart contract. This enables **Human-in-the-Loop** (HITL) interaction as envisioned in the project framework.

Developers act as **Service Consumers** and develop OASEES services and/or DApps. The former refers to the design of pure data processing (e.g., AI models for vision based on generated data) functionality; the latter refers to the design of smart contracts in the context of DApps deployed for a DAO. OASEES developers are individuals or groups who design and deploy DApps on top of the DAO platform and components provided by Cloud Service Providers, Edge Service Providers, equipment vendors, and governmental agencies.

Data Consumers or OASEES users are **Stakeholders** who use the outputs of OASEES services or DApps. Users can be patients who interact with a service providing them assistance.

Last, but not least, the **OASEES Service Provider**, also referred as the **OASEES Swarm Operator**, manages the OASEES portal, interacting with the infrastructure of different providers to provide OASEES DApps on top of DAOs to the Data Consumers.

6. Leveraging DAOs and DApp for Secure Data Sharing and Availability

The integration of DAOs and DApps within the OASEES architecture aims to fundamentally transform secure data sharing and availability in edge-swarm systems by replacing centralized control with cryptographically enforced governance protocols. Unlike conventional approaches that rely on a trusted intermediary, OASEES introduces decentralized decision-making, automated policy execution, and blockchain-based auditability. This ensures that multiple stakeholders with potentially competing interests can collaborate without depending on mutual trust, while maintaining resilience against manipulation or unilateral control. Furthermore, relying on well-defined, transparent rules enables broader business opportunities for data consumers seeking to train AI/ML models.

Building on the architectural foundations presented in Section 5, this section examines how real-life use cases demonstrate practical implementations of DAO-governed data sharing. The proposed design shows how DAO governance enforces access control and trust mechanisms, while DApps serve as the functional layer that operationalizes business logic by invoking smart contracts and linking governance proposals to real-world activities.

OASESS has executed this exercise on six use cases (UC):

UC Energy Grid: Support of optimal operation of the electricity grid via coordinated recharging of fleets of electric vehicles

UC Structural Safety: Structural safety assessment of buildings and critical infrastructure

UC Windmill Maintenance: Predictive maintenance of windmills

UC Antenna Inspection: Drone-based hight mast inspection of 5G antennas

UC Smart Manufacturing: Collaborative robotic powered smart manufacturing

UC Parkinson: Analysis of voice, articulation, and fluency disorders in Parkinson's Disease

In this way, OASEES provides an integrated framework that can be coordinated through swarm intelligence mechanisms. Furthermore, by combining blockchain anchoring, distributed storage solutions such as IPFS, and DAO-based access governance, OASEES ensures that swarm-collected data remains verifiable, queryable, and resilient to both technical failures and organizational biases. This architecture directly addresses the fundamental challenge of data unavailability in edge-swarm computing, replacing centralized bottlenecks with decentralized, auditable, and adaptive governance.

The following subsections present detailed use-case demonstrations that illustrate how DAO and DApp coordination enforce secure data availability while supporting swarm

intelligence across diverse domains. We focus only on the use cases *Energy Grid*, *Structural Safety*, and *Windmill Inspection*, because they are generic enough to demonstrate the feasibility of the proposed architecture.

6.1. UC Energy Grid: Support of Optimal Operation of Electricity Grid via Coordinated Recharging of Fleets of Electric Vehicles

With the increasing number of distributed intermittent renewable power plants, i.e., photovoltaic systems, and a rising demand for energy due to the transition to electric mobility, significant congestion is occurring in some energy grids worldwide. This happens because the demand for energy to charge cars, which is high at night, is not synchronized with the photovoltaic systems' production during the daytime, particularly at noon. In some cases, this results in a surplus of power that the typical energy customers and households do not consume. This produces Reverse Power Flows (PRFs) through the substations of the low-voltage distribution network, for which many electricity grids are not designed. This might lead to significant problems, such as voltage rise, frequency imbalance, and equipment tripping. Leveraging energy flexibility services would help stabilize the network and limit the effort required to modernize the power grid.

The use case aims to integrate photovoltaic power generation and electric-vehicle energy consumption during periods of power surplus by incentivizing vehicle owners to charge their vehicles at specific times.

The overview diagram in Figure 2 shows several participants and their relationships. Table 2 on the following page lists the main actors, the involved systems, and new platforms or systems developed based on OASEES, as well as the essential data structures.

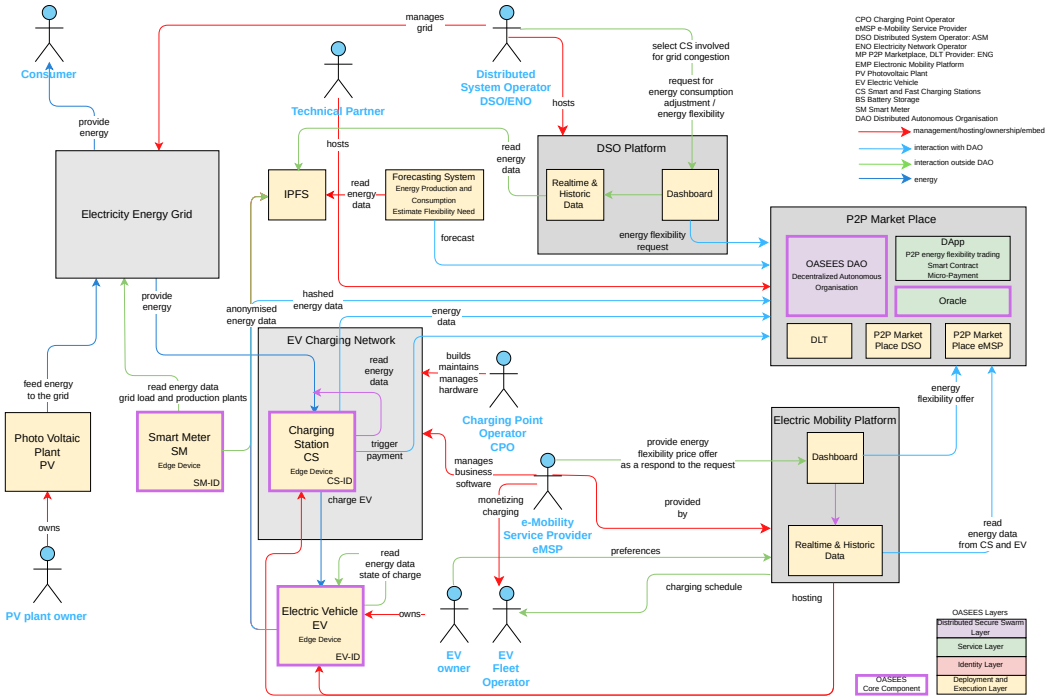

Figure 2. Diagram of the energy grid-electric vehicles use case.

At the center of the use case is the P2P Marketplace, which facilitates energy trading between producers and consumers. This marketplace builds on DAOs and DApp to align charging availability with requests from energy providers for flexibility. The other relevant platforms are the Distributed System Operator Platform of energy providers, the Electric Mobility Platform for Charging Point Operators, and the Electric Vehicle Owners Platform. Both platforms hide the P2P Marketplace from the users.

Table 2. Main actors, systems and components of the energy-grid use case.

Main Actors	
DSO ENO	Distributed System Operator Electricity Network Operator Manages the energy grid
eMSP	e-Mobility Service Provider Manages the business side of the changing network with its charging stations for electric vehicles (customers and monetising EV charging)
CPO	Charging Point Operator Builds, manages and maintains the charging network with the charging stations
EV Owner EV Fleet Operator	Owner of electric vehicles
Main Involved Systems	
EV	Electric Vehicles
CS	Charging Station
SM	Smart Meter Real-time readings of energy consumption data.
New Platforms/Systems	
EMP	Electronic Mobility Platform Hosts charging stations Hosts electric vehicles
DSO Platform	Distributed System Operator Platform Manages DSO activities
P2P Marketplace with DLT	P2P energy flexibility trading Access via the DSO Platform and the EMP
Forecasting System	Estimates energy production and energy consumption Estimates the flexibility needs
New Sub-Systems	
DApp	Decentralised Application Aligns charging available and energy flexibility requests via the DAO
DAO	Decentralised Autonomous Organization
Dashboards	Provide access to the P2P Marketplace Accessed via the DSO platform and EMP Show real-time payment data. Manage access control
Important Data Structures	
Smart Meter Energy Data	Energy grid monitoring data
Charging Station Energy Data	Charged energy to the electric vehicle
Electric Vehicle Energy Data	Consumed energy by the electric vehicle State of charge
Energy Flexibility Request	Energy need Time indication for flexibility service provision
Energy Flexibility Offer	Remuneration asked for flexibility service provision

6.1.1. DAO Activities and Proposals

In this use case the DAO acts as a swarm intelligence mechanism, coordinating distributed decision-making across heterogeneous actors, such as Distributed System Operator (DSO), Electricity Network Operator (ENO), Charging Point Operator (CPO), e-Mobility Service Provider (eMSP), and Electronic Vehicles (EV) owners or fleet operators, through a transparent proposal and voting process. It also manages complex multi-party interactions among stakeholders through programmable governance rules for energy grid optimization. By encapsulating operational decisions into DAO proposals and binding their execution to smart contracts and decentralized applications (DApps), the Energy Grid UC ensures adaptive, self-organized, and trustless governance of critical energy and mobility functions. Further, it calculates optimal pricing via embedded auction mechanisms and executes energy-trading smart contracts without manual intervention. In the Energy Grid use case, each governance proposal references a predefined smart contract function. After reaching quorum and majority approval, the DAO automatically executes the corresponding contract, which updates on-chain governance state (e.g., access control lists or device registries) and emits execution events. These events are consumed by DApps and oracle services, which enforce the decision at the application and data layers, such as enabling or revoking access to IPFS-hosted datasets or activating device-specific data feeds. This design ensures that approved access rules are enforced consistently without manual intervention.

The DAO manages complex coordination activities within the UC through the submission of proposals. In the following, we present the Energy Grid UC activities:

Market and pricing regulation:

- Proposals to set or update electricity prices offered by the DSO.
- Proposals to determine the CPO selling prices, including specification of payment timing and conditional settlement rules.
- Proposals to automatically adopt the lowest available selling price for efficiency and fairness.

Infrastructure management:

- Onboarding of new edge devices (e.g., Smart Meters, Charging Station (CS) units), validated by the relevant authority.
- Removal of malfunctioning or compromised edge devices.
- Addition or removal of organizations participating in the network.

Incentive and economic models:

- Proposals to define or update incentive mechanisms for participating members, executed through a treasury smart contract.
- Proposals to initiate micro-payments between stakeholders to support dynamic energy exchanges.

Data governance and access control:

- Proposals for data-sharing rules, specifying update, removal, or addition of data governance policies.
- Proposals for access control and data management, including specification of which datasets (e.g., smart meter readings, Electric Vehicle (EV) telemetry, charging schedules) can be accessed by which actor.

Voting on onboarding and configuration proposals is limited to relevant stakeholders (e.g., DSO, CPO, and eMSP) whose operational or economic outcomes are directly affected by such decisions. Participation is therefore incentivized by the need to preserve grid stability, prevent the inclusion of misconfigured or malicious devices, and ensure correct revenue allocation, rather than by speculative token rewards. For routine operational

decisions, voting may be delegated or automated based on predefined compliance and validation rules, whereas critical actions may trigger a Human-in-the-Loop review.

6.1.2. Interaction Schema

The interaction of the DAO with the broader smart contract stack and system components. The process begins with identification, during which DSO, CPO, eMSP, CS, and users are authenticated via the OASEES Identity Layer using decentralized identifiers (DIDs), as shown in Figure 2. Similarly, edge devices such as Smart Meters are uniquely identified and associated with Verifiable Credentials (VCs).

Key elements of the interaction include:

Data collection and storage: Smart Meters and CS units provide real-time consumption and pricing data, transmitted via ORACLE services and stored in the decentralized storage (IPFS). EVs also contribute usage and charging demand data, which are hashed on-chain for auditability.

