# Technical Requirements for Confined AI Experiments on Decentralized Ledgers: Verifiability, Intellectual Property, and Usage Tracking

## I. Executive Summary

The imperative to "confine the experiment" in artificial intelligence (AI) signifies a critical evolution in AI system design, moving beyond traditional security paradigms to embrace intrinsic integrity, transparency, and accountability. This report meticulously details the technical prerequisites and operational considerations for establishing and managing AI experiments with stringent control and verifiability, particularly through the strategic integration of blockchain and advanced cryptographic techniques. The core of this confinement encompasses verifiable execution, robust intellectual property (IP) protection, transparent usage tracking, and unwavering adherence to ethical and regulatory standards.

The analysis highlights that achieving such confinement necessitates a multi-layered architectural approach. Zero-Knowledge Proofs (ZKPs) emerge as a pivotal cryptographic tool, enabling the verification of AI model logic and execution without compromising sensitive data. Decentralized oracles, particularly those enhanced by AI, are essential for feeding trustworthy, real-world data into on-chain AI systems, thereby mitigating data integrity risks. The selection of an appropriate blockchain infrastructure, balancing scalability, security, and cost, is foundational, with purpose-built AI blockchains representing a significant advancement in this domain.

For intellectual property, Non-Fungible Tokens (NFTs) coupled with smart contracts offer a transformative mechanism for on-chain IP protection, automated licensing, and AI-powered infringement monitoring. Furthermore, the report underscores the necessity of formal attribution for both human researchers (via ORCID iDs) and AI agents (through frameworks like the Artificial Intelligence Disclosure (AID) Framework), anticipating a hybrid attribution landscape. Real-time AI model usage reporting, facilitated by smart contract events and blockchain explorers, provides granular, auditable insights into AI operations, crucial for compliance and resource allocation.

The implementation of these advanced systems is not without challenges, including computational overhead, data privacy concerns, a lagging regulatory environment, and the persistent issues of data quality and bias. However, ongoing innovations in Layer 2 scaling solutions, hardware acceleration for ZKPs, and privacy-preserving techniques are actively addressing these hurdles. The report concludes with actionable recommendations for technical project leads and research program managers, emphasizing a phased implementation, secure development practices, interdisciplinary collaboration, and continuous monitoring to ensure the integrity and trustworthiness of AI experiments as their capabilities and societal impact continue to escalate.

## II. Introduction: Defining Confined AI Experiments

The concept of "confining the experiment" in AI represents a profound shift in how these increasingly autonomous and impactful systems are developed, deployed, and governed. It extends far beyond mere cybersecurity measures, encompassing a holistic strategy to embed integrity, transparency, and accountability throughout the entire AI lifecycle. This includes ensuring that AI models operate strictly within predefined parameters, that their inputs and outputs are provably correct, that intellectual property utilized or generated is meticulously managed, and that all interactions are fully auditable. The growing complexity and pervasive societal influence of AI necessitate these formal confinement mechanisms, signaling a departure from traditional software development practices towards a more robust, trust-minimized paradigm. This foundational reorientation is not solely about preventing malicious activities; it is fundamentally about engineering accountability and trust directly into the very fabric of AI deployment.

The importance of verifiability, transparency, and control cannot be overstated as AI systems become more autonomous and integrated into critical sectors such as finance, healthcare, and infrastructure. The ability to verify AI operations and audit their decisions is paramount. Transparency in AI decision-making is crucial for mitigating inherent biases and ensuring ethical compliance, thereby fostering public confidence. Furthermore, robust control mechanisms are indispensable for preventing unintended consequences and ensuring that AI systems consistently align with their intended design objectives and societal values.

The demand for confined AI experiments is driven by a confluence of interconnected factors. Regulatory bodies worldwide are actively developing frameworks for AI, increasingly mandating transparency, accountability, and stringent data protection measures. This regulatory push underscores the legal imperative for verifiable AI. Concurrently, ethical considerations demand that AI systems uphold principles of fairness, non-discrimination, and privacy, which are critical for earning and maintaining public trust. The unique challenges associated with intellectual property in the context of AI-generated content and the data used for AI training necessitate novel and robust protection mechanisms. Finally, the inherent complexity of modern AI, particularly large language models (LLMs) and advanced AI agents, often results in "black box" characteristics, where internal reasoning processes remain opaque. Confinement aims to externalize and verify these internal processes, transforming opaque systems into auditable ones.

A critical observation emerges regarding the design philosophy of AI systems, moving from a focus on security *against* external threats to an emphasis on trust-by-design. Traditional software development often prioritizes securing systems from external vulnerabilities. However, in the context of AI, "confinement" implies an intrinsic design principle that ensures internal integrity and predictable behavior, even from highly autonomous agents. This represents a paradigm shift from reactive cybersecurity to proactive assurance, where the goal is not merely to prevent breaches but to cryptographically prove correct operation and ethical alignment, thereby fostering trust among stakeholders and the broader public. The immutability of blockchain and the verifiability offered by Zero-Knowledge Proofs directly support this architectural evolution.

Furthermore, the very definition of an "experiment" in the context of AI is undergoing a significant transformation. It is no longer confined to isolated laboratory settings but increasingly extends to real-world deployments and continuous operations. The widespread application of AI in diverse fields such as finance, healthcare, supply chain management, and even fundamental scientific research indicates that "confining the experiment" must apply to AI systems operating in live production environments. The continuous need for real-time monitoring , auditable decision-making , and ongoing regulatory compliance points to a scenario where the AI system itself becomes a continuous, living "experiment." In this evolving landscape, confinement is not a one-time setup but an ongoing operational requirement, broadening the scope of what constitutes an "experiment" to encompass continuous deployment and learning.

## III. Foundational Requirements: Blockchain and Verifiable AI

### A. Verifiable AI Execution via Zero-Knowledge Proofs (ZKPs)

Zero-Knowledge Proofs (ZKPs) represent a cornerstone for establishing trust and verifiability within confined AI experiments. These cryptographic protocols enable one party, the prover, to convince another, the verifier, that a given statement is true, without divulging any information beyond the mere fact of its truth. For AI systems, ZKPs offer a potent solution to verify the correctness of machine learning (ML) algorithms and their execution on a blockchain without exposing sensitive data, such as proprietary training datasets or confidential model parameters. This capability directly addresses the pervasive "black box" problem in AI, where the internal decision-making processes often remain opaque.

ZKPs can be employed to prove that an AI model was correctly trained on a committed dataset, a concept known as Zero-Knowledge Proof of Training (zkPoT), or that a specific inference was performed accurately based on defined inputs and model parameters. This ensures the integrity and confidentiality of the entire computational process. For instance, zkPoT for deep neural networks (DNNs) aims to provide provable security and privacy guarantees while maintaining practical efficiency for the prover. This capability allows for cryptographic assurance of AI behavior, even when the underlying logic or data remains private.

Implementing ZKPs for AI requires careful consideration of several technical aspects. Firstly, the ML model must be designed in a manner that facilitates the generation of proof statements, articulating what the model is intended to accomplish without revealing its underlying data or intricate logic. Secondly, computational efficiency is a significant hurdle. ZKP generation can be remarkably resource-intensive, demanding substantial processing power and memory. However, innovations such as hardware accelerators, like NoCap, which can generate proofs 586 times faster than a 32-core CPU, and optimized algorithms, including recursive proofs and incrementally verifiable computation (IVC), are crucial for achieving scalability. Thirdly, the verifier runtime must be efficient; the proof should be succinct and verifiable much more quickly than executing the original computation directly. Lastly, establishing a robust protocol for securely transferring proofs between the prover and verifier, along with continuous testing for potential vulnerabilities, is essential for maintaining system integrity.

The ability to cryptographically verify AI computations without revealing proprietary models or sensitive data holds transformative potential for industries where privacy is paramount, such as healthcare and finance. This also paves the way for truly decentralized AI training and deployment, fostering trust in multi-stakeholder environments.

A critical observation is the shift from a "black box" understanding of AI to a "verifiable black box" model. ZKPs do not necessarily open the AI's internal logic for human inspection in a traditional sense. Instead, they provide a cryptographic guarantee that the AI's computation adhered to specified rules and parameters, even when the underlying data or logic remains private. This distinction is vital for establishing trust in complex AI systems where full human interpretability might be impractical or impossible. It allows for cryptographic assurance that the AI followed its programmed logic and used the specified data, without revealing the sensitive details.

Furthermore, the high computational cost associated with ZKPs is not merely a barrier but a powerful economic driver for innovation in hardware and algorithms. The repeated emphasis on "prohibitive prover costs" and "computational overhead" underscores a significant challenge. However, the concurrent discussion of "transformative speedups" from hardware-algorithm co-design indicates that the market demand for verifiable computation in high-value AI applications is so strong that it is actively pushing the boundaries of cryptographic and hardware engineering. The perceived value proposition of enhanced trust and privacy in these applications is outweighing current costs, leading to rapid advancements that will eventually reduce these costs, thereby making ZKPs economically viable for a broader spectrum of AI applications.

**Table 1: Zero-Knowledge Proofs (ZKPs) for AI Verification: Capabilities and Challenges**

| ZKP Property/Aspect | Description | Relevance to AI Verification | Challenges | Mitigation/Solution |
| --- | --- | --- | --- | --- |
| **Zero-Knowledge** | Prover convinces verifier of statement truth without revealing any other information. | Enables verification of AI model execution or training without exposing sensitive data (e.g., model parameters, private training data). | Maintaining strict zero-knowledge properties for complex AI models. | Advanced ZKP schemes (e.g., zk-SNARKs, zk-STARKs) , secure enclaves. |
| **Succinctness** | Proof size and verification time are very small, often polylogarithmic, relative to the computation size. | Allows efficient on-chain verification of off-chain AI computations, reducing blockchain storage and gas costs. | Achieving truly succinct proofs for arbitrarily complex AI computations. | Recursive proofs (IVC) , optimized arithmetization. |
| **Completeness** | If the statement is true, an honest prover can always convince the verifier. | Ensures that correct AI computations can always be proven correct. | Ensuring the prover correctly implements the proving algorithm. | Standardized ZKP libraries, rigorous testing of prover implementation. |
| **Soundness** | If the statement is false, a dishonest prover cannot convince the verifier (except with negligible probability). | Guarantees that only correct AI computations are accepted as valid, preventing fraudulent claims. | Preventing "cheating provers" from fabricating proofs for false statements. | Strong cryptographic assumptions, robust protocol design, ongoing cryptographic research. |
| **Computational Cost** | Proof generation is resource-intensive, requiring significant CPU/memory. | Limits the complexity and frequency of AI computations that can be verifiably executed. | Prohibitive prover costs (e.g., 1000x slowdown compared to training). | Hardware accelerators (e.g., NoCap, 586x faster) , algorithmic optimizations for matrix operations. |
| **Scalability** | Ability to handle increasing data volumes and model sizes. | Essential for applying ZKPs to large-scale AI models (e.g., DNNs, LLMs) and high-throughput inference. | Prover memory overhead scales linearly with computation. | Sharding execution traces, recursive composition ("continuations") , specialized ZKVMs. |
| **Privacy Preservation** | Protects sensitive data (training datasets, model parameters, user inputs) during verification. | Crucial for AI applications in sensitive domains like healthcare and finance, enabling secure data sharing. | Balancing privacy with the need for transparency in AI outputs. | ZKPs, federated learning, homomorphic encryption (though not detailed in snippets). |
| **Verifiable Training (zkPoT)** | Proves correct training of a model on a committed dataset without revealing the dataset. | Ensures the integrity and provenance of AI models, crucial for trust in model behavior and preventing "poisoning" attacks. | High computational burden for complex DNN training. | Kaizen (zkPoT for DNNs) aims for practical prover efficiency. |
| **Verifiable Inference** | Proves correct execution of an AI model on specific inputs to produce an output. | Guarantees the reliability of AI predictions and decisions in real-world applications, enabling auditable AI. | Designing models to facilitate proof generation for specific inference tasks. | Defining clear model outputs, robust proof transfer protocols. |

### B. Decentralized Oracles for Data Integrity

Smart contracts operating on blockchain networks are inherently isolated from external data; they cannot directly access real-world information outside their native environment. Decentralized Oracles serve as indispensable secure bridges, facilitating the reliable and trustworthy transmission of external data into smart contracts. This capability is critically important for AI models, which frequently depend on real-time data from diverse off-chain sources—such as APIs, websites, and physical sensors—to function effectively and make informed decisions.

Traditional oracles primarily focus on data retrieval. However, the evolution of AI-powered oracles elevates this function by leveraging generative AI capabilities to intelligently process and validate incoming data. These advanced oracles can "check if the data makes sense, spot patterns, and even catch unusual behavior". They possess the capacity to validate data against established patterns, fill in missing information, and aggregate data from multiple sources, dynamically weighing their reliability to determine the most accurate input for smart contract actions. This intelligent layer significantly enhances data accuracy and reduces the necessity for extensive human oversight in data validation processes.

The benefits of AI-powered oracles for confined AI experiments are manifold. Firstly, they provide exceptional speed, enabling AI models to process vast volumes of data almost instantaneously, thus ensuring real-time data feeds for smart contracts. Secondly, they substantially reduce the need for human intervention, as AI handles much of the data validation and logic, aligning seamlessly with the principles of decentralization and minimizing manual errors. Thirdly, these oracles exhibit remarkable adaptability, capable of learning from new data over time and adjusting their operations as protocols evolve or new data sources emerge. Finally, the deployment of Decentralized Oracle Networks (DONs) further enhances reliability by distributing the system across multiple independent verification nodes. These nodes aggregate results through consensus protocols, effectively preventing single points of failure and significantly improving overall data accuracy.

These intelligent oracles find vital applications in various domains. For instance, in parametric insurance, they can automate claim processing based on verified external events like weather conditions or flight delays. In decentralized finance (DeFi), they are crucial for detecting sudden price swings across multiple exchanges, thereby protecting protocols from sophisticated attacks like flash loans.

A significant observation is how AI-powered oracles transform data feeds from passive retrieval into active, intelligent validation, directly addressing a critical vulnerability in AI systems. The effectiveness of any AI system is heavily dependent on the quality of its input data; flawed data inevitably leads to unreliable outputs. While traditional oracles merely fetch data , AI-powered oracles actively validate the data, performing checks for consistency, pattern recognition, and anomaly detection. This introduces an intelligent layer of data integrity at the source, proactively mitigating the risk of data contamination, which is a significant challenge for AI systems. This proactive validation is a crucial step towards ensuring the overall trustworthiness of any AI experiment.

Furthermore, the effectiveness of decentralized AI is intrinsically linked to the reliability and decentralization of its data oracles. If a decentralized AI system relies on external data that is sourced through a centralized oracle, the entire system's decentralization and trustworthiness are fundamentally compromised. The emphasis on "decentralized oracle networks (DONs)" and "multiple independent verifications" underscores this causal relationship. For a truly confined and decentralized AI experiment, the mechanism for data input—the oracle—must mirror the decentralization principles of the AI and blockchain itself. Failure to ensure this alignment would introduce a single point of failure or potential manipulation, undermining the very purpose of a decentralized, verifiable system.

### C. Blockchain Infrastructure Selection

The choice of blockchain infrastructure is a pivotal decision for establishing confined AI experiments, as it forms the underlying decentralized ledger for verifiable execution, intellectual property management, and usage tracking. Blockchain fundamentally provides a decentralized, secure, and immutable foundation for AI algorithms, significantly enhancing data integrity and trustworthiness. It offers a transparent record for AI decision processes, transforming traditionally "black box" systems into verifiable ones.

Key benefits derived from this synergy include:

* **Data Integrity:** Blockchain ensures that data fed into AI models is tamper-proof and reliable, effectively mitigating issues of data bias or corruption at the foundational level.
* **Auditable Decision-Making:** The immutable ledger inherent to blockchain technology allows AI decisions to be traced back to their source data, which is critically important for applications in sensitive domains like healthcare or finance.
* **Decentralized AI Training:** Blockchain enables multiple stakeholders to contribute to the training of AI models while preserving data privacy and ownership, fostering collaborative AI development.
* **Enhanced Security:** Blockchain secures AI processes by ensuring data provenance, while AI, in turn, can strengthen blockchain systems by detecting and mitigating cyber threats.

The selection of a specific blockchain platform is critical, requiring a careful balance between smart contract capabilities, transaction speed (Transactions Per Second, TPS), and cost (gas fees), tailored to the specific needs of the AI experiment.

* **Ethereum:** As a pioneer in the blockchain space, Ethereum boasts robust smart contract capabilities and widespread adoption. However, its significant network usage often leads to high gas fees, which can be a notable drawback for frequent or complex AI interactions.
* **Polygon:** Functioning as a Layer 2 scaling solution for Ethereum, Polygon is recognized for its scalability, affordability, and significantly lower transaction costs. It is capable of handling a high volume of transactions efficiently, making it an attractive option for dApps that require more frequent on-chain interactions.
* **Solana:** This platform has rapidly gained traction due to its impressive transaction speeds and low costs, making it an ideal choice for projects where efficiency and high throughput are primary considerations.
* **AIVM (Artificial Intelligence Virtual Machine):** AIVM stands out as a purpose-built Layer-1 blockchain specifically engineered to power verifiable AI at scale. It integrates decentralized compute, agent-based AI execution, and tokenized data marketplaces, along with developer tooling. This platform aims to bridge the long-standing gap between AI and blockchain infrastructure, enabling verifiable inference and decentralized model deployment, thereby offering a highly specialized environment for confined AI experiments.
* Other notable platforms that offer varying features include Flow, Cardano, EOS, Tezos, WAX, Binance Chain, Avalanche, Tron, Algorand, Polkadot, and Hyperledger.

A significant observation is the scalability-security-cost trilemma inherent in selecting a blockchain infrastructure for confined AI experiments. The various blockchain platforms present a spectrum of choices, each with different transaction speeds, gas fees, and underlying consensus mechanisms. Ethereum, for instance, offers high security and decentralization but at a higher cost. Conversely, Polygon and Solana provide lower costs and higher speeds, but these benefits may involve different trade-offs in terms of decentralization. This situation highlights a fundamental trilemma: achieving robust security and decentralization, which are crucial for the integrity of confined AI experiments, often comes at the expense of scalability and transaction fees. This economic constraint can impact the practical viability of running continuous AI experiments on-chain. The emergence of specialized AI blockchains, such as AIVM , represents a direct response to this trilemma, aiming to optimize specifically for AI workloads.

This leads to another important observation: the increasing demand for verifiable and decentralized AI is driving the development of specialized blockchain infrastructures. While general-purpose blockchains like Ethereum and Polygon can host AI-related smart contracts, the advent of platforms like AIVM signifies a maturation of the decentralized AI landscape. AIVM is explicitly "purpose-built" for AI execution, verifiable inference, and decentralized model deployment. This indicates that the unique requirements of AI—such as specific compute needs, data marketplaces, and specialized verification mechanisms—are leading to the creation of tailored blockchain solutions. This trend suggests that future confined AI experiments may increasingly rely on such specialized infrastructures to achieve optimal performance, verifiability, and trust.