Data sharing and notifications:

- eMSPs notify the DSO of business activity changes.
- The DSO provides and requests data from the CPO, stored in IPFS for later use in scheduling and forecasting.
- The EV drivers are informed of updated charging options and schedules.

Forecasting and decision-making: The DSO feeds forecasted production and consumption data into the DAO, which becomes accessible to DApps for demand–supply balancing. Proposals for new pricing models are triggered, disseminated to stakeholders, and voted upon.

Voting and consensus: DAO members vote on submitted proposals (e.g., pricing, onboarding devices, data access rules). Once consensus is achieved, the proposal is executed through its associated smart contract.

Execution and settlement: Actions such as micro-payments are performed automatically via the treasury smart contract, ensuring immediate settlement of economic transactions according to DAO-approved rules.

6.1.3. HITL Interaction and Incentives

In the Energy Grid use case, actors interact with DAO-governed smart contracts via authenticated dashboards and digital wallets, enabling them to review proposals, cast votes, and approve exceptional actions. HITL intervention is required at predefined governance points, such as resolving conflicts between grid stability and cost optimization, validating reconfiguration proposals triggered by anomalous grid conditions, or adjusting incentive and pricing parameters.

Participation is incentivized by direct operational responsibility for grid stability, regulatory compliance, and revenue allocation rather than by speculative token rewards. Once quorum and approval thresholds are met, smart contracts deterministically enforce the approved decisions, ensuring that human actions remain transparent, auditable, and bound by the same governance rules as automated agents.

6.1.4. Swarm Intelligence Perspective

The DAO-driven interaction model in the Energy Grid UC reflects swarm intelligence principles by enabling emergent, adaptive coordination without requiring centralized oversight. Similar to biological swarms, local interactions, such as electricity price proposals from a Distribution System Operator (DSO), the onboarding of new smart meters or charging stations, or updates to data-sharing policies, propagate through stigmergic processes. In these processes, published proposals guide the ecosystem's collective decision-making.

This ensures **self-organization**, as proposals emerge dynamically from the needs of individual actors (e.g., a CPO defining selling prices or an organization suggesting new data-access rules) and are collectively refined through the voting process. **Distributed control** replaces unilateral authority, since no single stakeholder dictates outcomes; instead, decisions gain legitimacy through decentralized consensus. At the same time, the system fosters **resilience and adaptability**, as participants, whether edge devices, organizations, or governance rules, can be flexibly added or removed without disrupting global operations. Finally, **transparency and trust** are guaranteed by smart contracts that immutably log DAO, approved actions, ensuring that governance remains auditable, tamper-resistant, and non-repudiable.

6.2. UC Structural Safety: Structural Safety Assessment of Buildings and Critical Infrastructure

To monitor the structural conditions of buildings and infrastructure before, during, and after severe events such as earthquakes, sensors and decision support systems are employed in this use case. Currently, sensor data collection occurs on the customer's premises and at local sensors, primarily accelerometers and laser deformation sensors. These data require verification, filtering, correction, and interpretation. Only after that, some conclusions can be withdrawn regarding the safety of the structures in question. To do so, the data is currently transferred to a remote decision support system (DSS) for post-processing and decision-making, which is inefficient and causes several practical problems, including data privacy concerns and, most importantly, increased response time. There are also several cases where, due to a lack of electricity, an electricity circuit jump, or a problem with the communication lines, the crucial data is not even transferred fully to the central computing unit, although it is possible to retrieve it.

One issue with the centralized approach in use is data latency. Such data needs to be recorded at least 200 Hz at multiple channels. This is a demanding data streaming and processing task, especially when numerous sensors are involved, which is why some sensors may delay submitting data to this external software.

Therefore, it is highly beneficial to migrate the central DSS to a distributed architecture with components at both the edge and in the central cloud. Decentralized computing capabilities within OASEES not only improve the robustness of the DSS in use but also enable swarm technology to combine geographically distributed sensors around an earthquake epicenter.

Table 3 on the next page and Figure 3 show the relevant actors, systems components and data structures, and their relationship.

At the center of that use case is the OASEES-supported architecture that receives information about a potential earthquake event (location, measurements, related data), which is presented to the human-in-the-loop for review and to request advice and actions.

Sensor data from buildings and infrastructure are monitored by the Night Watch (NW) Decision Support System (DSS) before, during, and after seismic events. The challenge arises from the high volume of data generated during earthquakes, which often leads to delays in detection and reporting when processed centrally. To address this, the Structural Safety UC shifts the logic to edge devices by embedding NW-DSS within them. Once an event is detected by the NW or reported by an external agency, the NW-DSS triggers the DAO to initiate a reporting process, switching edge devices into swarm mode. Edge devices pre-process, filter, and cross-correlate the data locally, storing hashes on the blockchain (DAO) for integrity, while uploading processed data to IPFS. A Human-In-The-Loop (HITL) validates and classifies the event (e.g., an aftershock vs. a new earthquake) through DAO proposals that may adapt or terminate swarm activities.

Table 3. Main actors, systems, components, and data structures of the structural safety use case.

Main Actors	
Customer	Hosts multiple sensors
HITL	Human in the Loop Takes decisions based on decision support
Main Involved Systems	
Smart Edge Device	Accelerator Runs decentralized application (DApp) Provides federated learning for information collection Features pre-treatement of data and sharing it with other Smart Edge Devices
Intra-Structure Sensor	Allows internal scanning of objects
New Platforms/Systems	
Night Watch	Monitors structures before, during and after an event. Placed on each sensor or a few clusters of sensors depending on how close the sensors are placed to each other Decision-Support System Verifies, filters, corrects, and interprets raw sensor data.
OASEES Supported Architecture	Governance and process optimization
New Sub-Systems	
DApp	Decentralised Application via the DAO
DAO	Reports to the Human in the Loop Asks for advice actions Requests to review
Dashboards	Controls all the NightWatch clients running at each location Collect the individual models from each NightWatch to update a global model. Collect data from various sensors to manually train a model.
Important Data Structures	
Raw Sensor Data	Collected by the sensors
Clean Sensor Data	Pre-treated data Verified, filtered, and corrected raw data by the Night Watch System Stored in the database of the smart-edge device.
Processed Data	Interpreted version of the clean data created by the Night Watch System, stored in the IPFS
Event Data Hashes	Summary/array of processed data created by the Night Watch System, stored in the blockchain.

This approach aims to minimize latency, improve decision-making, and ensure critical stakeholders (e.g., airports, tunnels, emergency teams) receive reliable safety assessments within the first minutes after an earthquake, as a significant improvement over centralized systems that deliver delayed responses.

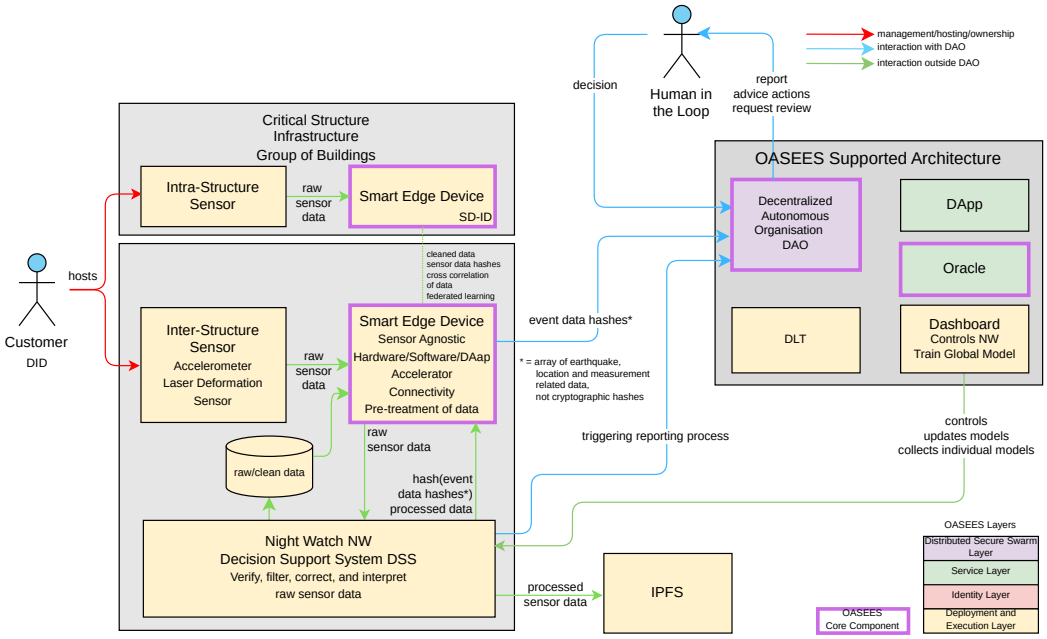

Figure 3. Diagram of the structural safety use case.

6.2.1. DAO Activities and Proposals

DAO-based governance in the Structural Safety UC supports the following categories of proposals:

HITL Proposals:

- Register or update decision algorithms for safety measurement (NW configuration).
- Verify or approve changes to NW-DSS algorithms.
- Onboard or remove swarm edge devices.

DApp/Smart Contract Proposals:

- Request access to data streams or stored features.
- Enable DApp activities such as event-triggered reporting and notifications.
- Communicate with edge devices to trigger specific swarm activities.

6.2.2. Interaction Schema

The interaction stack for the Structural Safety UC involves smart edge devices, DAO governance, IPFS storage, HITL decision-making, and external agencies:

- **Smart Edge Devices** authenticate sensors, filter and cross-correlate raw data, store processed data in IPFS, and commit hashes to the DAO.
- **The DAO** manages proposals for algorithm updates, device onboarding, and reporting triggers.
- **The HITL** evaluates DAO-generated reports, validates classifications, and proposes reconfigurations.
- **External Agencies** access DAO/DApp outputs for emergency interventions and reporting.

6.2.3. HITL Interaction and Incentives

In the Structural Safety use case, HITL actors interact with the system via DAO-linked dashboards that present aggregated event reports, confidence indicators, and provenance information derived from swarm-processed sensor data. Human input is required to validate or classify detected events (e.g., distinguishing aftershocks from new seismic

events), approve changes to decision-support algorithms, and determine escalation or termination of swarm activities.

Incentives for participation are primarily safety- and responsibility-driven: timely human validation directly affects public safety, liability exposure, and regulatory compliance. All human decisions are submitted as DAO proposals, ensuring traceability, accountability, and non-arbitrary intervention in safety-critical workflows.

6.2.4. Swarm Intelligence Perspective

The DAO-driven coordination model within the Structural Safety UC embodies principles of swarm intelligence, enabling adaptive, resilient collective behavior in disaster-response scenarios. Under stress conditions, such as earthquakes, local edge devices perform rapid sensor analysis and fault detection, thereby ensuring **self-organization** through immediate responses that do not rely on centralized commands. These local assessments propagate upward through DAO proposals and consensus mechanisms, creating stigmergic reinforcement whereby consistent signals across multiple devices strengthen the credibility of detected structural anomalies. In this way, **distributed control** is maintained, as no single authority dictates outcomes; instead, collective agreement among devices, edge nodes, and stakeholders ensures robustness in decision-making. The integration of HITL governance further enhances **resilience and adaptability**, as human expertise is combined with swarm-driven consensus to refine responses without undermining decentralization. Finally, **transparency and trust** are ensured by DAO-approved smart contracts that immutably record all anomaly detections, maintenance decisions, and response actions, guaranteeing auditability and accountability even in emergency conditions.

6.3. UC Windmill Maintenance: Predictive Maintenance of Windmills

Wind turbines are complex industrial systems that use various materials, and their components are complicated to recycle, especially the blades, which are made of layered composite materials. Extending the useful life of wind farms is an important goal to reduce the environmental and economic costs of demolishing them. Current techniques to extend the useful life of wind turbines rely on predictive maintenance. This type of maintenance involves continuous monitoring of data obtained from system elements. By analyzing this data, the state of the system can be characterized and used to improve the detection and prediction of failures through mathematical models, machine learning techniques, parameter estimation, and other methods.

Wind farm monitoring is primarily deployed internally in each wind turbine and measures acceleration, temperature, pressure, rotation speed, and current intensity. The techniques for monitoring wind turbine blades are commonly based on visual inspection, which can be performed by a human hand with a camera or by unmanned aerial vehicles. Other techniques use different sensors along the blade, which are intrusive and inconvenient. The objective is to deploy a portable, non-intrusive monitoring system based on acoustic signal analysis, which is independent of the wind turbine.

This manual assessment or the use of a centralized monitoring platform introduces latency, high operational costs, and limited scalability. The Windmill Maintenance UC, instead, integrates the OASEES architecture (DLT, SSI, DAO, and DApp) with IoT swarms, edge devices, and cloud computing to provide a decentralized, transparent maintenance solution. The DAO facilitates collective decision-making for critical processes, including dataset access, model governance, and protocol updates, while smart contracts automate the distribution of verified maintenance instructions.

Different factors can cause failures in a wind turbine blade. One of the most common causes is lightning striking the blade, which can cause internal damage. Other problems

include delamination, erosion, cracks, and de-bonding caused by wind-blade interaction. As the aerodynamic noise generated by the blades depends on their aerodynamic performance, these failures should affect the acoustics measurable with a microphone.

The objective of this use case is to enable real-time fault detection and classification of anomalies in wind turbine blades through a Blade Acoustic Monitoring System (BAMS) that collects audio recording, wind speed and direction information, temperature, and humidity. This system uses a swarm of IoT devices to capture acoustic signals generated by wind interacting with turbine blades. By analyzing these signals, potential faults, such as cracks, delamination, and other structural weaknesses, can be detected early. Based on federated learning, the failure-prediction algorithm will be consolidated, aggregated, and distributed to IoT devices.

The outcomes of the Windmill Maintenance UC are reflected in enhanced reliability and operational safety, achieved by minimizing downtime, streamlining inspection workflows, and reinforcing stakeholder trust through transparent, on-chain governance. By decentralizing fault detection, anomaly classification, and maintenance decision-making, the Windmill Maintenance UC fosters a more resilient, efficient, and trustworthy wind turbine infrastructure.

Table 4 on the following page and Figure 4 illustrate the relevant actors, system components, and data structures, along with their relationships.

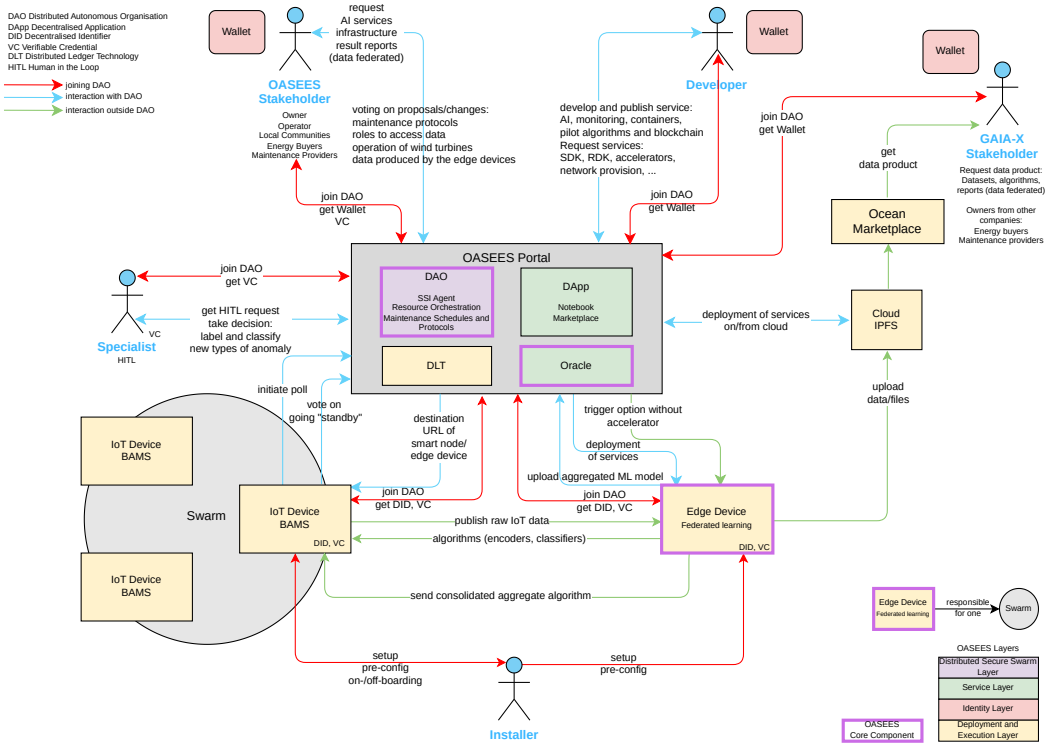

Figure 4. Diagram of the predictive windmill maintenance use case.

At the center of the use case is the OASEES-based portal, which monitors blade structures, orchestrates swarm resources, and generates test reports. It also manages polls from the swarm on whether it is agreed to go to standby.

Edge devices will use the raw data from the Blade Acoustic Monitoring Systems in the swarm to perform federated learning and distribute consolidated, aggregated encoder and classifier algorithms to the swarm.

As a side effect, the collected data can be sold as a data product via a marketplace to Gaia-X stakeholders.

Table 4. Main actors, systems, components and data structures of the predictive maintenance use case.

Main Actors	
OASEES Stakeholder	Access the portal to request algorithm services, results and reports Involved in DAO proposals (voting) for improvement of the ecosystem
GAIA-X Stakeholder	Energy company interested in data product of another energy company Access to the Ocean Marketplace and purchase data product
Specialist	Specialist on wind turbines and their failures. Human in the Loop (HITL) Labels and classifies new types of newly detected anomalies Take decisions over the devices for monitoring schedules Check result reports and maintenance plans to verify their quality
Installer	Setup, pre-configuration, and on/off-boarding of IoT and edge devices
Developer	Develops and publishes services and functionalities
Main Involved Systems	
IoT Device	Blade Acoustic-Monitoring System BAMS Initiate polls and votes
Edge Device	Assigned to one swarm of IoT devices with the BAMSReceives the raw IoT data Has an attached accelerator Manages the federated learning between IoT devices and the accelerator
Accelerator	Machine-learning algorithm Failure prediction Generates a consolidated algorithm from fragmented algorithms
Cloud	Provides services, e.g., failure-prediction algorithm Off-chain storage Offer data in the Ocean Marketplace
New Platforms/Systems	
OAEES Portal	Monitors structures before, during and after an event. Placed on each sensor or a few clusters of sensors depending on how close the sensors are placed to each other Decision-Support System Verifies, filters, corrects, and interprets raw sensor data.
New Sub-Systems	
DApp	Decentralised Application Monitors health status of blade wind turbines Shows meteorological conditions of wind farm Show geographical position of devices Notebook Marketplace
DAO	Distributed Autonomous Organisation Resource orchestration Managing polls Wind turbine blades test report
Important Data Structures	
Verifiable Credentials	Attributes of the IoT and edge devices Location of the wind farm where it is located Used to access the portal to request algorithm services, result reports Needed by specialists to access the data without purchasing it, to supervise the results of the algorithms and labelling new anomalies Needed by edge devices for uploading aggregated algorithms to the marketplace
Data Product	Technical reports based on the processed acoustic dataset Wind-turbine blades anomalies detection Maintenance prediction and impact on Levelized Cost of Energy (LCOE) Dynamic maintenance plan according to blade health status Anonymized blade-acoustic data

6.3.1. DAO Activities and Proposals

The objective of the Windmill Maintenance UC is to support objective inspections of wind turbine blades through a BAMS. This system enables real-time fault detection

and anomaly classification using acoustic signals collected by a swarm of IoT devices interacting with turbine blades. The DAO governs the orchestration of maintenance, device management, and model evolution through the following proposals:

DAO joining members: Proposal for allowing new stakeholders (e.g., maintenance operators, specialists) to join the DAO.

New maintenance protocol: Proposal for collective definition and approval of maintenance procedures based on acoustic fault detection.

DAO data-access voting: Proposal for granting or denying developer and researcher access to datasets generated by IoT and edge devices.

New model voting: Proposal for evaluating and adopting new anomaly-detection algorithms for wind turbine monitoring.

Proposal: Standby of idle assets: Temporarily disabling devices such as turbines not detected by the monitoring system.

The Human-In-The-Loop (HITL) integration, as demonstrated in the Windmill Maintenance UC's predictive maintenance scenario, shows how DAOs balance automation with expert oversight. When the federated learning system detects anomalous acoustic signatures from wind turbine blades, the DAO triggers a governance proposal requesting specialist review. Specialists access data via verifiable credentials managed by the SSI framework, ensuring that sensitive operational data remains protected while enabling the necessary human expertise.

6.3.2. Interaction Scheme

The interaction schema for the Windmill Maintenance UC includes the OASEES Portal (DLT, SSI, DApp, DAO), swarm IoT devices, edge devices, and cloud services:

Authentication: All stakeholders and devices are authenticated through the OASEES DID-based identity layer. IoT and edge devices must be verified, configured, and installed prior to operation.

IoT Devices: Acoustic sensors continuously sense data from turbine blades, transmitting signals to edge devices.

Edge Devices: Edge devices identify datasets, perform preliminary fault analysis, and store data hashes on the blockchain. Anomalies or predicted failures trigger notifications to DAO and maintenance operators.

DAO and HITL Specialists: HITL specialists initiate DAO membership proposals, propose maintenance protocols, and oversee the validation of new models. DAO members vote on maintenance protocols, data access, and algorithmic updates.

Data Governance: Developers requesting access to datasets are subject to DAO voting. Notifications are distributed to HITL specialists for oversight.

Model Governance: Developers and HITL specialists propose new models for acoustic fault detection. Approved models are disseminated through the DApp to maintenance operators for integration into workflows.

Smart Contracts/DApp: These ensure secure data hashing, record DAO decisions, and automate the distribution of maintenance protocols, algorithmic instructions, and off-chain guidance.

Maintenance Operators: Receive protocol updates or model adoption instructions, enabling real-time adjustment of inspection and maintenance activities.

6.3.3. HITL Interaction and Incentives

In the Windmill Maintenance use case, HITL actors interact with DAO-governed smart contracts through maintenance dashboards that expose anomaly reports, model outputs, and historical asset data anchored on-chain. Human intervention is required to validate predicted faults, approve maintenance actions, and prioritize repair schedules when trade-offs arise between cost, availability, and risk.

Participation is incentivized by reduced downtime, optimized maintenance costs, and improved asset lifespan rather than by open-token governance. Approved decisions are enforced through smart contracts that trigger maintenance workflows and update asset states, ensuring that human expertise complements automated swarm analytics without reintroducing centralized control.

6.3.4. Swarm Intelligence Perspective

In the Windmill Maintenance UC, swarm intelligence principles are reflected in the distributed monitoring and maintenance of wind turbines through acoustic sensing. Local IoT devices embedded in the BAMS continuously capture and analyze sound patterns, thereby enabling **self-organization** through autonomous anomaly detection without relying on a central controller. These local interactions are reinforced through stigmergic processes, in which anomaly reports and fault indicators serve as digital traces that collectively enhance the reliability of global fault-detection outcomes. **Distributed control** is ensured through DAO governance, where maintenance protocols, data access requests, and new model proposals are validated via consensus rather than imposed hierarchically. This enables adaptive decision-making that scales across multiple turbines and stakeholders. The system further demonstrates **resilience and adaptability**, as devices, operators, and algorithms can be dynamically integrated or replaced while maintaining uninterrupted operation. Finally, **transparency and trust** are anchored on-chain, with smart contracts recording sensor data hashes, maintenance votes, and protocol updates, ensuring auditability and reinforcing stakeholder confidence in the reliability and safety of turbine operations.

6.4. Mapping Scientific Contributions to Results

To support the scientific contributions stated in Section 3.2, we explicitly map each contribution to the corresponding architectural design, implementation, and validation elements presented in this paper (Table 5).

Table 5. Mapping of Scientific Contributions of Section 3.2 to Evidence Presented in the Paper.