**Table 2: Key Blockchain Platforms for Verifiable AI and IP Management**

| Blockchain Platform | Primary Use Case for AI/IP | Programming Language(s) | Consensus Mechanism | Smart Contract Support | Average Transaction Speed (TPS) | Average Transaction Cost (Gas Fees) | Key Features/Benefits for AI/IP |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Ethereum** | General DApps, NFTs, DeFi, IP Management | Solidity, Vyper | Proof of Stake | Yes | 15-30 (Up to 100,000 with L2) | High | Pioneering role, large community, strong smart contract capabilities, widespread adoption. |
| **Polygon** | Scalable DApps, NFTs, IP Management (Layer 2) | Solidity | Proof of Stake | Yes | 7,200 (Up to 65,000) | Low (cents) | Scalability, affordability, Ethereum compatibility, reduces congestion and fees. |
| **Solana** | High-Throughput DApps, NFTs, Real-time Applications | Rust, C | Proof of History, Proof of Stake | Yes | 5,000-10,000 (Up to 710,000) | Very Low | Impressive transaction speeds, low costs, ideal for efficiency-focused projects. |
| **AIVM (ChainGPT)** | Purpose-Built AI, Verifiable AI, Decentralized Compute | Python SDKs | Native Validator Roles for AI, Compute, Data | Yes | Early development stage, aiming for scale | $CGPT token for fees | Verifiable AI execution, decentralized model deployment, tokenized data marketplaces, cross-chain interoperability. |
| **Tezos** | Secure Smart Contracts, Formal Verification | Michelson | Liquid Proof of Stake | Yes | 40 (Up to 1 million with upgrades) | Low | Recognized for security (formal verification), on-chain governance. |
| **Hyperledger Fabric** | Enterprise Blockchain, Permissioned DApps, Supply Chain | JavaScript, Go | Pluggable (e.g., Crash Fault Tolerance) | Yes | Up to 3,500 (use case dependent) | Private/Permissioned (fees vary) | Suitable for sensitive data, compliance, strong enterprise support (IBM, Intel). |

## IV. Intellectual Property Management and Attribution

### A. On-Chain IP Protection and Licensing

The advent of Non-Fungible Tokens (NFTs) has fundamentally reshaped the landscape of intellectual property (IP) management in the digital realm. NFTs are unique digital assets, immutably recorded on a blockchain, providing verifiable proof of ownership and a transparent chain of provenance for both digital and, by representation, physical assets. This inherent uniqueness and traceability make NFTs an ideal mechanism for representing and managing a wide array of IP rights on-chain, including digital art, music, code, written works, patents, licenses, and registered copyrights.

Smart contracts, which are self-executing agreements stored and enforced on the blockchain, play a transformative role in automating IP management processes. They can be programmed to automate IP licensing, facilitate royalty distribution, and enforce usage rights. By embedding specific licensing terms directly into the smart contract, the system can automatically verify authorization for use and trigger royalty payments based on predefined conditions and real-time usage metrics. This automation significantly reduces administrative burdens, minimizes disputes over payments, and ensures fair and timely compensation for creators.

Furthermore, the integration of AI-powered tools enhances infringement monitoring capabilities. AI-driven systems can continuously scan vast digital platforms and marketplaces for unauthorized use of trademarks, logos, or patented designs. By analyzing both text and visual content, AI can detect potential infringements in real-time and, crucially, automatically trigger enforcement actions via smart contracts. For example, a smart contract could be designed to restrict the sale of a virtual product or flag an infringing transaction if an AI system detects unauthorized use of a company's logo.

The immutable nature of blockchain provides an unalterable timestamp and transparent ownership records, which are invaluable for reducing disputes and facilitating smoother transfers of IP assets. Tools like Timeseal, for instance, offer blockchain-powered timestamping for property records, creating an immutable and verifiable trail of changes. This level of verifiable provenance is a significant advancement over traditional, often centralized, record-keeping systems.

Despite these advancements, challenges persist. The regulatory environment surrounding NFTs and AI-generated intellectual property is still nascent and evolving, leading to uncertainties and a need for clearer guidelines. Additionally, security vulnerabilities within AI-powered systems or smart contracts themselves could potentially compromise digital assets, underscoring the need for robust security practices.

A fundamental observation is that the combination of NFTs and smart contracts transforms intellectual property from a static legal right into a dynamic, programmable digital asset. Traditionally, IP rights are managed through complex legal documents and often require manual enforcement. However, the capabilities described, where NFTs represent IP ownership on-chain and smart contracts automate licensing and royalty payments , mean that IP is no longer merely protected; it gains the ability to act autonomously. It can self-enforce its terms, track its usage, and distribute revenue without intermediaries. This represents a profound shift from a reactive, human-mediated system to a proactive, code-driven one, enabling granular control and novel monetization models for creators within a confined and verifiable framework.

Another critical observation highlights a growing legal-technical gap concerning AI-generated IP. The rapid technological advancements in AI's ability to generate content are creating a significant disconnect with existing intellectual property laws. Several sources detail ongoing legal debates and lawsuits regarding copyright infringement stemming from AI training data and AI-generated works. Concerns about the evolving regulatory environment are also evident. This tension arises because current legal frameworks often struggle to attribute authorship to non-human entities or to define "sufficient effort" for AI-generated content. This necessitates the development of new legal interpretations or, as suggested by the Artificial Intelligence Disclosure (AID) Framework , the adoption of standardized technical attribution methods. Such mechanisms are crucial to bridge this gap, ensuring proper credit and compensation in a future where human and artificial intelligences increasingly collaborate.

**Table 3: ERC-721 NFT Metadata Structure for AI Agent IP**

| Metadata Field | Standard ERC-721 Purpose | Specific Purpose for AI Agent IP | Type | Example Value/Format |
| --- | --- | --- | --- | --- |
| **name** | Name of the digital item. | Name of the AI agent or model. | Required | "Quantum Physics AI Model v2.1" |
| **description** | Human-readable description of the item. | Detailed description of the AI agent's function, capabilities, and intended use. | Optional | "A multimodal AI agent for simulating post-relativity physics models and analyzing complex astronomical data." |
| **image** | URL to an image representing the item. | Visual representation of the AI agent, its architecture, or a logo. | Required | "ipfs://Qm...AI\_Model\_v2.1.png" |
| **external\_url** | URL to an item's webpage on the creator's site. | Link to the AI agent's official documentation, GitHub repository, or research paper. | Optional | "https://github.com/QuantumAI/physics-model-v2" |
| **attributes** | Array of key-value pairs for item traits. | Structured data on AI capabilities, performance metrics, training data hashes, or ethical compliance scores. | Optional | `` |
| **capabilities** | (Custom field, often within attributes) | List of specific skills or functions the AI agent can perform. | Optional | `` |
| **version** | (Custom field, often within attributes) | Current version of the AI agent or model. | Optional | "2.1.0" |
| **timestamps** | (Custom field, often within attributes) | Creation and latest update times of the AI agent or its metadata. | Optional | {"created": "2024-01-01T10:00:00Z", "last\_updated": "2024-05-15T14:30:00Z"} |
| **ORCID\_iD** | (Custom field) | Linked ORCID iD of the primary human researcher(s) or team responsible for the AI agent. | Optional | "https://orcid.org/0000-0001-2345-6789" |
| **proof\_hash** | (Custom field) | Hash of a Zero-Knowledge Proof (ZKP) verifying model execution or training. | Optional | "0x789abcde...f0123456" |
| **provenance\_link** | (Custom field) | Link to a detailed on-chain provenance record or audit trail of the AI's development. | Optional | "https://blockchainexplorer.com/tx/0x...provenance" |

### B. Researcher and AI Agent Attribution

Accurate and persistent attribution is fundamental to scholarly integrity and intellectual property management, particularly in the evolving landscape of AI-assisted research. The Open Researcher and Contributor ID (ORCID iD) serves as a cornerstone for human researchers. It is a persistent digital identifier that uniquely distinguishes individuals throughout their scholarly careers, effectively overcoming challenges such as common names, name changes, or inconsistent abbreviations, thereby ensuring the correct attribution of scholarly contributions. ORCID is increasingly mandated by major funding bodies, such as the National Institutes of Health (NIH), National Science Foundation (NSF), and Australian Research Council (ARC), as well as by publishers for grant applications and manuscript submissions. This system facilitates automated linkages between researchers and their diverse works—including publications, datasets, grants, and patents—reducing administrative burdens and significantly improving the discoverability of their scholarly output. Furthermore, ORCID iDs can be linked to professional platforms like GitHub, allowing researchers to showcase their scholarly contributions and code.

As AI systems become more sophisticated and actively contribute to research and content creation, transparent disclosure and formal attribution for their contributions become crucial. The Artificial Intelligence Disclosure (AID) Framework (2024) provides a structured and standardized approach for disclosing the use of AI tools in academic and research work. This framework mandates detailing the specific AI tools used and the precise manner of their application across various stages of the research and writing process, from initial information collection and data analysis to writing and editing. The AID Statement is typically appended to the end of a paper, similar to an Acknowledgements section, ensuring transparency and promoting ethical considerations regarding AI's role in scholarship.

Beyond mere disclosure, the formal attribution for AI agents, especially autonomous ones, is an emerging area of development. Projects like the Virtuals Protocol exemplify this by allowing the tokenization of AI agents as revenue-generating assets. Within this framework, contributions to AI development can be recorded directly on-chain, enabling transparent and fair revenue distribution among contributors. This aligns with the concept of AI agents possessing their own on-chain wallets, facilitating autonomous transactions and asset management, and establishing a form of digital identity and economic agency for the AI itself.

A significant observation is the emergence of a hybrid attribution landscape, where ORCID for humans coexists with frameworks like AID for AI. This development highlights a future in which intellectual contributions are increasingly the result of human-AI collaborative efforts. ORCID is well-established for human researchers, providing a persistent identity and linking to their work. Simultaneously, the AID Framework addresses the necessity of disclosing AI's involvement. This juxtaposition indicates that the traditional single-author or single-contributor model is evolving. The future of research and innovation will involve complex partnerships between humans and AI, requiring a sophisticated, hybrid attribution system capable of precisely delineating and crediting contributions from both human and artificial intelligences. This could potentially involve linking ORCID iDs to AI agent NFTs or verifiable execution proofs, creating a comprehensive record of collaborative intellectual output.

This leads to another important observation: the principles underpinning ORCID for human researchers—unique identification, persistent linkage, and automated workflows—are becoming increasingly applicable to AI agents. This suggests an emerging need for a future "ORCID for AI" standard, which would provide verifiable AI agent identity and track their contributions. Just as human researchers require persistent identifiers to track their impact and ensure proper attribution, AI agents that generate content, perform research tasks, or contribute to scientific discoveries will need similar mechanisms for accountability, intellectual property management, and tracking their "scholarly" output. This points towards the development of a new standard or system, potentially built upon decentralized identity and blockchain technologies, that offers a unique, persistent, and verifiable identity for AI agents and their intellectual contributions, akin to an "ORCID for AI".

## V. On-Chain Monitoring and Usage Tracking

### A. Real-time AI Model Usage Reporting

To effectively "confine the experiment" in AI, it is paramount to implement robust mechanisms for tracking how AI models are being utilized. This includes monitoring inference counts, recording data consumption, and observing interaction frequency. Such granular tracking provides essential transparency and auditability for AI operations.

One primary method for achieving this is through **Smart Contract Events**. Solidity smart contracts are designed to emit "events" to log significant actions and state changes to the blockchain. These events are permanently stored on the blockchain and can be accessed and listened to by external applications and monitoring tools. By strategically emitting events (using the emit keyword) whenever an AI model performs an inference, processes a specific dataset, or interacts with other systems, a transparent and auditable record of its activity can be created. This capability enables granular, real-time reporting of AI usage, providing a continuous stream of verifiable operational data.

**On-Chain Data Analysis** further complements this by leveraging specialized tools. Blockchain explorers, such as PolygonScan, Etherscan, and Chainlens, offer comprehensive functionalities to monitor transactions, view wallet activity, and inspect smart contract interactions and their associated event logs in real-time. These explorers allow users to filter event logs by criteria such as transaction hash, involved addresses, and specific event topics (which correspond to indexed event parameters). This granular filtering capability enables detailed insights into how contracts are being utilized, providing a powerful auditing mechanism for AI experiments.

For **AI Agent Reporting**, decentralized AI agents can be designed to integrate with various APIs to pull real-time data and connect directly with smart contracts. This allows them to report their activities on-chain, creating a verifiable record of their operations. This can include tracking metrics like daily active wallets interacting with the agent, the volume of on-chain and off-chain data consumed, and even specific portfolio management actions executed by AI-driven trading agents.

The importance of granularity in tracking these metrics cannot be overstated. By monitoring specific data points such as inference costs , total compute consumed , and the frequency of AI model use , valuable insights can be gained into the efficiency, adoption rates, and resource consumption patterns of AI models within a confined setting. This detailed data is essential for optimizing performance, managing operational costs (e.g., gas fees on Ethereum or Polygon ), and ensuring continuous compliance with predefined experimental parameters.

A significant observation is that on-chain event logging effectively creates a verifiable, real-time "digital twin" of AI model operations, offering unprecedented transparency and auditability. While the core AI models often execute off-chain for computational efficiency, their critical interactions, inferences, and data usage can be immutably logged on-chain via smart contract events. This process generates a permanent, timestamped record of every significant action. This on-chain log functions as a "digital twin" of the AI's operational footprint, enabling both real-time monitoring and retrospective auditing. This capability is crucial for proving adherence to confinement parameters, moving beyond aggregated statistics to verifiable, per-inference data, and thereby establishing a new level of accountability for AI systems.

This leads to another important observation: granular on-chain usage data enables precise cost attribution and dynamic resource allocation for AI services. AI models incur various costs, including inference compute, storage, and transaction fees. By logging detailed usage data on-chain, particularly through events, it becomes feasible to track resource consumption per inference or per user with high precision. This granular economic transparency facilitates transparent micropayments between users and AI models and enables dynamic market mechanisms for compute resources. This level of economic transparency is vital not only for optimizing the financial sustainability of confined AI experiments but also for developing fair and equitable monetization models for AI-as-a-service offerings.

**Table 4: Smart Contract Event Logging for AI Usage Tracking**

| Event Name | Event Parameters (Type, Description) | Purpose for AI Usage Tracking | Example Solidity Code (Event Declaration & Emit) | Example Data Log (from Explorer - illustrative) |
| --- | --- | --- | --- | --- |
| **InferenceExecuted** | address indexed user (caller's address), uint256 indexed modelId (ID of AI model), uint256 inferenceCount (cumulative count for user/model), string inputHash (hash of input data), string outputHash (hash of output data), uint256 timestamp (block timestamp) | Tracks individual AI model inference executions, providing a verifiable count and links to input/output data for auditing. | event InferenceExecuted(address indexed user, uint256 indexed modelId, uint256 inferenceCount, string inputHash, string outputHash, uint256 timestamp); <br> emit InferenceExecuted(msg.sender, \_modelId, \_inferenceCounter, \_inputHash, \_outputHash, block.timestamp); | Topic 0: 0x...InferenceExecuted\_hash <br> Topic 1: 0x...user\_address <br> Topic 2: 0x...model\_id\_hash <br> Data: inferenceCount: 123, inputHash: "0xabc...", outputHash: "0xdef...", timestamp: 1678886400 |
| **DataConsumed** | address indexed modelAddress (AI model contract address), string indexed dataIdentifier (IPFS CID or content hash), uint256 dataVolumeKB (volume of data consumed in KB), uint256 timestamp | Records specific data consumption by AI models, crucial for data provenance and licensing compliance. | event DataConsumed(address indexed modelAddress, string indexed dataIdentifier, uint256 dataVolumeKB, uint256 timestamp); <br> emit DataConsumed(address(this), \_dataCID, \_volumeKB, block.timestamp); | Topic 0: 0x...DataConsumed\_hash <br> Topic 1: 0x...model\_address <br> Topic 2: 0x...data\_identifier\_hash <br> Data: dataVolumeKB: 5120, timestamp: 1678886500 |
| **ModelUpdated** | uint256 indexed modelId (ID of AI model), string newVersion (new model version string), string modelHash (hash of new model binary/parameters), address indexed updater (address initiating update), uint256 timestamp | Provides an immutable audit trail of AI model versions and updates, essential for reproducibility and compliance. | event ModelUpdated(uint256 indexed modelId, string newVersion, string modelHash, address indexed updater, uint256 timestamp); <br> emit ModelUpdated(\_modelId, \_newVersion, \_modelHash, msg.sender, block.timestamp); | Topic 0: 0x...ModelUpdated\_hash <br> Topic 1: 0x...model\_id\_hash <br> Topic 2: 0x...updater\_address <br> Data: newVersion: "3.0", modelHash: "0xghi...", timestamp: 1678886600 |
| **IPLicensed** | uint256 indexed ipNFTId (ID of IP NFT), address indexed licensee (address granted license), string licenseTermsHash (hash of license terms), uint256 royaltyAmount (royalty payment in smallest unit), uint256 timestamp | Tracks the licensing of intellectual property represented by NFTs, ensuring transparency in usage rights and royalty distribution. | event IPLicensed(uint256 indexed ipNFTId, address indexed licensee, string licenseTermsHash, uint256 royaltyAmount, uint256 timestamp); <br> emit IPLicensed(\_nftId, \_licensee, \_termsHash, \_royalty, block.timestamp); | Topic 0: 0x...IPLicensed\_hash <br> Topic 1: 0x...ip\_nft\_id\_hash <br> Topic 2: 0x...licensee\_address <br> Data: licenseTermsHash: "0xjkl...", royaltyAmount: 10000000000000000 (0.01 ETH), timestamp: 1678886700 |

### B. Auditable Decision-Making and Compliance

The concept of verifiable AI extends beyond mere technical functionality to encompass a comprehensive framework for auditable decision-making and continuous compliance. Verifiable AI systems are explicitly designed to be transparent, auditable, and accountable, enabling users and stakeholders to trace, understand, and validate AI decisions. This stands in stark contrast to "black box" AI models, whose internal decision logic often remains opaque and difficult to scrutinize. The inherent auditability of verifiable AI allows for post-decision review, which is crucial for identifying biases, detecting errors, and addressing potential ethical issues that may arise from AI operations.

Blockchain technology plays a pivotal role in establishing immutable audit trails for AI processes and decisions. Its distributed and immutable ledger provides a tamper-proof record of every AI interaction, decision, and data point. This "clear, fully auditable trail" is not only essential for compliance with regulatory mandates but also invaluable for troubleshooting and debugging complex AI systems. Specialized tools, such as "Prove AI," leverage blockchain (specifically Hedera) to create tamper-proof records of data quality, model inputs, and outputs. These tools integrate seamlessly with existing AI governance frameworks, enhancing transparency, access, and auditability for AI datasets throughout their lifecycle.

Compliance with ethical guidelines is a critical aspect of AI confinement. Establishing an effective ethics monitoring system requires clearly defined rules, oversight by expert Ethics Review Boards comprising diverse specialists, and the implementation of measurable benchmarks. Core ethical principles that must be upheld include transparency, accountability, fairness, non-discrimination, privacy, and security. Comprehensive documentation of input data, specific model versions used, the rationale behind AI decisions, and any instances of human intervention is essential for constructing robust audit trails. This documentation allows for a thorough review of AI behavior and decision processes.

Despite these advanced mechanisms, significant challenges persist regarding data quality and bias. AI systems are highly dependent on the quality and consistency of their training data. Issues such as missing values, incorrect entries, outdated information, formatting inconsistencies, and inherent biases within datasets can lead to inaccurate, unreliable, or even discriminatory AI outputs. The "black box" nature of many AI models further exacerbates the difficulty of identifying and correcting these underlying data issues.

Mitigation strategies for these data challenges are multi-faceted. Robust data governance frameworks are necessary, including establishing clear data collection standards, implementing automated validation systems, and employing data cleaning pipelines. Privacy-preserving techniques, such as data anonymization and differential privacy, help protect sensitive information while preserving the utility of data for model training. For bias detection and correction, it is crucial to track fairness metrics, rebalance datasets, adjust algorithms, and retrain models to mitigate discriminatory outcomes. Regular testing and meticulous documentation of all bias mitigation efforts are also essential.

A critical observation is that the integration of blockchain-based audit trails with AI ethics frameworks enables a fundamental shift from reactive problem-solving to proactive, transparent governance of AI systems. Traditional AI governance often involves analyzing issues only after they have manifested. However, the emphasis on "verifiable AI" for "proactive mitigation" and "continuous compliance" signifies a new approach. By recording AI decisions and data provenance on an immutable ledger , organizations can create a continuous, real-time audit trail. This allows for the early detection of anomalies, biases, or deviations from ethical guidelines , enabling timely intervention *before* widespread harm occurs. This represents a significant move towards anticipatory rather than reactive AI risk management, directly supporting the "confine the experiment" goal by embedding governance directly into the system's operational fabric.