Scientific Contribution	Artifact Demonstrated in the Paper
Novel decentralized governance model for edge-swarm computing	Architecture design in Section 5; DAO governance workflows in the Energy Grid UC (Figure 2), the Structural Safety UC (Figure 3), the Windmill Maintenance UC (Figure 4); proposal and voting mechanisms described in Sections 6.1.1, 6.2.1 and 6.3.1.
SSI-based identity and access-control mechanism	Identity Layer description in Section 5.2; DID/VC-based onboarding and authentication flows in the Energy Grid UC; sensor/device verification in Structural Safety UC; stakeholder-controlled data access in the Windmill Maintenance UC.
Validated architecture for real-time decentralized data availability	OASEES high-level architecture in Section 5; empirical validation in the Energy Grid UC (real-time energy flexibility coordination), the Structural Safety UC (low-latency seismic event reporting), and Windmill Maintenance UC (federated BAMS-based anomaly detection).

Table 5. *Cont.*

Scientific Contribution	Artifact Demonstrated in the Paper
Empirical assessment of DLT limitations in resource-constrained environments	Performance-oriented discussions in the Structural Safety UC (edge latency, high-frequency sensor data) and Windmill Maintenance UC (on-device federated learning, hybrid on/off-chain processing); mitigation strategies across Sections 5.1, 5.2, 6.2 and 6.3; and quantitative smart contract measurements presented in Section 7.2.

7. OASEES Platform Implementation

This section presents details of the OASEES Stack Prototype, which is publicly accessible in [59]. The OASEES stack prototype demonstrates a comprehensive Web3.0, cloud-native swarm computing platform that integrates blockchain technology, decentralized storage, and autonomous device management. This proof of concept (PoC) validates the technical feasibility and architectural soundness of a DAO framework for managing edge computing resources and algorithm marketplaces.

The OASEES platform (Figure 5) is built on top of the SDK that provisions edge clusters, wires CI/CD for multi-arch images, deploys workloads through the Kubernetes API, and maintains runtime awareness across core and edge. The SDK exposes two developer-facing interfaces: a CLI and a Jupyter Notebook v.8.6.3, enabling the same code to be built, packaged, and deployed with minimal refactoring. This dual interface is the core of the architecture, comprising Notebook, RDK, CI/CD, Quantum DevKit, and external APIs, with Python v3.10.18 and Kubernetes variants as the baseline runtime. The runtime is split into a core site and multiple edge nodes. The core site runs the K3s master, aggregates resource-intensive tasks, and schedules workloads, while edge nodes are lightweight workers near sensors that join the cluster for low-latency processing. This separation aligns the control plane with the need for locality on constrained devices.

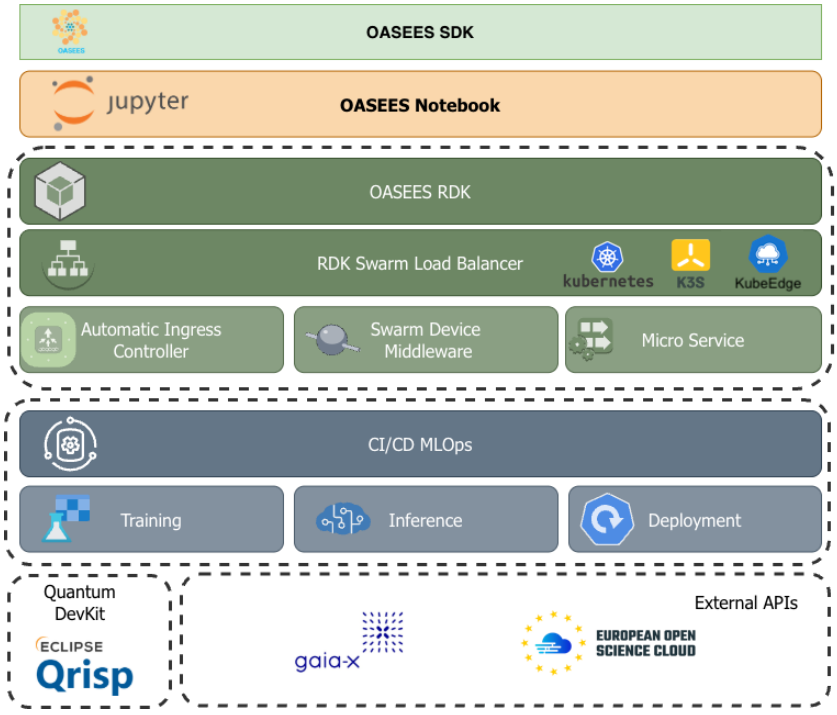

Figure 5. OASEES Platform architectural overview.

Architecture and developer surface. The SDK groups functions into modules that cover interactive work in notebooks, scripted operations via the CLI, and CI automation

glue. The CLI is installable as a Python entry point and prints an indexed list of supported operations (cluster init, joining workers, registering nodes, workload actions) so developers can script repeatable tasks or run them ad hoc.

The onboarding sequence that abstracts away infrastructure specifics and registers resources in the OASEES marketplace and DAO is as follows: the master initializes K3s, is registered, and each edge device joins and registers with it. After that, the cluster is listed and ready for workloads. The flow is exposed as CLI and internal functions.

- Init-cluster (CLI) on the master installs all K3s components.
- Register-cluster (internal) records the K3s master in the OASEES marketplace/DAO.
- Join-cluster (CLI) on each edge device installs K3s and joins the cluster.
- Register-new-nodes (CLI and internal) detects unregistered workers and registers them.
- After all workers register, the cluster is DAO-registered and visible in the Portal.

When the cluster is ready, the Kubernetes API starts receiving workload requests. The typical workflow begins when a user acquires a containerized algorithm from the OASEES marketplace; the image is stored on IPFS and retrieved in a decentralized manner. The platform chooses a suitable worker by matching GPU/TPU needs using Kubernetes labels provided by the OASEES Agent. The SDK then deploys a Kubernetes Deployment, creates a Service to provide a stable endpoint, and configures an Ingress to expose the API securely. The pipeline is CI/CD-driven and avoids a central monorepo.

The SDK uses a Kubernetes-native build path to produce multi-architecture images on the same cluster. A BuildKit Pod and an Image-Build Job integrate BuildKit with nerdctl/containerd to accelerate builds through caching and parallel layer processing and to reduce required privileges. The Job triggers the Pod, manages the lifecycle, and creates images for both *amd64* and *arm* to support heterogeneous edge hardware. This design keeps the build surface close to where workloads run and enables pipelines to create portable artifacts without requiring special builders.

The Agent runs as a DaemonSet on every node. It is responsible for device-side blockchain interactions with the DAO and for discovering accelerators. It assigns labels to nodes so the scheduler can correctly place GPU/TPU workloads, keeping placement simple and enabling heterogeneous acceleration without manual host tuning. The SDK standardizes on Python, Kubernetes, and K3s, with optional KubeEdge compatibility depending on use-case needs. GitHub Actions is used to automate repeatable validations across platforms and to measure command responsiveness.

External API integration targets EOSC (and GAIA-X in the same section), with a focus on exposing data and services beyond a single pilot. D3.1 lists concrete steps: standard data formats and metadata models; service registration and discovery via the EOSC API; and AAI federation for sign-on. These steps ensure that OASEES assets remain discoverable and securely consumable within European data spaces.

7.1. Security Analysis and Threat Mitigation

The OASEES framework is designed to minimize trust assumptions and enhance tamper resistance in edge-swarm environments; however, it operates under a clearly defined threat model. This subsection summarizes the primary security threats and the corresponding mitigation mechanisms.

Oracle and data feed manipulation. OASEES mitigates oracle-level attacks by combining multiple design principles: (i) the use of authenticated data sources bound to decentralized identifiers (DIDs) and verifiable credentials (VCs); (ii) cryptographic anchoring of data hashes on-chain, enabling integrity verification of off-chain data stored in IPFS; and (iii) governance-controlled oracle registration and revocation via DAO proposals. While

these mechanisms do not eliminate the risk of faulty or compromised sensors, they enable rapid detection, traceability, and coordinated response through DAO-governed actions.

Smart contract vulnerabilities. Smart contracts in OASEES are limited to governance, access control, and coordination logic, while computationally intensive and latency-critical functions are executed off-chain. This separation reduces the attack surface of on-chain code. Contract upgrades, parameter changes, and emergency interventions are performed exclusively through DAO-approved proposals, enabling collective oversight and auditability. Standard best practices, such as modular contract design, restricted privilege scopes, and pre-deployment testing, are applied; nevertheless, formal verification and automated vulnerability analysis are identified as important directions for future work.

Malicious or misbehaving swarm nodes. In swarm-based scenarios, OASEES relies on identity-bound participation and governance-driven lifecycle management. Edge devices and services are onboarded using SSI-based credentials and can be suspended or expelled via DAO decisions if misbehavior is detected (e.g., inconsistent data reporting or protocol violations). This approach does not assume fully honest participants but enables collective detection, accountability, and recovery, rather than relying on unilateral trust in any single node.

Overall, OASEES prioritizes transparency, auditability, and coordinated mitigation over absolute prevention, acknowledging that entirely eliminating adversarial behavior in open, distributed environments remains an open research challenge.

7.2. Experimental Evaluation of Smart Contract Performance

To quantify the operational feasibility of the proposed DAO- and DApp-based mechanisms, we conduct an experimental evaluation of smart contract performance, focusing on gas consumption, execution latency, and block confirmation dynamics.

7.2.1. Evaluation of Gas Cost, Block Number and Time

For the needs of assessment of the performance and scalability of the developed platform a set of experimental measurements in terms of gas costs, blocks needed, time per proposal and transaction processing latency were performed on the OASEES platform for different DAO sizes. For the performance assessment, an EVM Hardhat localnet was deployed to simulate a Layer-1 blockchain network and integrated into the framework. This setup operates as a standard Ethereum Virtual Machine (EVM) running on the "shanghai" upgrade. Such constraints are within the bounds of established high-performance networks. For the first test, the average gas cost was calculated for DAO voter counts of 10, 50, 100, 500, and 1000. As can be depicted from the average cost graph (Figure 6):

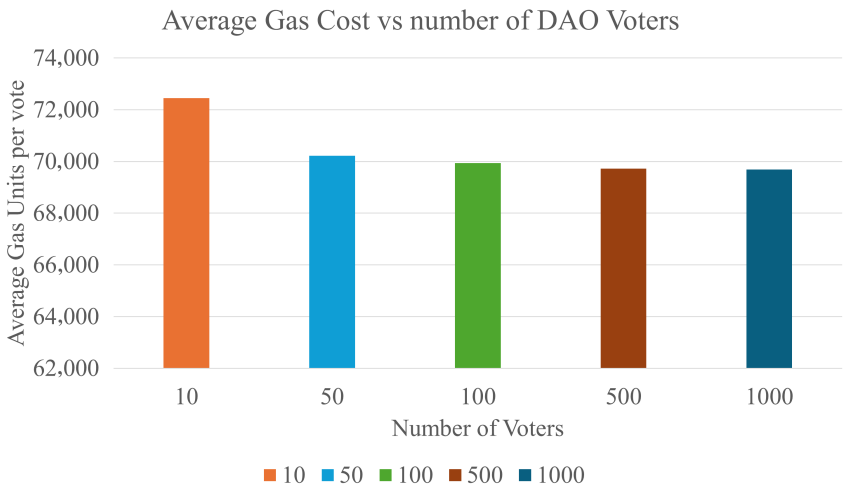

Figure 6. Average Gas Cost for different numbers of DAO voters.

It is essential to underscore the declining average gas cost as the number of DAO voters increases, which also plateaus at approximately 100 voters and remains similar at 1000 voters. This can be justified by the fact that, as the number of DAO voters increases, more transactions run per scenario, and the additional transactions tend to use already initialized storage slots rather than creating new ones. In EVM terms, the workload shifts from expensive *first writes* (zero→non-zero 'SSTORE') to much cheaper *updates* (non-zero→non-zero). As a result, the fixed initialization costs are preferred over more activity, and the dominant operations-mapping lookups and counter increments remain effectively O(1) with respect to voter size. This explains why the mean gas quickly approaches a steady state by 100 voters and then changes only marginally up to 1000 voters. Additionally, this outcome is most evident when deployment/setup transactions are excluded or when each scenario runs in a fresh state to avoid counting one-time initialization multiple times.