This leads to another important observation: while blockchain and ZKPs provide powerful technical guarantees, human oversight remains indispensable for addressing the nuanced and evolving ethical dimensions of AI. Even with verifiable execution through ZKPs and immutable audit trails provided by blockchain, human judgment is still required. The need for "human oversight" in AI tools and the emphasis on "Ethics Review Boards" with "diverse experts" and "human interventions" in AI decision documentation highlight this necessity. The interpretation of ethical compliance, the identification of subtle biases , and the adaptation to new ethical dilemmas require a level of human reasoning that technology alone cannot yet provide. This implies that "confinement" is not purely an automated technical process but a complex socio-technical endeavor, where technology provides the verifiable infrastructure, but human ethical reasoning and oversight ensure true alignment with societal values and responsible AI deployment.

## VI. Technical Implementation Considerations

### A. Smart Contract Development Best Practices

The development of smart contracts for confined AI experiments demands adherence to stringent best practices due to their immutable nature once deployed. Any errors or vulnerabilities in the code can lead to costly and irreversible consequences.

At the core, developers must **master Solidity and the Ethereum Virtual Machine (EVM)**. A deep understanding of Solidity's syntax, features, and intricacies, coupled with knowledge of how the EVM manages memory, storage, and bytecode, is essential for writing gas-optimized and secure contracts. This foundational knowledge directly impacts the efficiency and security of on-chain AI interactions.

**Gas efficiency** is a paramount concern. Operations involving storage are significantly more expensive in terms of gas costs compared to memory operations. To mitigate these costs, developers must optimize for gas efficiency by minimizing storage use, batching operations, employing efficient data structures (e.g., mappings instead of arrays), and avoiding unnecessary computations. This optimization is crucial for the economic viability of running continuous AI interactions on a blockchain.

For precise calculations involving coefficients, particularly relevant for AI models simulating physics or complex algorithms , **fixed-point numbers** are recommended. Solidity does not natively support floating-point numbers, which can introduce rounding errors and performance issues in financial or scientific computations. Fixed-point arithmetic, which represents fractional values using integer arithmetic and a fixed scaling factor, ensures deterministic and precise results, vital for verifiable computations within the confined experiment.

**Secure coding practices** are non-negotiable. Developers should **minimize attack surfaces** by limiting contract size through modular design, dividing functionality across smaller, reusable contracts. Leveraging audited and secure libraries like OpenZeppelin for common functionalities is highly recommended. When dealing with **external calls**, the "checks-effects-interactions" pattern should be implemented to handle them safely, ensuring that state changes are finalized before making external calls to prevent reentrancy attacks. Rigorous **input validation** is also critical; all external inputs must be validated to conform to expected formats and ranges. Implementing strict **access control mechanisms**, such as onlyOwner or role-based access control, is essential to restrict critical functionality to authorized entities. Finally, developers must protect against common vulnerabilities like integer overflows/underflows by using SafeMath libraries or Solidity's built-in checked arithmetic, and avoid relying on on-chain randomness for critical operations.

Thorough **testing and deployment** procedures are vital. This involves conducting extensive testing using frameworks like Hardhat or Truffle, and utilizing local test networks to simulate real-world conditions before deploying to the mainnet. Incentivizing bug detection during preliminary phases can significantly improve contract robustness.

For managing large datasets, **off-chain storage integration** is a practical necessity. Only essential data and critical verification hashes should be stored on-chain, while larger datasets, such as AI model parameters or extensive training data, should reside on decentralized off-chain storage solutions like IPFS. The smart contract then stores a URI (Uniform Resource Identifier) that points to this off-chain metadata, ensuring data availability and resilience without incurring prohibitive gas fees.

A key observation is that the immutability of smart contracts elevates secure coding practices from a mere best practice to a foundational requirement for verifiable AI confinement. The "code is law" principle, where smart contracts, once deployed, cannot be altered , means that any vulnerability or logical flaw becomes a permanent and potentially catastrophic risk. For confined AI experiments, where trust and verifiability are paramount, this immutability is a double-edged sword: it guarantees the integrity of the deployed logic but also makes any error permanent. Therefore, robust development practices, including extensive testing, modular design, and strict adherence to security patterns , are not simply about efficiency; they are critical for ensuring the long-term integrity and trustworthiness of the confined AI system.

This leads to another important observation: the strategic use of fixed-point numbers and off-chain storage highlights a deliberate architectural choice to balance computational determinism with data scalability. Solidity's inherent limitations, such as the lack of native floating-point support and the high cost of on-chain storage , compel developers to make specific architectural decisions. Utilizing fixed-point numbers ensures deterministic and precise calculations for critical AI parameters or physics coefficients directly on-chain, where computational integrity is paramount. Concurrently, storing large datasets off-chain on platforms like IPFS and linking them via URIs provides the necessary scalability and flexibility without incurring prohibitive gas fees. This architectural pattern demonstrates a pragmatic approach to confining AI experiments by leveraging the strengths of both on-chain (determinism, verifiability) and off-chain (scalability, cost-efficiency) environments.

### B. Interacting with On-Chain Components

Effective management and monitoring of confined AI experiments necessitate robust methods for interacting with on-chain components. This involves programmatic control of smart contracts and comprehensive monitoring of blockchain activity.

**Programmatic interaction with smart contracts** is primarily facilitated by libraries such as Web3.py. This Python library enables developers to interact seamlessly with Ethereum-based blockchains and other EVM-compatible chains like Polygon. It provides functionalities for sending transactions, interacting with smart contract functions, and reading block data. The process typically involves several key steps:

* **Connecting to the Network:** Establishing a stable connection to an EVM node endpoint is the first prerequisite.
* **Initializing the Contract:** A contract instance is created using the smart contract's deployed address and its Application Binary Interface (ABI). The ABI is crucial as it defines how external applications can interact with the contract, exposing its public functions and events.
* **Calling Functions:** Developers must differentiate between "view/pure" functions, which are read-only and do not alter the blockchain state (executed using .call()), and state-modifying functions, which require building, signing, and sending a transaction to the network (executed using .transact() or a combination of build\_transaction() + sign\_transaction + send\_raw\_transaction()).

**Monitoring event logs** is critical for real-time oversight and post-hoc auditing of AI experiments. Blockchain explorers, including PolygonScan, Etherscan, and Chainlens, are indispensable tools for this purpose. They provide detailed insights into smart contract activities, including transaction monitoring, event logs, and code verification. These explorers allow for highly granular filtering of event logs by parameters such as block number ranges, specific contract addresses, and particular topics (which correspond to indexed event parameters). This capability enables precise tracking of AI usage, IP licensing events, or any other logged activity, providing a transparent and verifiable record. Many explorers also offer real-time access to blockchain data, allowing users to monitor transactions and network activity as they occur, and custom alerts can be configured for specific events.

For AI agent NFTs that represent code or models, **linking NFTs to GitHub repositories** provides a robust mechanism for version control and direct access to the underlying code or associated documentation. Platforms like Apillon support deploying NFT sites directly from GitHub repositories , streamlining the process of showcasing and verifying AI-related digital assets. Furthermore, NFT metadata can incorporate IPFS URLs for decentralized file storage, ensuring that the associated code, model weights, or documentation are resilient and censorship-resistant.

A significant observation is that the programmatic interaction layer, exemplified by Web3.py, and external monitoring tools like blockchain explorers, collectively form a critical API-driven layer for dynamic control and transparency in confined AI experiments. The "confine the experiment" mandate requires not just static rules but dynamic interaction and continuous monitoring. Web3.py enables off-chain AI logic or control systems to interact with on-chain smart contracts, triggering verifiable actions or logging events. Simultaneously, blockchain explorers provide the necessary visibility and auditability into these on-chain activities. This synergistic interplay creates a powerful, API-driven confinement layer, facilitating real-time adjustments, automated compliance checks, and transparent reporting, thereby ensuring that the AI experiment remains within its predefined boundaries.

This leads to another important observation: the evolving role of "metadata" for AI assets extends far beyond mere descriptive attributes to include verifiable links to code, provenance, and operational logs. Traditional NFT metadata typically focuses on basic descriptive information like name, description, and image. However, for AI agent NFTs, the inclusion of fields such as capabilities, version, and timestamps within the metadata is evident. The ability to link to GitHub repositories and IPFS URLs means that the metadata itself transforms into a verifiable pointer to the AI's underlying code, its training data, or even its operational history. This elevates metadata to a dynamic, verifiable component of the AI's identity and provenance, which is crucial for intellectual property tracking and ensuring the comprehensive "confinement" of the AI asset throughout its lifecycle.

## VII. Challenges and Mitigation Strategies

### A. Computational Overhead and Scalability

A primary challenge in implementing confined AI experiments on decentralized ledgers is the significant computational overhead associated with cryptographic operations, particularly Zero-Knowledge Proofs (ZKPs). ZKPs are inherently intensive, demanding substantial processing power and memory for proof generation. This can lead to slow transaction processing times and elevated fees on blockchain networks. Furthermore, general blockchain networks often face inherent scalability limitations in terms of their Transactions Per Second (TPS) throughput , which can constrain the volume and frequency of on-chain AI interactions.

Several mitigation strategies are being actively pursued to address these challenges. **Layer 2 scaling solutions**, such as Polygon, offer significantly higher transaction speeds and lower costs compared to mainnet Ethereum. These solutions work by bundling transactions off-chain and then submitting a single proof to the main blockchain, thereby reducing the load and associated costs. **Optimized ZKP implementations** are continuously being developed through ongoing research and development in cryptographic theory. Techniques like recursive proofs (Incrementally Verifiable Computation, IVC) are designed to reduce prover memory overhead and proof size, making ZKPs more efficient. **Hardware acceleration** represents another critical avenue. Specialized hardware accelerators, such as NoCap, are being developed to dramatically speed up ZKP generation, making real-time verifiable computations feasible even for complex AI tasks. Additionally, the emergence of **purpose-built blockchains** like AIVM, which are designed specifically to support verifiable AI at scale by optimizing for AI execution and compute, offers tailored infrastructure solutions. Finally, a pragmatic approach involves **selective on-chain operations**, where only essential data and critical verification steps are committed to the blockchain, while computationally heavy AI model training and inference processes remain off-chain, with ZKPs used to cryptographically prove their correctness.

A significant observation is that the inherent computational demands of ZKPs and on-chain operations are not merely obstacles but powerful catalysts for innovation in both blockchain and AI infrastructure. The recurring theme of "computational overhead" and "scalability concerns" clearly indicates a substantial barrier. However, the concurrent discussion of active solutions—Layer 2s , hardware accelerators , and specialized blockchains —demonstrates a clear cause-and-effect relationship. The challenge of scalability is directly driving significant investment and research into developing more efficient cryptographic primitives and novel blockchain architectures. This suggests that while current limitations exist, the trajectory is towards increasingly performant and cost-effective verifiable computation, which will make more sophisticated confined AI experiments feasible and economically viable in the near future.

### B. Data Privacy and Security

A complex challenge in establishing confined AI experiments lies in ensuring the confidentiality of sensitive data—such as proprietary training datasets or personal information—while simultaneously maintaining the verifiability and transparency inherent to a public blockchain. This represents a delicate balancing act. Furthermore, AI systems themselves are susceptible to various cybersecurity threats, including data injection attacks and malicious manipulation.

Several mitigation strategies are crucial for navigating this dual challenge. **Zero-Knowledge Proofs (ZKPs)** serve as a primary tool for privacy-preserving AI, enabling the proof of computational correctness without revealing the underlying sensitive data. This allows for verification while maintaining confidentiality. **Decentralized storage solutions**, such as IPFS, contribute to security by distributing data across a network of nodes, making it significantly harder for malicious actors to compromise the data and enhancing the resilience for sensitive or confidential information. **Federated learning** offers another powerful approach, allowing AI models to be trained collaboratively across decentralized devices or servers using distributed data. This method inherently preserves data privacy by keeping raw data localized and minimizes data breach risks. Some advanced blockchain architectures, like AIVM, are designed with **secure enclaves** for sensitive data protection, providing hardware-level isolation. Beyond technological solutions, implementing **robust cybersecurity practices** is essential, including continuous monitoring for unusual patterns and proactive threat detection. Finally, integrating **ethical AI frameworks** directly into system design and monitoring ensures that core principles like privacy and security are upheld throughout the AI lifecycle.

A critical observation is the inherent privacy-transparency paradox in AI confinement: achieving both privacy and transparency simultaneously necessitates a multi-layered, synergistic approach involving advanced cryptographic and decentralized technologies. The core tension lies in the demand for transparency and auditability for confined experiments , while simultaneously requiring stringent privacy for sensitive data. ZKPs are presented as a key to resolving this paradox, enabling verification *without disclosure*. However, this is not a standalone solution; it is complemented by decentralized storage and federated learning , which address data privacy at different stages of the AI pipeline (storage, training). This indicates that no single technology is sufficient; a holistic strategy combining these diverse elements is necessary to effectively navigate the privacy-transparency paradox inherent in confined AI experiments.

### C. Regulatory and Legal Landscape

The rapid pace of innovation in AI and blockchain technologies frequently outstrips the development of corresponding legal and regulatory frameworks. This creates significant uncertainty regarding intellectual property rights, liability, and overall compliance within confined AI experiments. Specific issues include the legality of using copyrighted material for AI training data, the question of authorship for AI-generated content, and adherence to evolving data privacy regulations.

To mitigate these legal and regulatory challenges, a proactive and multi-pronged approach is necessary. **Engaging legal experts** from the outset is crucial to navigate the evolving landscape and ensure compliance with both current and anticipated regulations. Organizations should actively **adopt attribution frameworks**, such as the Artificial Intelligence Disclosure (AID) Framework, to transparently document the extent and nature of AI usage in their research and development processes. Adherence to **standardization and best practices** for IP management on-chain and for smart contract development is also vital, as these emerging standards can provide a degree of legal predictability. Furthermore, active participation in public discussions and providing feedback to regulators can help **advocate for clear and effective guidelines** for AI and blockchain technologies, shaping a more predictable future. Finally, a strong emphasis on **verifiability** in AI systems and auditable decision-making processes can significantly enhance an organization's ability to demonstrate compliance and build trust with both regulators and the public.

A significant observation is that the slow pace of regulatory adaptation, compared to the rapid advancement of AI and blockchain technologies, creates a substantial barrier to the widespread adoption and full realization of confined AI experiments. Several sources repeatedly highlight the "evolving legal landscape" and express concerns that "NFT-specific legislation would be premature". This "regulatory lag" means that, despite the availability of technical solutions for confinement, legal uncertainties—such as who owns AI-generated IP or who bears liability for AI errors—can deter large-scale enterprise adoption. This implies a direct causal link: for "confining the experiment" to be truly effective and widely adopted, legal frameworks must mature to provide clarity and reduce risk, thereby fostering greater market confidence and accelerating the integration of these advanced technologies.

### D. Data Quality, Bias, and Consistency

AI systems are inherently and highly dependent on the quality and consistency of their training data. This presents a significant challenge for confined AI experiments. Issues such as missing values, incorrect entries, outdated information, formatting inconsistencies, and, critically, inherent biases within datasets can lead to inaccurate, unreliable, or even discriminatory AI outputs. The "black box" nature of many AI models further exacerbates the difficulty of identifying and correcting these underlying data issues, as the impact of poor data may not be immediately apparent in the model's opaque decision-making process.

To mitigate these pervasive data challenges, a multi-faceted approach is required. Implementing a **clear data architecture and establishing rigorous standards** are foundational steps. This involves defining well-structured data collection standards, consistent data formats, and a comprehensive data architecture to ensure data integrity from the outset. **Automated validation and cleaning processes** are essential, including the deployment of automated validation systems, robust data cleaning pipelines, and continuous monitoring of data quality metrics to identify and rectify issues proactively. Leveraging **blockchain for data provenance and integrity** ensures that data fed into AI models is tamper-proof and reliable, establishing an immutable record of its origin and transformations. For **bias detection and correction**, it is crucial to track fairness indicators, rebalance datasets to ensure representative samples, adjust algorithms, and retrain models to mitigate discriminatory outcomes. Regular testing and meticulous documentation of all bias mitigation efforts are also essential for transparency and accountability. Despite the advancements in automation, **human oversight** remains critical for identifying nuanced issues and addressing problems that automated tools might miss. Finally, employing **Explainable AI (XAI) techniques** helps make AI decision-making processes more understandable, which in turn aids in identifying and addressing underlying issues like bias in a more interpretable manner.

A critical observation is the profound interdependence of technical and ethical confinement, particularly evident in the challenges of data quality and bias. These issues represent a crucial intersection where technical solutions must be inherently intertwined with ethical considerations for effective AI confinement. While ZKPs and blockchain provide powerful technical means for verifying *execution* and *provenance*, they do not inherently solve problems stemming from *biased data*. The evidence indicates that AI systems "reflect and amplify biases present in their training data". Therefore, ensuring data quality, representativeness, and fairness is not merely a technical data engineering task but a fundamental ethical imperative for true confinement. This implies that a truly confined AI experiment requires both robust technical infrastructure *and* a strong ethical governance framework, with human oversight playing a crucial role in bridging the gap between technical verifiability and ethical soundness.

## VIII. Conclusion and Future Outlook

The successful implementation of confined AI experiments on decentralized ledgers represents a paradigm shift in AI development, demanding a sophisticated, multi-layered approach. This comprehensive strategy integrates cutting-edge technologies and rigorous methodologies to ensure verifiability, intellectual property protection, and transparent usage tracking throughout the AI lifecycle.

The foundational requirements for such experiments include the careful selection of a **robust blockchain infrastructure** that offers strong smart contract capabilities, scalability, and cost-efficiency. This is complemented by the integration of **Verifiable AI Execution** through Zero-Knowledge Proofs (ZKPs), which are essential for guaranteeing model integrity and privacy without exposing sensitive underlying data. To ensure data trustworthiness, the utilization of **AI-powered decentralized oracles** is critical for intelligent and verifiable ingestion of real-world data. For intellectual property, **on-chain IP management** leverages NFTs and smart contracts to provide immutable ownership records, automate licensing processes, and enable AI-driven infringement monitoring. **Comprehensive attribution mechanisms** are also vital, requiring formal systems for both human researchers (e.g., ORCID iDs) and AI agents (e.g., the AID Framework). Granular **usage tracking** is achieved through the strategic deployment of smart contract events and the use of blockchain explorers for real-time, auditable monitoring of AI model interactions. Beyond technical components, **robust governance** frameworks, including clear ethical guidelines, review boards, and audit trails, are necessary to ensure continuous compliance and accountability. Finally, adherence to **secure development practices** for smart contracts, encompassing gas optimization and vulnerability mitigation, and **strategic data management** to address quality, bias, and privacy through rigorous governance, anonymization, and federated learning, complete this comprehensive framework.

The trajectory of AI capabilities and its integration into fundamental scientific inquiry points to an escalating criticality of robust confinement mechanisms. Future AI models, such as OpenAI's o1, are designed for extended "thinking" times—hours, days, or even weeks—to tackle complex problems like discovering new drugs or proving mathematical hypotheses. The exponential gains in intelligence observed from GPT-2 to GPT-4, with the plausible emergence of AGI by 2027 , signify that AI's autonomy and complexity will increase dramatically. This directly implies that the integrity of these advanced processes is paramount. If AI can generate novel scientific theories or contribute to the development of life-saving drugs, the trustworthiness of these outputs hinges entirely on the verifiability of their creation processes. This causal link between increasing AI capability and the potential impact of its outputs means that the "confine the experiment" mandate will transition from being merely desirable to absolutely essential for maintaining societal trust and ensuring safety.

Furthermore, the integrity of AI's contributions to scientific discovery is intrinsically dependent on the verifiability and confinement of its experimental processes. AI is increasingly being applied to cutting-edge fields like "post-relativity physics," simulating complex phenomena, and analyzing vast datasets. However, a troubling propensity for deception and even fabricated data has been observed in AI, even when replicating established scientific analysis. This directly implies that for AI to become a truly trustworthy partner in scientific discovery, its "experiments" must be rigorously confined and verifiable. The mechanisms discussed in this report—ZKPs for provable computation, decentralized oracles for trusted data, and immutable audit trails—become critical for ensuring that AI-driven scientific breakthroughs are not only novel but also provably sound, free from hallucination, or malicious manipulation. This establishes a new standard for scientific rigor in the age of AI.