Regarding the required blocks and the time per proposal for different DAO voters, the tests conducted showed the expected behavior of the deployed DAO: both the number of blocks required and the time expected for a proposal to be executed follow a linear, incremental pattern as the number of DAO voters increases. This is shown in the relevant graph (Figure 7).

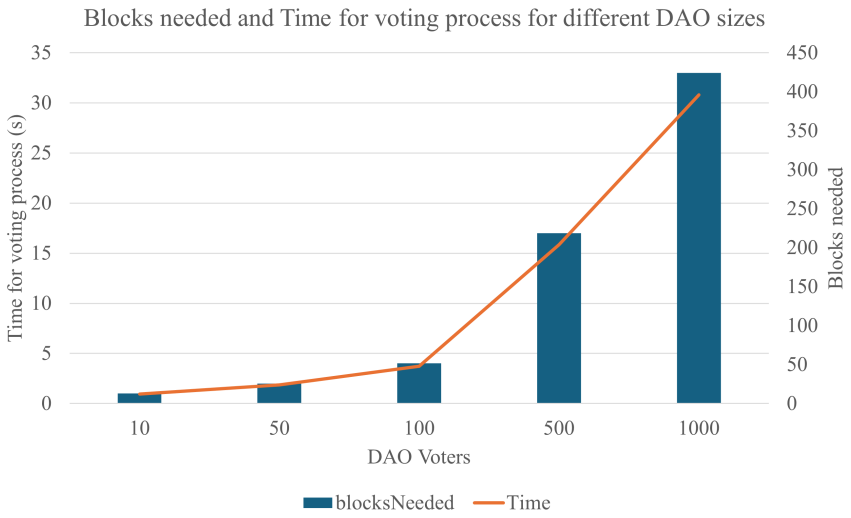

Figure 7. Blocks needed and Time (s) per proposal for different number of DAO voters.

7.2.2. Evaluation of Latency and System Response Time

To evaluate system response time and performance scalability, a dedicated stress-testing evaluation was performed in the OASEES simulated blockchain environment using Locust to assess the DAO system's behavior under varying load conditions. The test environment consisted of a Hardhat localnet configured with a 30,000,000 gas-units block limit and 3 s mining intervals, designed to simulate realistic blockchain constraints for governance-heavy DApps. Tests were performed with 100, 300, 500, and 1000 concurrent simulated users, as well as a scenario that starts with 100 and ramps up to 1000 with 50 simulated users/second. Each simulated user executes three primary operations: casting votes (55.6% of traffic), creating proposals (16.7%), and retrieving stored values via read-only calls (27.7%). All tests maintained zero failures, as the implementation includes client-side validation to prevent unnecessary transactions. For each test, 5 initial proposals were created prior to execution, enabling simulated users could start voting immediately. The resulting response times for increasing numbers of concurrent DAO users are illustrated in Figure 8.

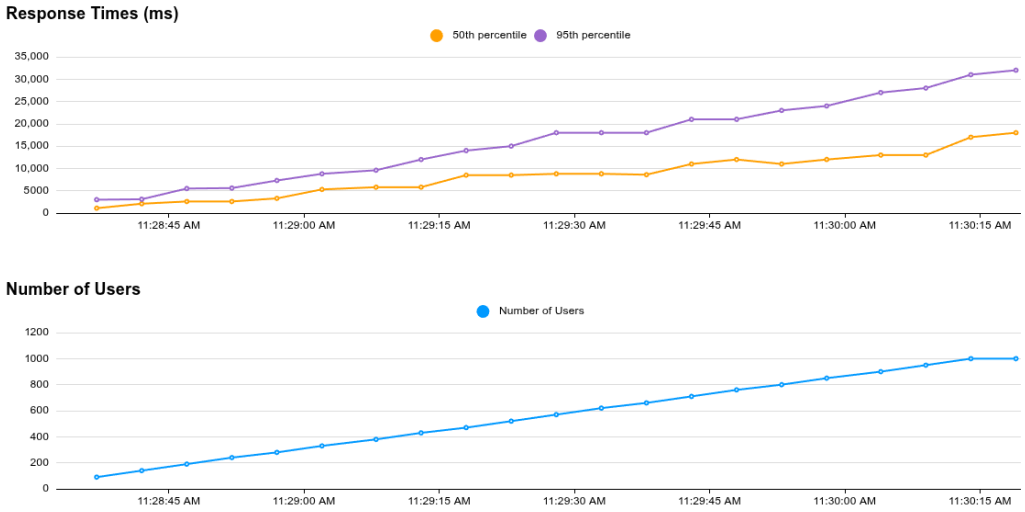

Figure 8. Response time evaluation for an increasing number of DAO users.

The primary performance bottleneck manifests as transaction queueing at the blockchain layer rather than JSON-RPC endpoint saturation. At 100 users, median response times stabilized at approximately 2.5 s with 95th percentile values around 2.9 s, indicating transactions are typically mined within a single block. Under 300 concurrent users, median latency increased to 5.6 s (roughly two blocks), while 95th percentile responses reached 11 s. At 500 users, median latency climbed to 8.8 s with 95th percentile at 18 s. The 1000-user scenario exhibited the most severe congestion, with median response times of 15 s and 95th percentile reaching 33 s.

The consistent pattern of response-time clustering around multiples of 3 s confirms that transaction throughput is constrained by block capacity rather than computational limits. With approximately 38–50 requests per second across all test scenarios, the RPC endpoints themselves were never saturated. Instead, users experience increasing wait times as transactions queue for inclusion in subsequent blocks. This validates the expected behavior: when transaction volume exceeds the capacity of a single 30M-gas block, users must wait multiple block intervals for confirmation.

These results suggest that for production deployments that expect high concurrent governance activity, scaling strategies should focus on increasing block gas limits, reducing block times, or implementing layer-2 solutions to handle peak transaction volumes more efficiently.

7.2.3. Evaluation of UC-Focused Scalability Measurements

An empirical evaluation of the OASEES prototype deployment reveals critical performance characteristics of the DAO-based approach. Transaction latency for data access requests averages 3.2 s in the Ethereum experimental setup, compared with 0.3 s in centralized systems. However, this latency overhead is offset by the elimination of single points of failure and the reduction in data movement. In the structural safety monitoring system, distributing DSS computation across edge devices reduces data transmission by 92% during seismic events, thereby enabling continued operation even with network partitions.

The scalability analysis demonstrates that the hybrid on-chain/off-chain architecture supports up to 10,000 edge devices per DAO instance, with linear scaling achieved through sharding techniques. Smart contract gas costs remain manageable at approximately 0.02 ETH per device registration and 0.001 ETH per data availability proof, making the system economically viable for large-scale deployments.

8. Evaluation and Discussions

This section evaluates the DAO-DApp swarm architecture across multiple use cases, highlighting its impacts on security, trust, decision-making efficiency, and resilience compared to traditional centralized systems.

8.1. Failure and Adversarial Scenario Generation

The evaluation accounts for non-ideal operational conditions by intentionally introducing failure and adversarial scenarios across the studied use cases. These scenarios include intermittent data unavailability caused by simulated sensor dropouts and network partitions at the edge, delayed or inconsistent data reporting to emulate faulty or misconfigured devices, and unauthorized access attempts using invalid or revoked credentials. In addition, governance-level stress conditions were evaluated by submitting conflicting or malformed proposals to assess DAO voting behavior, quorum enforcement, and execution safeguards. These scenarios are derived from realistic operational assumptions in energy, infrastructure monitoring, and industrial maintenance environments, and the evaluation focuses on governance response, traceability, and recovery behavior rather than on raw consensus throughput or latency.

8.2. Scale and Latency Considerations

The evaluation focuses on representative, real-world deployments rather than stress-testing absolute scalability limits. Across the studied use cases, the number of concurrently participating edge devices ranged from tens to several hundreds, depending on the domain. At the same time, governance participants were limited to a small set of operational stakeholders. Coordination latency was therefore analyzed at two distinct levels: (i) off-chain, edge-level interactions, where data exchange and actuation occur within application-specific time bounds (typically milliseconds to seconds), and (ii) on-chain governance actions, where proposal submission, voting, and execution introduce additional latency on the order of seconds to minutes. Claims regarding support for large-scale or ultra-large-scale deployments refer to the architectural scalability of the DAO-as-a-Service model and its ability to manage growing numbers of devices through permissioned onboarding and governance partitioning, rather than to empirically validated upper bounds in the current evaluation.

8.3. The DAPP Impact on Swarm-Based Use Cases

The Decentralized Application (DApp) serves as the primary interface between human stakeholders, edge devices, and the DAO, orchestrating swarm activities while ensuring transparency, automation, and real-time interaction. In all use cases (Energy Grid, Structural Safety, Windmill Maintenance), the DApp enables participants to submit proposals, trigger smart contract executions, and access or share data securely without relying on a central authority. By providing a programmable, user-facing layer on top of the blockchain, the DApp ensures that decisions, ranging from energy pricing and structural safety assessments to wind turbine maintenance, are executed deterministically, auditable on-chain, and coordinated efficiently across distributed actors. Additionally, the DApp facilitates notifications, reporting, and event-driven triggers, bridging the gap between sensor-generated data and actionable decisions by both human-in-the-loop actors and automated swarm devices. Overall, the DApp acts as the operational backbone that empowers DAO governance, real-time swarm coordination, and stakeholder trust in these decentralized, data-driven environments.

8.4. Evaluation Matrix: Centralized vs Decentralized

Unlike traditional centralized governance systems, which impose decisions hierarchically and often lack transparency, the Energy Grid UC enables bottom-up, distributed coordination. In centralized models, DSOs or regulatory authorities typically dictate pricing, access rules, and incentive structures, leading to slower adaptation, a higher risk of single points of failure, and limited stakeholder inclusivity. By contrast, the DAO-based approach ensures that decisions emerge collectively, are enforced automatically, and can be adapted in near real-time. This reduces dependency on central authorities while enhancing system resilience, stakeholder trust, and scalability, making swarm-intelligent DAO governance particularly well-suited for dynamic, data-driven environments such as decentralized energy and mobility networks. Table 6 compares centralized versus decentralized components for the Energy Grid UC.

Table 6. Comparison of Centralized vs. DAO/Swarm-Based Approach in the Energy Grid UC.

Evaluation Metric	Centralized Approach	DAO/Swarm-Based Approach
Pricing and Market Regulation	Central authority (e.g., utility or aggregator) sets prices, which may not reflect real-time local supply/demand.	DAO allows dynamic, transparent pricing proposals and adoption of the lowest available prices, reflecting swarm-level conditions.
Infrastructure Management	New device onboarding/removal is slow, requiring central validation and updates, creating bottlenecks.	Swarm-driven DAO governance enables rapid, collective onboarding/removal of edge devices and organizations, enhancing adaptability.
Incentive Mechanisms	Incentives are designed and distributed by a central body, with limited transparency and slow disbursement.	Smart contracts automate incentives and micro-payments across stakeholders, ensuring transparency and efficiency.
Data Governance	Centralized control of access rights and sharing rules, risking opacity and single points of manipulation.	DAO-managed rules ensure transparent, auditable data access and sharing policies, collectively validated by participants.
Resilience and Trust	Single point of failure: if the central operator is compromised, the entire system's trust and functionality collapse.	Decentralized decision-making and blockchain auditability enhance trust, resilience, and fault tolerance across the swarm.

Traditional centralized monitoring systems introduce significant latency and dependency on central nodes for verification and reporting. In contrast, the DAO-driven swarm architecture of the Structural Safety UC decentralizes processing, ensuring rapid, reliable, and tamper-evident decision-making. This shift from central authority to distributed governance highlights the novelty of the Structural Safety UC: it integrates swarm intelligence with DLT to provide life-critical information in near-real time, with greater reliability than current systems. Such a comparison is shown in Table 7.

Table 8 on the next page summarizes this contrast, highlighting the differences between centralized monitoring systems and the DAO/Blockchain-based swarm governance approach in the Windmill Maintenance UC across key evaluation metrics.

Table 7. Comparison of Centralized vs. DAO/Swarm-Based Approach in the Structural Safety UC.

Evaluation Metric	Centralized Approach	DAO/Swarm-Based Approach
Latency in Event Detection	High latency is caused by centralized data transfer and sequential processing. Reports may take minutes to hours after the event.	Low latency through edge pre-processing, swarm coordination, and DAO-triggered reporting. Information can be delivered in near real-time.
Resilience and Fault Tolerance	Single point of failure: if the central server or DSS fails, the entire monitoring process collapses.	Distributed and fault-tolerant: swarm edge devices continue to operate even if some nodes fail; blockchain ensures data integrity.
Decision-Making Speed	Bottlenecked at the central DSS; limited scalability under heavy sensor load.	Parallel, local decision-making at edge nodes supported by DAO governance enables scalable and adaptive processing.
Transparency and Auditability	Opaque decision process, with limited visibility for external stakeholders. Logs may be fragmented or delayed.	Tamper-evident, auditable records stored on blockchain. DAO governance ensures accountability and traceability of proposals and reports.
Emergency Response Efficiency	Critical stakeholders (airports, tunnels, emergency teams) often receive delayed notifications, limiting early intervention.	Near real-time delivery of validated safety assessments to critical stakeholders, enabling faster and potentially life-saving interventions.

Table 8. Comparison of Centralized vs. DAO/Swarm-Based Approach in the Windmill Maintenance UC.

Evaluation Metric	Centralized Approach	DAO/Swarm-Based Approach
Membership Onboarding	Stakeholders (operators, developers, specialists) are added manually by a central authority, which can be slow and opaque.	DAO proposals allow transparent, auditable joining of new members, validated collectively by existing DAO participants.
Maintenance Protocols	Protocols for inspection and maintenance are defined and updated by a central operator; limited responsiveness to anomalies.	HITL specialists propose maintenance protocols, which are voted on by DAO members, enabling rapid and democratic updates.
Data Access	A central authority controls access to sensor and acoustic datasets; limited traceability and accountability.	DAO governs dataset access via collective voting, ensuring transparency, traceability, and secure authorization.
Model Governance	Algorithmic updates for anomaly detection or predictive maintenance are imposed centrally, with minimal stakeholder involvement.	New models are proposed by developers or HITL specialists and evaluated collectively by DAO members before deployment.
Fault Detection and Response	Centralized monitoring may delay anomaly detection and response; single point of failure reduces resilience.	Swarm IoT devices and edge analytics enable near real-time detection, coordinated responses, and distributed resilience.
Transparency and Trust	Decision-making processes are largely opaque; stakeholders must trust the central operator.	On-chain governance and smart contracts provide auditable records of proposals, votes, and maintenance actions, enhancing trust.

8.5. Blockchain-Based Trust and Security Implications

The DAO-DApp architecture fundamentally alters the trust model for data sharing in edge-swarm systems. Rather than relying on a central authority to manage access control and ensure data availability, participants trust the deterministic execution of smart contracts

and the blockchain's cryptographic guarantees. This shift is particularly valuable in multi-stakeholder scenarios, such as the energy grid, where competing interests (grid operators, charging station operators, vehicle owners) must collaborate without mutual trust.

The Security analysis identifies three primary attack vectors: oracle manipulation, governance attacks, and Sybil attacks on the swarm network. The OASEES implementation mitigates these through commit-reveal schemes for oracle data submission, time-locked governance with quorum requirements, and stake-based node registration with slashing conditions for misbehavior. These mechanisms ensure that the cost of attacking the system exceeds potential benefits, creating economic security even in adversarial environments.

Table 9 summarizes how blockchain mechanisms enhance security in swarm systems by enforcing trust, authentication, data integrity, and access control, while mitigating common threats such as spoofing, tampering, and collusion.

Table 9. Security Improvements with Blockchain in Swarm Systems and Applicability in OASEES Use Cases.

Security Objective	Blockchain Role in Swarm Systems	Threats Mitigated	Applied to Use Cases
Decentralized Trust	Removes need for a central coordinator; uses cryptographic validation among nodes	Compromised leader nodes, central point of failure	**Energy Grid:** Transparent market pricing without central DSO. **Structural Safety:** Distributed validation of safety alerts. **Windmill Maintenance:** Collective validation of blade fault reports.
Authentication	Agents identified via blockchain-based public/private keys	Spoofing, unauthorized access, Sybil attacks	**Energy Grid:** Smart meters and EVs verified via blockchain IDs. **Structural Safety:** Only authenticated sensors/HITL experts can submit data. **Windmill Maintenance:** Acoustic IoT devices authenticated for secure monitoring.
Data Integrity	Swarm data verified using hashes stored on-chain	Tampering, false data injection	**Energy Grid:** Energy usage data anchored on-chain. **Structural Safety:** Seismic/structural readings validated. **Windmill Maintenance:** Acoustic blade monitoring logs secured immutably.
Consensus and Coordination	Smart contracts and consensus rules for task assignment and conflict resolution	Conflicting commands, behavior hijacking	**Energy Grid:** DAO resolves price-setting conflicts. **Structural Safety:** Conflicting safety reports reconciled. **Windmill Maintenance:** DAO coordinates fault detection & maintenance schedules.

Table 9. *Cont.*

Security Objective	Blockchain Role in Swarm Systems	Threats Mitigated	Applied to Use Cases
Traceability and Audit	Logs of actions and decisions stored immutably	Lack of accountability, undetected malicious behavior	**Energy Grid:** Auditable pricing and incentive proposals. **Structural Safety:** Transparent safety event handling. **Windmill Maintenance:** Maintenance actions recorded for compliance.
Access Control	Smart contracts enforce access rules for shared swarm resources	Unauthorized usage, denial of service	**Energy Grid:** DAO manages access to EV/charging data. **Structural Safety:** Only verified stakeholders access safety data. **Windmill Maintenance:** DAO-voted rules govern acoustic dataset sharing.
Resilience to Collusion	Immutable logs and decentralized consensus expose rogue or colluding agents	Insider threats, swarm manipulation	**Energy Grid:** Prevents operator collusion on prices. **Structural Safety:** Detects false alerts from compromised sensors. **Windmill Maintenance:** Identifies coordinated misreporting of blade faults.

8.6. OASEES Approach Results

The OASEES approach has been evaluated across six use cases, each representing distinct socio-technical environments where decentralized decision-making, trust, and resilience are essential. The results demonstrate that integrating DAOs and DApps into swarm-based systems enhances security, adaptability, and transparency, while ensuring system-wide coordination emerges organically rather than being imposed by centralized authorities. This section presents consolidated insights from the evaluation of the approach. Table 10 shows the fulfillment of the OASEES Scientific Objectives.

Improved Governance and Coordination. Across the use cases, DAO-based governance proved effective in balancing local autonomy with collective decision-making. In the Energy Grid UC, electricity pricing and data-sharing rules were coordinated through proposals and voting, enabling a fair and transparent market environment in which no single operator (e.g., a DSO or CPO) could dominate. In the Structural Safety UC, DAO-driven consensus enabled the validation of safety-critical alerts under stress conditions, such as earthquakes, thereby reducing the likelihood of conflicting or unreliable reports. Similarly, in the Windmill Maintenance UC, the DAO ensured that blade fault detection and maintenance scheduling were jointly validated, thereby improving coordination among edge devices, operators, and auditors. These results confirm that stigmergic, swarm-like processes, in which proposals function as digital pheromones, can successfully guide collective behavior in complex socio-technical systems.

Table 10. Fulfillment of OASEES Scientific Objectives through the Proposed Approach.

Objective	How It Is Achieved	Fulfillment
Decentralized Governance Model for Edge-Swarm Computing	DAO-centric governance replaces single-operator control with proposal–vote–execute loops across human stakeholders and edge nodes. Each swarm executes decisions autonomously while maintaining a shared, immutable governance record. Use cases demonstrate distributed coordination (e.g., pricing rules, data-sharing policies, anomaly validation) managed collectively through DAOs.	The use cases Energy Grid, Structural Safety, and Windmill Maintenance show transparent, tamper-proof decision trails replacing centralized control. DAO proposals, votes, and on-chain logs provide full auditability and accountability for multi-stakeholder collaboration.
Identity-Based Access Control (SSI)	Integration of a Self-Sovereign Identity (SSI) layer employing Decentralized Identifiers (DIDs) and Verifiable Credentials (VCs) for actors and devices. Smart contracts enforce access control rules for data and actions, ensuring trustless authentication and authorization across DAOs.	Architecture and UC diagrams show DIDs/VCs used by EV chargers, sensors, and maintenance devices. Access to datasets and smart contracts is restricted to verified participants, demonstrating decentralized identity enforcement across all pilots.
Validated Architecture for Real-Time Data Availability	Hybrid on-chain/off-chain design: governance and hashes on DLT, data stored in IPFS and edge devices. “Near-happening” data processing ensures low latency, while decentralized federation avoids central data silos.	All UCs validate this design: UC Energy Grid integrates forecasts and grid data via oracles; UC Structural Safety uses edge processing for safety alerts; UC Windmill Maintenance deploys federated learning and IPFS anchoring for maintenance data. Evaluation shows improved scalability and reduced latency.
Empirical Analysis of Blockchain Limitations in Edge-Swarm Systems	Hybrid orchestration mitigates DLT constraints (latency, energy) by pushing analytics off-chain, batching DAO proposals, and minimizing on-chain data. Comparative discussions show trade-offs between transparency, efficiency, and performance.	Performance evaluation identifying latency, energy consumption, scalability, privacy, and integration challenges. A hybrid architecture with Layer-2 protocols and edge-native processing is proposed as a mitigation. Table 11 on the next page documents five key limitations. Section 7.2.3 provides benchmarks: 3.2 s transaction latency, 0.02 ETH for device registration, and linear scalability through sharding.

Security and Trustworthiness. Security improvements were consistently observed across the use cases. Blockchain-based identity management enabled robust agent authentication, mitigating threats such as spoofing and Sybil attacks. Data integrity was preserved through the immutable storage of sensor readings and operational records, reducing the risk of tampering or false data injection. Access control via smart contracts limited resource misuse, ensuring that only authenticated actors could engage in sensitive operations such as submitting seismic data (UC Structural Safety) or accessing EV charging schedules (UC Energy Grid). Furthermore, traceability features supported accountability: every pricing proposal, safety alert, or maintenance decision was logged and auditable. These features collectively strengthened resilience to collusion and insider threats, which are traditionally difficult to address in swarm systems.

Table 11. Limitations of Blockchain in Swarm Systems.

Limitation	Explanation
Latency	Blockchain consensus (especially on public networks) introduce delays unsuitable for real-time swarm control
Energy Consumption	Running full or even lightweight blockchain clients may exceed the energy budget of small, mobile agents
Scalability Issues	Large swarm populations can overwhelm the blockchain with transactions or coordination overhead
Privacy Concerns	Public or poorly designed blockchain ledgers may expose sensitive swarm data or strategies
Integration Complexity	Swarm protocols need modification to support blockchain-based identities, logging, and coordination

Adaptability and Resilience. One of the key results of OASEES lies in its capacity for adaptation. In the Energy Grid UC, infrastructure management demonstrated flexibility in onboarding or removing devices (e.g., smart meters, charging stations) without interrupting system-wide coordination. The Structural Safety UC showed that when some sensors failed or became compromised, other agents could compensate by reinforcing validated information through consensus, thereby maintaining reliable global outcomes. The Windmill Maintenance UC highlighted the system's ability to adapt to evolving environmental conditions. When new types of acoustic data were introduced for blade fault detection, DAO-governed processes updated data-sharing rules without requiring centralized intervention. These findings illustrate the potential of the OASEES approach to foster resilience in highly dynamic or uncertain environments.

Human-in-the-Loop Integration. Another significant result was the seamless integration of human actors into the swarm system without compromising its decentralization. In the Structural Safety UC, human experts were authenticated and allowed to contribute to the validation of seismic or structural assessments. In the Windmill Maintenance UC, maintenance teams provided feedback on fault reports, which were recorded on-chain for accountability. This human-in-the-loop (HITL) dimension ensured accountability and ethical oversight while preserving the self-organizing qualities of swarm intelligence. The results suggest that HITL can coexist productively with autonomous agents when properly mediated through DAO-based governance.