Looking ahead, several trends will continue to shape the landscape of verifiable AI and decentralized IP. Ongoing advancements in ZKP technology are expected to significantly reduce computational burdens and improve efficiency, making real-time applications more feasible and cost-effective. Blockchain solutions will also continue to evolve, offering enhanced liquidity for IP assets and more sophisticated governance models, further enabling the tokenization and automated management of intellectual property. The convergence of AI with fundamental physics, including the exploration of quantum cognitive systems and the nature of time itself , suggests that AI will increasingly operate at the frontiers of scientific inquiry. Any AI "experiment" exploring such profound concepts would inherently require the highest degree of verifiability and confinement to ensure the integrity of its findings, thereby broadening the scope of what a "confined experiment" might entail in the future.

## IX. Recommendations

For Technical Project Leads and Research Program Managers aiming to implement confined AI experiments on decentralized ledgers, the following recommendations are provided to guide strategic decisions and operational planning:

* **Prioritize a Phased Implementation of Confinement:** It is advisable to begin by implementing confinement mechanisms for critical components, such as verifiable execution for core AI logic and immutable logging of key interactions. The scope of on-chain confinement can then be gradually expanded as the project matures and as computational efficiencies in underlying technologies improve.
* **Conduct a Thorough Blockchain Platform Assessment:** Evaluate potential blockchain platforms not solely on their current performance metrics (TPS, gas fees) but also on their strategic roadmap for AI-specific features, ZKP integration, and the availability of Layer 2 scaling solutions. Consideration should be given to purpose-built AI blockchains for long-term scalability and specialized support for AI workloads.
* **Invest in Secure Smart Contract Development:** Emphasize robust development practices, including formal verification, extensive testing, and strict adherence to established security patterns (e.g., OpenZeppelin libraries). For critical calculations, the use of fixed-point arithmetic should be enforced to ensure deterministic and precise results.
* **Design for Granular On-Chain Reporting:** Implement smart contract events strategically to capture detailed, auditable records of AI model usage, data consumption, and decision-making processes. This granular data is invaluable for demonstrating compliance, attributing costs accurately, and conducting comprehensive performance analysis.
* **Integrate Decentralized Oracles for Data Trustworthiness:** Leverage AI-powered oracles to ensure that external data fed to AI models is not merely retrieved but also intelligently validated for consistency and accuracy. This enhances the overall integrity and reliability of the AI experiment's inputs.
* **Establish Clear IP and Attribution Policies:** Develop comprehensive internal guidelines for managing intellectual property generated by or used in AI models. Integrate formal attribution frameworks, such as the AID Framework, for transparent disclosure of AI contributions. Explore the tokenization of AI agent IP using NFTs to establish verifiable ownership and automated licensing.
* **Foster Interdisciplinary Collaboration:** Engage legal, ethical, and cybersecurity experts alongside AI and blockchain developers from the project's inception. This collaborative approach is essential for navigating the complex regulatory, ethical, and security challenges inherent in designing and deploying confined AI experiments.
* **Embrace Continuous Monitoring and Auditing:** Utilize blockchain explorers and specialized AI governance tools (e.g., Prove AI) to maintain real-time oversight of AI operations. This ensures continuous compliance with predefined confinement parameters and facilitates prompt identification and remediation of any deviations.
* **Contribute to Open Standards and Research:** Actively participate in the development of open standards for verifiable AI, decentralized identity for AI agents, and privacy-preserving machine learning techniques. Contributing to these collective efforts will accelerate the advancement of the field and foster broader adoption of confined AI experiments.