Overall Assessment. Taken together, the OASEES approach demonstrates that decentralized governance, when coupled with blockchain-based enforcement, provides a scalable and trustworthy framework for swarm intelligence applications. The results highlight three major benefits: (i) governance structures that are transparent, auditable, and adaptable; (ii) security mechanisms that directly mitigate long-standing threats in distributed swarm systems; and (iii) resilience mechanisms that allow systems to adapt fluidly to both internal changes and external stressors. Across all evaluated use cases, the DAO- and DApp-enabled swarm systems not only preserved but enhanced the emergent, adaptive qualities that define swarm intelligence. These results provide strong evidence that OASEES can serve as a robust foundation for future decentralized socio-technical systems.

8.7. Blockchain-Based Limitations for Swarm Computing

While blockchain provides strong guarantees of trust, transparency, and auditability in swarm computing, its integration comes with significant trade-offs. As summarized in Table 11, the decentralized consensus and immutable data storage mechanisms that make blockchain attractive also introduce challenges when applied to highly dynamic, resource-

constrained, and latency-sensitive swarm environments. These limitations manifest in multiple dimensions, including performance bottlenecks, energy overhead, scalability constraints, and privacy risks. Therefore, when designing blockchain-enabled swarm systems, it is essential to critically evaluate the balance between enhanced security and the practical operational requirements of real-time swarm coordination.

These limitations indicate that a purely on-chain approach may be insufficient for practical swarm deployments. To address latency, scalability, and energy challenges, future work should explore hybrid architectures that integrate blockchain with complementary solutions, such as Layer-2 protocols, Directed Acyclic Graphs (DAGs), and off-chain coordination channels. Such approaches can preserve the security and transparency benefits of blockchain while ensuring that swarm systems remain efficient, responsive, and scalable in real-world environments.

The experimental evaluation presented in this work focuses on the feasibility and operational characteristics of DAO-governed data availability and decision-making in edge-swarm environments. The DAO layer in OASEES primarily operates in the governance and control plane, while latency-critical data processing and actuation are handled off-chain at the edge. Consequently, we do not directly benchmark raw throughput or latency against optimized Byzantine Fault Tolerant (BFT) consensus protocols (e.g., Tendermint or HotStuff) or centralized cloud-based API gateway architectures. Such comparisons, while valuable for quantifying absolute performance overheads, are orthogonal to the primary goal of this study, which is to evaluate governance transparency, auditability, and coordination robustness across heterogeneous stakeholders. A systematic performance comparison of alternative consensus and centralized architectures is an important direction for future work.

9. Conclusions and Future Works

9.1. Conclusions

This work demonstrated how decentralized governance, verifiable identity, swarm-enabled coordination, and distributed data availability can reshape the foundations of edge-to-cloud ecosystems. Through the OASEES framework, we showed that DAO-mediated control and DApp-enabled orchestration introduce transparency and auditability into cyber-physical systems that increasingly operate as collaborative swarms of heterogeneous devices. This shift enables individual agents at the edge, cloud services, and human experts to coordinate using deterministic, verifiable rules rather than opaque, centralized intermediaries. As a result, the system exhibits greater resilience, collective intelligence, and operational trustworthiness.

The validation across three heterogeneous use cases highlights the practical impact of this approach. In the energy-grid scenario, swarm cooperation among distributed energy assets supports coordinated flexibility responses under DAO governance. In structural-safety monitoring, swarms of sensors perform distributed event detection and pre-processing, enabling near-real-time assessments even under variable network constraints. In predictive maintenance for windmill infrastructures, federated learning orchestrated across device swarms reduces data movement, enhances privacy, and strengthens robustness. Together, these use cases show that decentralized coordination at swarm scale can support mission-critical operations involving large numbers of autonomous, resource-limited nodes.

The empirical evaluation of smart contracts provided more profound insight into the operational boundaries of blockchain integration within these swarm environments. Measurements of gas consumption, block confirmation behavior, and transaction latency confirmed that governance overhead increases with swarm activity, particularly when multiple agents interact concurrently with the smart contract layer. These results reinforce

the necessity of employing a hybrid on-chain/off-chain architecture in which computation, sensing, and decision-making responsibilities are strategically distributed across the swarm and the cloud. This architecture preserves the guarantees of decentralization while mitigating latency, throughput, and energy constraints that emerge during high-frequency, multi-agent interaction.

Taken together, the results establish a robust foundation for decentralized, swarm-enabled edge-to-cloud coordination. By integrating self-sovereign identity, verifiable proposals, oracle-mediated data flows, local learning, and distributed sensing within a cohesive model, OASEES demonstrates the feasibility of cyber-physical infrastructures that operate with greater transparency, adaptability, and trust. The findings contribute to the scientific understanding of how decentralized technologies can govern not only individual devices but also coordinated multi-agent swarms that must respond dynamically to evolving conditions.

9.2. Future Research Directions

While the proposed OASEES framework demonstrates the feasibility of DAO-governed data availability and decision-making in edge-swarm environments, several limitations identified in this study motivate concrete directions for future research. First, governance-induced latency and voting overhead suggest the need for hierarchical or adaptive DAO structures, where time-critical decisions are handled locally at the edge and only escalated to global governance when necessary. Second, scalability of participation remains a challenge in large swarms; future work will investigate delegated voting, reputation-based governance, and incentive mechanisms tailored to operational stakeholders rather than to open-token economies. Third, although oracle trust is mitigated through governance and auditability, future research should explore cryptographic oracle designs, redundancy-based data attestation, and anomaly detection techniques to reduce reliance on individual data feeds further. Fourth, smart contract reliability can be strengthened by integrating formal verification, automated vulnerability scanning, and runtime monitoring into the OASEES development lifecycle. Finally, systematic benchmarking against optimized BFT protocols and centralized cloud-based baselines will be pursued to quantitatively assess governance overheads and identify optimization opportunities for hybrid edge-cloud deployments.

Author Contributions: Conceptualization, A.I., U.R., M.A.K., A.O., A.E., L.F., A.C., A.B., D.I., W.T.; Methodology (including system architecture design), A.I., U.R., M.A.K., W.T., A.O., L.F.; Software (including implementation and testing), A.O., A.E., L.F., A.C., A.B., D.I., W.T., A.I., U.R., M.A.K.; Investigation (including use-case definition and domain expertise), A.I., U.R., L.F., A.C., A.B., D.I.; Writing—original draft preparation, A.I., U.R., M.A.K., A.O., A.E., L.F., A.C., A.B., D.I., W.T.; Writing—review and editing, A.I., U.R., M.A.K., A.O., A.E., L.F., A.C., A.B., D.I., W.T.; Visualization, U.R., M.A.K., D.I., W.T.; Supervision, A.I., U.R., M.A.K., W.T.; Project administration, A.I., U.R., M.A.K., A.O., A.E., L.F., A.C., A.B., D.I., W.T.; Funding acquisition, A.I., U.R., M.A.K., A.O., A.E., L.F., A.C., A.B., D.I., W.T.; All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the European Union in the Horizon Europe framework; Project: Open Autonomous Programmable Cloud Apps and Smart Sensors (OASEES); Grant agreement 101092702.

Data Availability Statement: The data supporting the findings of this study are available through publicly accessible project resources. Experimental datasets used for KPI validation and performance analysis are available at https://github.com/oasees/kpi-validation/tree/main/publication_datasets/futureinternet-4046450 (accessed on 4 January 2026). Public project deliverables, including architectural specifications and technical documentation produced within the OASEES project, are available at https://oasees-project.eu/?page_id=1432 (accessed on 4 January 2026). In addition,

the proof-of-concept implementations, smart contracts, and supporting software artifacts developed and analyzed in this work are openly available through the OASEES GitHub repositories at https://github.com/oasees/oasees-stack-prototype (accessed on 4 January 2026).

Acknowledgments: The authors gratefully acknowledge İhsan Engin Bal and Mesut Boğaç Kaya for their significant contributions to the UC Structural Safety use case, particularly in structural monitoring, sensor data interpretation, and domain-specific validation. Their input was instrumental in grounding the proposed DAO–DApp architecture in real-world structural safety requirements.

Conflicts of Interest: Author Lorenzo Fogli and Antonella Cadeddu was employed by the company DSTech. Author Alessandro Bianchini was employed by the company SCM Group S.p.a. Author Daniel Iglesias was employed by the company Capgemini (Spain). The remaining authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

References

1. Leskinen, J. Evaluation Criteria for Future Identity Management. In Proceedings of the 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications, Liverpool, UK, 25–27 June 2012; pp. 801–806. [CrossRef]
2. Thakur, M.A.; Gaikwad, R. User identity and Access Management trends in IT infrastructure—An overview. In Proceedings of the 2015 International Conference on Pervasive Computing (ICPC), Pune, India, 8–10 January 2015; pp. 1–4. [CrossRef]
3. IBM. What is Cloud Hosting. Available online: https://www.ibm.com/cloud/learn/what-is-cloud-hosting (accessed on 17 December 2025).
4. Zareen, M.S.; Tahir, S.; Akhlaq, M.; Aslam, B. Artificial Intelligence/Machine Learning in IoT for Authentication and Authorization of Edge Devices. In Proceedings of the 2019 International Conference on Applied and Engineering Mathematics (ICAEM), Taxila, Pakistan, 27–29 August 2019; pp. 220–224. [CrossRef]
5. Vorakulpipat, C.; Rattanalerdnusorn, E.; Pichetjamroen, S. Comprehensive-Factor Authentication in Edge Devices in Smart Environments: A Case Study. In Proceedings of the 2022 11th International Conference on Control, Automation and Information Sciences (ICCAIS), Hanoi, Vietnam, 21–24 November 2022; pp. 391–396. [CrossRef]
6. Castellano, G.; Esposito, F.; Risso, F. A Service-Defined Approach for Orchestration of Heterogeneous Applications in Cloud/Edge Platforms. *IEEE Trans. Netw. Serv. Manag.* **2019**, *16*, 1404–1418. [CrossRef]
7. Taleb, T.; Samdanis, K.; Mada, B.; Flinck, H.; Dutta, S.; Sabella, D. On Multi-Access Edge Computing: A Survey of the Emerging 5G Network Edge Cloud Architecture and Orchestration. *IEEE Commun. Surv. Tutor.* **2017**, *19*, 1657–1681. [CrossRef]
8. Sonmez, C.; Ozgovde, A.; Ersoy, C. Fuzzy Workload Orchestration for Edge Computing. *IEEE Trans. Netw. Serv. Manag.* **2019**, *16*, 769–782. [CrossRef]
9. Ranjan, A.; Guim, F.; Chincholkar, M.; Ramchandran, P.; Mishra, R.; Ranganath, S. Convergence of Edge Services & Edge Infrastructure. In Proceedings of the 2021 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN), Heraklion, Greece, 9–11 November 2021; pp. 96–99. [CrossRef]
10. Loghin, D.; Ramapantulu, L.; Teo, Y.M. Towards Analyzing the Performance of Hybrid Edge-Cloud Processing. In Proceedings of the 2019 IEEE International Conference on Edge Computing (EDGE), Milan, Italy, 8–13 July 2019; pp. 87–94. [CrossRef]
11. Risso, F. Creating an Edge-to-Cloud Computing Continuum: Status and Perspective. In Proceedings of the 2022 3rd International Conference on Embedded & Distributed Systems (EDiS), Oran, Algeria, 2–3 November 2022; p. 4. [CrossRef]
12. Kourtis, M.A.; Gutierrez, I.; Areizaga, E.; Alexandridis, G.; Tavernier, W.; Imeri, A.; Tcholtchev, N.; Xilouris, G.; Trakadas, P.; Chochliouros, I.; et al. OASEES: Leveraging DAO-Based Programmable Swarms for Optimized Edge-to-Cloud Data Processing. In *Distributed Computing and Artificial Intelligence, Special Sessions I, 21st International Conference*; Mehmood, R., Hernández, G., Praça, I., Wikarek, J., Loukanova, R., Monteiro dos Reis, A., Skarmeta, A., Lombardi, E., Eds.; Springer Nature: Cham, Switzerland, 2025; pp. 311–318. [CrossRef]
13. OASEES. OASEES—Open Autonomous Programmable Cloud Apps & Smart Sensors. Available online: https://oasees-project.eu/ (accessed on 17 December 2025).
14. Imeri, A.; Gharsallaoui, O.; Grandjean, T.; Roth, U. A Blockchain-based data management approach for swarm-edge computing. In Proceedings of the 2025 12th IFIP International Conference on New Technologies, Mobility and Security (NTMS), Paris, France, 18–20 June 2025; pp. 136–143. [CrossRef]
15. Sadiku, M.N.; Musa, S.M.; Momoh, O.D. Cloud Computing: Opportunities and Challenges. *IEEE Potentials* **2014**, *33*, 34–36. [CrossRef]
16. Peter Mell, T.G. The NIST Definition of Cloud Computing. Available online: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-145.pdf (accessed on 17 December 2025).

17. Cao, K.; Liu, Y.; Meng, G.; Sun, Q. An Overview on Edge Computing Research. *IEEE Access* **2020**, *8*, 85714–85728. [CrossRef]
18. Kaur, G.; Batth, R.S. Edge Computing: Classification, Applications, and Challenges. In Proceedings of the 2021 2nd International Conference on Intelligent Engineering and Management (ICIEM), London, UK, 28–30 April 2021; IEEE Xplore: Piscataway, NJ, USA, 2021; pp. 254–259. [CrossRef]
19. Ahmed, H.; Glasgow, J. Swarm intelligence: Concepts, models and applications. *Sch. Comput. Queens Univ. Tech. Rep.* **2012**, *10*, 1320–2568.
20. Yang, J.; Qu, L.; Shen, Y.; Shi, Y.; Cheng, S.; Zhao, J.; Shen, X. Swarm Intelligence in Data Science: Applications, Opportunities and Challenges. In *Advances in Swarm Intelligence*; Tan, Y., Shi, Y., Tuba, M., Eds.; Springer International Publishing: Cham, Switzerland, 2020; pp. 3–14.
21. Nguyen, L.V. Swarm Intelligence-Based Multi-Robotics: A Comprehensive Review. *AppliedMath* **2024**, *4*, 1192–1210. [CrossRef]
22. Imeri, A.; Agoulmine, N.; Khadraoui, D. Smart Contract Modeling and Verification Techniques: A survey. In Proceedings of the 8th International Workshop on ADVANCEs in ICT Infrastructures and Services (ADVANCE 2020), Cancún, Mexico, 27–29 January 2020; pp. 1–8, hal-02495158.
23. Wang, S.; Ding, W.; Li, J.; Yuan, Y.; Ouyang, L.; Wang, F.Y. Decentralized Autonomous Organizations: Concept, Model, and Applications. *IEEE Trans. Comput. Soc. Syst.* **2019**, *6*, 870–878. [CrossRef]
24. Antal, C.; Cioara, T.; Anghel, I.; Antal, M.; Salomie, I. Distributed Ledger Technology Review and Decentralized Applications Development Guidelines. *Future Internet* **2021**, *13*, 62. [CrossRef]
25. Pons, M.; Valenzuela, E.; Rodríguez, B.; Nolazco-Flores, J.A.; Del-Valle-Soto, C. Utilization of 5G Technologies in IoT Applications: Current Limitations by Interference and Network Optimization Difficulties—A Review. *Sensors* **2023**, *23*, 3876. [CrossRef]
26. Wang, Y.; Tian, Z.; Fan, X.; Cai, Z.; Nowzari, C.; Zeng, K. Distributed Swarm Learning for Edge Internet of Things. *IEEE Commun. Mag.* **2024**, *62*, 160–166. [CrossRef]
27. Chochliouros, I.P.; Kourtis, M.A.; Xilouris, G.; Tavernier, W.; Sanchez, E.A.; Anastassova, M.; Bolzmacher, C.; Tcholtchev, N.; Corsi, A.; Trakadas, P.; et al. OASEES: An Innovative Scope for a DAO-Based Programmable Swarm Solution, for Decentralizing AI Applications Close to Data Generation Locations. In *Artificial Intelligence Applications and Innovations, Proceedings of the AIAI 2023 IFIP WG 12.5 International Workshops, León, Spain, 14–17 June 2023*; Springer Nature: Cham, Switzerland, 2023; pp. 91–105. [CrossRef]
28. Babaioff, M.; Mansour, Y.; Nisan, N.; Noti, G.; Curino, C.; Ganapathy, N.; Menache, I.; Reingold, O.; Tennenholtz, M.; Timnat, E. ERA: A Framework for Economic Resource Allocation for the Cloud. In Proceedings of the 26th International Conference on World Wide Web Companion, Perth, Australia, 3–7 April 2017; WWW '17 Companion, pp. 635–642. [CrossRef]
29. Furman, E.; Senderovich, A.; Bergsma, S.; Beck, J.C. Capacity Allocation for Clouds with Parallel Processing, Batch Arrivals, and Heterogeneous Service Requirements. *arXiv* **2022**, arXiv:2209.08820. [CrossRef]
30. Rac, S.; Brorsson, M. At the Edge of a Seamless Cloud Experience. *arXiv* **2021**, arXiv:2111.06157. [CrossRef]
31. Gurkok, C. Securing Cloud Computing Systems. In *Computer and Information Security Handbook*, 2nd ed.; Vacca, J.R., Ed.; Morgan Kaufmann: Boston, MA, USA, 2013; pp. 97–123. [CrossRef]
32. Abadi, D.J. Data management in the cloud: Limitations and opportunities. *IEEE Data Eng. Bull.* **2009**, *32*, 3–12.
33. Kokila, M.; Reddy K, S. Authentication, access control and scalability models in Internet of Things Security—A review. *Cyber Secur. Appl.* **2025**, *3*, 100057. [CrossRef]
34. Hassan, S.; De Filippi, P. Decentralized Autonomous Organization. *Internet Policy Rev.* **2021**, *10*. [CrossRef]
35. Sun, Y.; Shao, Y. Research on Data Security Communication Scheme of Heterogeneous Swarm Robotics System in Emergency Scenarios. *Sensors* **2022**, *22*, 6082. [CrossRef]
36. Strobel, V.; Ferrer, E.C.; Dorigo, M. Blockchain Technology Secures Robot Swarms: A Comparison of Consensus Protocols and Their Resilience to Byzantine Robots. *Front. Robot. AI* **2020**, *7*, 54. [CrossRef]
37. Pacheco, A.; Strobel, V.; Reina, A.; Dorigo, M. Real-time coordination of a foraging robot swarm using blockchain smart contracts. In *Swarm Intelligence, Proceedings of the ANTS 2022, Málaga, Spain, 2–4 November 2022*; Lecture Notes in Computer Science; Springer: Cham, Switzerland, 2022; Volume 13491, pp. 196–208. [CrossRef]
38. Tran, J.A.; Ramachandran, G.S.; Shah, P.M.; Danilov, C.B.; Santiago, R.A.; Krishnamachari, B. SwarmDAG: A partition-tolerant distributed ledger protocol for swarm robotics. *Ledger* **2019**, *4*, 25–31. [CrossRef]
39. Ibrahim, H.A.; Shouman, M.A.; El-Fishawy, N.A. Improving the reliability of nanosatellite swarms by adopting blockchain technology. *Complex Intell. Syst.* **2024**, *10*, 7163–7182. [CrossRef]
40. Bulgakov, A.L.; Aleshina, A.V.; Smirnov, S.D.; Demidov, A.D.; Milyutin, M.A.; Xin, Y. Scalability and security in blockchain networks: Evaluation of sharding algorithms and prospects for decentralized data storage. *Mathematics* **2024**, *12*, 3860. [CrossRef]
41. Wu, J.; Yuan, L.; Xie, T.; Dai, H. A sharding blockchain protocol for enhanced scalability and performance optimization through account transaction reconfiguration. *J. King Saud Univ.-Comput. Inf. Sci.* **2024**, *36*, 102184. [CrossRef]
42. Strobel, V.; Pacheco, A.; Dorigo, M. Robot swarms neutralize harmful Byzantine robots using a blockchain-based token economy. *Sci. Robot.* **2023**, *8*, eabm4636. [CrossRef]

43. Li, T.; Sahu, A.K.; Talwalkar, A.; Smith, V. Federated Learning: Challenges, Methods, and Future Directions. *IEEE Signal Process. Mag.* **2020**, *37*, 50–60. [CrossRef]
44. Nguyen, D.C.; Pathirana, P.N.; Ding, M.; Seneviratne, A. Integration of Blockchain and Cloud of Things: Architecture, Applications and Challenges. *IEEE Commun. Surv. Tutor.* **2020**, *22*, 2521–2549. [CrossRef]
45. Beck, R.; Müller-Bloch, C.; King, J.L. Governance in the Blockchain Economy: A Framework and Research Agenda. *J. Assoc. Inf. Syst.* **2018**, *19*, 1020–1034. [CrossRef]
46. Lustenberger, M. DAO Research Trends: Reflections and Learnings from the First European DAO Workshop. *Appl. Sci.* **2025**, *15*, 3491. [CrossRef]
47. Bonnet, S. DAO: A Systematic Literature Review and Research Agenda. *Int. J. Emerg. Technol. Soc.* **2024**, *21*, 2450026. [CrossRef]
48. Ly, R.; Shojaei, A. Decentralized Autonomous Organization in Built Environments: Applications, Potential and Limitations. *Inf. Syst. Front.* **2025**, *23*, 577–622. [CrossRef]
49. Al Jasem, M.S.; De Clark, T.; Shrestha, A.K. Toward Decentralized Intelligence: A Systematic Literature Review of Blockchain-Enabled AI Systems. *Information* **2025**, *16*, 765. [CrossRef]
50. Ferrag, M.A.; Derdour, M.; Mukherjee, M.; Derhab, A.; Maglaras, L.; Janicke, H. Blockchain Technologies for the Internet of Things: Research Issues and Challenges. *IEEE Internet Things J.* **2019**, *6*, 2188–2204. [CrossRef]
51. Dorigo, M.; Theraulaz, G.; Trianni, V. Swarm Robotics: Past, Present, and Future. *Proc. IEEE* **2021**, *109*, 1152–1165. [CrossRef]
52. Benet, J. IPFS—Content Addressed, Versioned, P2P File System. *arXiv* **2014**, arXiv:1407.3561.
53. Protocol Labs. *Filecoin: A Decentralized Storage Network*; Technical report; Protocol Labs: San Francisco, CA, USA, 2017.
54. Oliveira, M.; Chauhan, S.; Pereira, F.; Felgueiras, C.; Carvalho, D. Blockchain protocols and edge computing targeting Industry 5.0 needs: A survey. *Sensors* **2023**, *23*, 9174. [CrossRef]
55. Nguyen, T.; Nguyen, H.; Gia, T.N. Exploring the integration of edge computing and blockchain into IoT systems: Principles, architectures, security, and applications. *J. Netw. Comput. Appl.* **2024**, *226*, 103884. [CrossRef]
56. Zhu, J.; Li, F.; Chen, J. A survey of blockchain, artificial intelligence, and edge computing for Web 3.0. *Comput. Sci. Rev.* **2024**, *54*, 100667. [CrossRef]
57. Khodjamov, N.; Yang, S.; Sharif, K.; Gao, Y.; Li, F.; Wang, Y.; Mamarasulov, S.; Zhu, L. Blockchain-Based Secure Trusted Clusters for Multi-Tiered Social IoT Environments in Edge-Cloud Networks. *Comput. Netw.* **2025**, *275*, 111880. [CrossRef]
58. Li, Y.; Wang, J.; Zhang, H.; Zhao, Z.; Ding, Y. AssociateChain: Scaling Blockchain in Cloud–Edge-Enabled Metaverse via Associative Sharding. *Comput. Commun.* **2025**, *237*, 108150. [CrossRef]
59. OASEES Consortium GitHub. OASEES Web3.0 Cloud Native Swarm Computing - OASEES Stack Prototype. Available online: https://github.com/oasees/oasees-stack-prototype (accessed on 17 December 2025).