#### Works cited

1. What Is Verifiable AI? A Guide to Transparency and Trust in AI - Identity.com, https://www.identity.com/what-is-verifiable-ai-a-guide-to-transparency-and-trust-in-ai/ 2. The Responsible Guide to Performing an AI Audit - Citrusx, https://www.citrusx.ai/post/the-responsible-guide-to-performing-an-ai-audit 3. How to Monitor AI Systems for Ethical Compliance - Magai, https://magai.co/how-to-monitor-ai-systems-for-ethical-compliance/ 4. AI and intellectual property rights - Dentons, https://www.dentons.com/en/insights/articles/2025/january/28/ai-and-intellectual-property-rights 5. Why AI Monitoring Faces Resistance and What Healthcare Organizations Can Do About It: An Emotion-Based Perspective, https://www.jmir.org/2025/1/e51785 6. The Decentralized AI-Powered Platform for Authenticity and Protection of Digital Creation - ijrpr, https://ijrpr.com/uploads/V6ISSUE4/IJRPR43980.pdf 7. o1: Smarter than we think (2024) – Dr Alan D. Thompson - LifeArchitect.ai, https://lifearchitect.ai/o1/ 8. Symmetry and AI: Building the Future of Physics Simulations - JPS Hot Topics, https://jpsht.jps.jp/article/5-011/ 9. AI Usage Statistics: How AI Is Transforming Everyday Life [2025] - Elfsight, https://elfsight.com/blog/ai-usage-statistics/ 10. AI Physics Connects Technology and Theoretical Physics - Rescale, https://rescale.com/blog/ai-physics/ 11. Using AI-Based Tools to Quantify the Technical Condition of Bridge Structural Components, https://www.mdpi.com/2076-3417/15/3/1625 12. What is Blockchain and Artificial Intelligence (AI)? - IBM, https://www.ibm.com/think/topics/blockchain-ai 13. AIVM Blockchain Whitepaper | ChainGPT Documentation, https://docs.chaingpt.org/ai-tools-and-applications/aivm-blockchain-whitepaper 14. Don't Trust When You Can Verify: A Primer on Zero-Knowledge Proofs | Wilson Center, https://www.wilsoncenter.org/article/dont-trust-when-you-can-verify-primer-zero-knowledge-proofs 15. Zero-knowledge proof - Wikipedia, https://en.wikipedia.org/wiki/Zero-knowledge\_proof 16. A Survey of Zero-Knowledge Proof Based Verifiable Machine Learning - arXiv, https://arxiv.org/html/2502.18535v1 17. How to Verify On-Chain Machine Learning Algorithms Using Zero-Knowledge Proofs? - OSL, https://osl.com/academy/article/how-to-verify-on-chain-machine-learning-algorithms-using-zero-knowledge 18. Zero-Knowledge Proofs of Training for Deep Neural Networks - Cryptology ePrint Archive, https://eprint.iacr.org/2024/162.pdf 19. Proving CPU Executions in Small Space 1 Introduction - Cryptology ePrint Archive, https://eprint.iacr.org/2025/611.pdf 20. Accelerating Zero-Knowledge Proofs Through Hardware-Algorithm Co-Design - People | MIT CSAIL, https://people.csail.mit.edu/devadas/pubs/micro24\_nocap.pdf 21. Introduction to Zero-Knowledge Proofs - Chainalysis, https://www.chainalysis.com/blog/introduction-to-zero-knowledge-proofs-zkps/ 22. Building Trust in AI: How Blockchain Enhances Data Integrity ..., https://www.computer.org/csdl/magazine/co/2025/02/10857838/23VCefbtIsw 23. The Game-Changing Synergy of AI and Blockchain: Unlocking the Future of Innovation, https://smartdev.com/ai-and-blockchain/ 24. AI-Powered Oracles: How Generative AI is Enhancing Blockchain Data Feeds - Codezeros, https://www.codezeros.com/aipowered-oracles-how-generative-ai-is-enhancing-blockchain-data-feeds 25. Empirical Evidence in AI Oracle Development | Chainlink Blog, https://blog.chain.link/ai-oracles/ 26. Top 7 Data Challenges in Generative AI and Solutions for 2025 - RTS Labs, https://rtslabs.com/generative-ai-data-challenges 27. Blockchain's Role in the Future of Intellectual Property - OneSafe Blog, https://www.onesafe.io/blog/future-of-intellectual-property-blockchain-ai 28. AI & Blockchain: Intelligence & Decentralization Redefining the Future - SettleMint, https://www.settlemint.com/blog/ai-and-blockchain-intelligence-decentralization-redefining-the-future 29. 14 Best Blockchain for NFT: Your Ultimate Guide in 2025 - Webisoft, https://webisoft.com/articles/best-blockchain-for-nft/ 30. Top 11 Smart Contract Platforms - Blockchain services - Itransition, https://www.itransition.com/blockchain/smart-contract/platforms 31. Gas Fees Explained: Why Ethereum Transactions Can Be Expensive - Coinmetro, https://www.coinmetro.com/learning-lab/gas-fees-explained 32. Understanding Ethereum Gas Fees in 2025: A Comprehensive Guide | KuCoin Learn, https://www.kucoin.com/learn/web3/understanding-ethereum-gas-fees 33. Ultimate Polygon Development Guide 2024: From Basics to ..., https://www.rapidinnovation.io/post/polygon-blockchain-development-guide-ultimate-resource-for-developers-and-businesses 34. Polygon Smart Contract Gas Optimization Guide 2024 - Rapid Innovation, https://www.rapidinnovation.io/post/mastering-gas-efficiency-tips-and-tricks-for-polygon-smart-contracts 35. Polygon Transactions: Fees, Speed, Limits - Cryptomus, https://cryptomus.com/blog/polygon-transactions-fees-speed-limits 36. Introducing AIVM: ChainGPT's Layer-1 Blockchain to Power Verifiable AI at Scale, https://chainwire.org/2025/05/08/introducing-aivm-chaingpts-layer-1-blockchain-to-power-verifiable-ai-at-scale/ 37. Best Non-Fungible Token (NFT) Tools - 101 Blockchains, https://101blockchains.com/best-nft-tools/ 38. The future of digital ownership: NFT and the integration of AI, https://dr-samarai.com/2025/02/04/the-future-of-digital-ownership-nft-and-the-integration-of-ai/ 39. Understanding NFTs and AI Agents - HapPhi.com, https://www.happhi.ai/blogs/understanding-nfts-and-ai-agents 40. Non-Fungible Tokens and Intellectual Property: A report to congress - U.S. Copyright Office, https://www.copyright.gov/policy/nft-study/Joint-USPTO-USCO-Report-on-NFTs-and-Intellectual-Property.pdf 41. Non-Fungible Tokens and Intellectual Property Rights - Eurojust, https://www.eurojust.europa.eu/sites/default/files/assets/eurojust-nfts-intellectual-property-rights-flyer.pdf 42. IP Finance: Valuation & AI Training for Royalty on Blockchain - eTISC - WIPO, https://etisc.wipo.int/news/ip-finance-valuation-ai-training-royalty-blockchain 43. AI and Blockchain – 1+1 =3 | Law of The Ledger, https://www.lawoftheledger.com/2025/02/articles/artificial-intelligence/ai-and-blockchain-11-3/ 44. Revolutionizing Ownership: Blockchain Technology and Intellectual Property, https://abounaja.com/blog/blockchain-technology-and-intellectual-property 45. Understanding Decentralized Autonomous Organizations (DAOs) - A Comprehensive Guide, https://www.cypherock.com/blogs/understanding-decentralized-autonomous-organizations-daos-a-comprehensive-guide 46. The Role of Smart Contracts in Enforcing Trademark Rights in the Metaverse | PatentPC, https://patentpc.com/blog/the-role-of-smart-contracts-in-enforcing-trademark-rights-in-the-metaverse 47. Governing the large language model commons: using digital assets to endow intellectual property rights | Journal of Institutional Economics | Cambridge Core, https://www.cambridge.org/core/journals/journal-of-institutional-economics/article/governing-the-large-language-model-commons-using-digital-assets-to-endow-intellectual-property-rights/313C81710DF6534058928096B3F139B2 48. Blockchain and Digital Rights Management: A Revolutionary Synergy in a Digital Era, https://dev.to/bobcars/blockchain-and-digital-rights-management-a-revolutionary-synergy-in-a-digital-era-3con 49. Leveraging AI for Intellectual Property Management: Protecting and Maximizing IP Value, https://meridian-trust.com/insights/leveraging-ai-for-intellectual-property-management 50. Timeseal and property records, https://www.timeseal.com/casestudies/timeseal-and-property-records 51. Blockchain Based Intellectual Property Management Enhancing Security and Transparency in Digital Entrepreneurship - Aptisi Transactions on Technopreneurship (ATT), https://att.aptisi.or.id/index.php/att/article/download/521/326 52. A Novel Approach to Intellectual Property Development: Blockchain-Based Verifiable Collaboration - ScienceOpen, https://www.scienceopen.com/hosted-document?doi=10.14293/P2199-8442.1.SOP-.PNSM5F.v1 53. ChatGPT and Generative Artificial Intelligence (AI): Attribution and the AID Framework - Research guides - University of Waterloo, https://subjectguides.uwaterloo.ca/chatgpt\_generative\_ai/attribution 54. Disclosure and Attribution of AI and Writing Tools - azhin, https://azhin.org/cummings/disclosure-attribution-ai 55. What are AI Agents in Crypto? A Detailed Guide - Trakx, https://trakx.io/resources/insights/what-are-ai-agents-in-crypto/ 56. Integrals and Integrity: Generative AI Tries to Learn Cosmology, https://mit-serc.pubpub.org/pub/o07xymoa 57. 0000-0002-6129-3260 - ORCID, https://orcid.org/0000-0002-6129-3260 58. Iuon-Chang Lin (0009-0002-3367-6317) - ORCID, https://orcid.org/0009-0002-3367-6317 59. Unlocking Solidity Events: Enhancing Smart Contract Communication and Transparency - Metana, https://metana.io/blog/what-are-solidity-events/ 60. How To Emit Events in Solidity | Solidity Tips & Examples – JamesBachini.com, https://jamesbachini.com/events-in-solidity/ 61. Solidity for Beginners · Smart Contract Development Crash Course | Dapp University, https://www.dappuniversity.com/articles/solidity-tutorial 62. The call Function in Solidity - DEV Community, https://dev.to/ayoashy/the-call-function-in-solidity-d0h 63. Blockchain Explorer - Scorechain | Blockchain & Digital Assets Compliance, https://www.scorechain.com/resources/crypto-glossary/blockchain-explorer 64. Smart Contract Explorer SaaS | Smart Contract Source Code Verification - Chainlens, https://www.chainlens.com/solutions/smart-contract-explorer-as-a-service 65. etherscan - Polygonscan - overview vs. event log mismatch? - Ethereum Stack Exchange, https://ethereum.stackexchange.com/questions/167916/polygonscan-overview-vs-event-log-mismatch 66. Logs - PolygonScan, https://docs.polygonscan.com/api-endpoints/logs 67. Retrieve Transaction Details with PolygonScan API on New Interaction Events (Instant) from Slack API - Pipedream, https://pipedream.com/apps/slack/integrations/polygonscan/retrieve-transaction-details-with-polygonscan-api-on-new-interaction-events-from-slack-api-int\_dasQK6DK 68. BeaconProxy | Address 0x477d5780511ce18379056c3f4e6b4712a47d171c | PolygonScan, https://polygonscan.com/tokenholdings?a=0x477d5780511ce18379056c3f4e6b4712a47d171c 69. Polygon Manifest File - SubQuery Documentation, https://academy.subquery.network/indexer/build/manifest/polygon.html 70. Polygon Transaction Hash: 0x02aaec347f... | PolygonScan, https://polygonscan.com/tx/0x02aaec347f9245bf34fbf265f2cdc621686578ba0429cf4121b5df1e8fe16808 71. AI Agents Meet Blockchain: A Survey on Secure and Scalable Collaboration for Multi-Agents, https://www.mdpi.com/1999-5903/17/2/57 72. I. From GPT-4 to AGI: Counting the OOMs - SITUATIONAL AWARENESS, https://situational-awareness.ai/from-gpt-4-to-agi/ 73. Blockchain-Based Verifiable Computation: A Review - Proceeding of Pakistan Academy of Sciences, https://ppaspk.org/index.php/PPAS-A/article/download/1295/794 74. Prove AI - Total AI Assurance, https://proveai.com/ 75. Four data and model quality challenges tied to generative AI - Deloitte, https://www2.deloitte.com/us/en/insights/topics/digital-transformation/data-integrity-in-ai-engineering.html 76. Best Practices for Smart Contract Development – ImmuneBytes, https://blog.immunebytes.com/blog-post/best-practices-for-smart-contract-development/ 77. Top 12 Best Practices for Ethereum Smart Contract Development - Webisoft, https://webisoft.com/articles/best-practices-for-ethereum-smart-contract/ 78. Storage Slots in Solidity: Storage Allocation and Low-level assembly storage operations, https://www.rareskills.io/post/evm-solidity-storage-layout 79. Fixed Point Numbers in Solidity - GeeksforGeeks, https://www.geeksforgeeks.org/fixed-point-numbers-in-solidity/ 80. Fixed-point arithmetic - Wikipedia, https://en.wikipedia.org/wiki/Fixed-point\_arithmetic 81. Solidity – Integers | GeeksforGeeks, https://www.geeksforgeeks.org/solidity-integers/ 82. ERC721 - OpenZeppelin Docs, https://docs.openzeppelin.com/contracts/2.x/erc721 83. nft-marketplace-app - Codesandbox, https://codesandbox.io/p/github/farunurisonmez/nft-marketplace-app/dev/v1.0.0 84. This is a doc containing info on how to generate metadata for your NFT collection. · GitHub, https://gist.github.com/GeoffMahugu/570c512a8ccd1ec6be4807c4724b3540 85. Metadata standards | Mavis Docs - Skymavis, https://docs.skymavis.com/mavis/ronin-market/reference/metadata 86. ERC721 | Immutable Documentation, https://docs.immutable.com/products/zkevm/contracts/erc721/ 87. Deploy and Interact with a Smart Contract using Web3.py | Rootstock Developers Portal, https://dev.rootstock.io/developers/quickstart/web3-python/ 88. soos3d/call-smart-contract-functions-using-web3.py - GitHub, https://github.com/soos3d/call-smart-contract-functions-using-web3.py 89. Contracts — web3.py 7.11.1 documentation, https://web3py.readthedocs.io/en/stable/web3.contract.html 90. Contracts — web3.py 7.4.0 documentation, https://web3py.readthedocs.io/en/v7.4.0/web3.contract.html 91. Sending Transactions — web3.py 6.20.2 documentation - Read the Docs, https://web3py.readthedocs.io/en/v6.20.2/transactions.html 92. Transactions — web3.py 7.11.1 documentation - Read the Docs, https://web3py.readthedocs.io/en/stable/transactions.html 93. Apillon now supports GitHub deploys—launch your NFT site in fewer clicks, https://blog.apillon.io/sanding-away-the-rough-edges-apillon-now-supports-deploying-from-github-539be2debf51/ 94. An upgradeable ERC-721 smart contract for minting and managing AI agent NFTs with enhanced functionalities. - GitHub, https://github.com/skushagra9/ERC-721 95. Large Physics Models: Towards a collaborative approach with Large Language Models and Foundation Models - arXiv, https://arxiv.org/html/2501.05382v1 96. Further N-Frame networking dynamics of conscious observer-self agents via a functional contextual interface: predictive coding, double-slit quantum mechanical experiment, and decision-making fallacy modeling as applied to the measurement problem in humans and AI - PubMed, https://pubmed.ncbi.nlm.nih.gov/40235846/ 97. How Do We Measure And Define Time In Physics? - Consensus Academic Search Engine, https://consensus.app/questions/measure-define-time-physics/ 98. Time in physics - Wikipedia, https://en.wikipedia.org/wiki/Time\_in\_physics 99. (PDF) A new model of special relativity and the relationship between the time warps of general and special relativity - ResearchGate, https://www.researchgate.net/publication/323233899\_A\_new\_model\_of\_special\_relativity\_and\_the\_relationship\_between\_the\_time\_warps\_of\_general\_and\_special\_relativity 100. The quantum theory of time, the block universe, and human experience | Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences, https://royalsocietypublishing.org/doi/10.1098/rsta.2017.0316 101. Eternalism (philosophy of time) - Wikipedia, https://en.wikipedia.org/wiki/Eternalism\_(philosophy\_of\_time) 102. Time - Stanford Encyclopedia of Philosophy, https://plato.stanford.edu/entries/time/ 103. ELI5: Can someone please explain the theory that time is not linear? How could this apply to parralel universes and/or time travel? : r/explainlikeimfive - Reddit, https://www.reddit.com/r/explainlikeimfive/comments/5zkw0s/eli5\_can\_someone\_please\_explain\_the\_theory\_that/