MEMORANDUM

To: Crypto Task Force Meeting Log
From: Crypto Task Force Staff
Re: Meeting with Representatives of Lagrange Labs Inc.

On September 12, 2025, Crypto Task Force Staff met with representatives from Lagrange Labs Inc.

The topic discussed was approaches to addressing issues related to regulation of crypto assets. Lagrange Labs Inc. representatives provided the attached documents, which were discussed during the meeting.

Attendees (Lagrange Labs):

- Ismael Hishon-Rezaizadeh, Chief Executive Officer – to provide company vision and strategic alignment.
- Brian Novell, Esq., Head of Business Development – to cover partnership opportunities and business strategy.
- Babis Papamanthou, Chief Scientist and co-director of the Applied Cryptography Lab at Yale University – to provide technical depth on our verifiable computation and modular rollup research.

Proposed Agenda:

The meeting will begin with introductions from both sides to establish context and clarify the objectives of our discussion. We will share Lagrange Labs' broader vision, highlighting our work in the rapidly evolving landscape of Web3. This will provide a strategic foundation by outlining the systemic challenges across the ecosystem and how Lagrange is positioned to help address them.

Next, we will outline our go-to-market approach and highlight the types of Web3 collaborations we are currently executing and pursuing. This section will illustrate how Lagrange is working with partners to unlock opportunities leveraging AI on-chain in safe and trustworthy ways, creating a basis for discussion on how our organizations can align along similar principles.

The conversation will then transition to a deeper technical exploration led by our Chief Scientist. This segment will focus on our verifiable computation framework as applied in the blockchain context, the state of our research on modular rollups, and the implications for scalability, security, and efficiency. This portion is designed to move beyond conceptual positioning and into the concrete mechanics of how our technology can be applied within Web3, while also giving your team the opportunity to raise technical questions or challenges.

At this point, we would like to create space for your perspective, with a particular emphasis on understanding how the SEC is currently applying and exploring artificial intelligence within the nuances of the crypto sector – whether in supervision, enforcement, market monitoring, or internal efficiency. We see this as an opportunity to learn directly how your Web3 priorities and initiatives are evolving, and to consider whether our research and capabilities might intersect with those objectives.

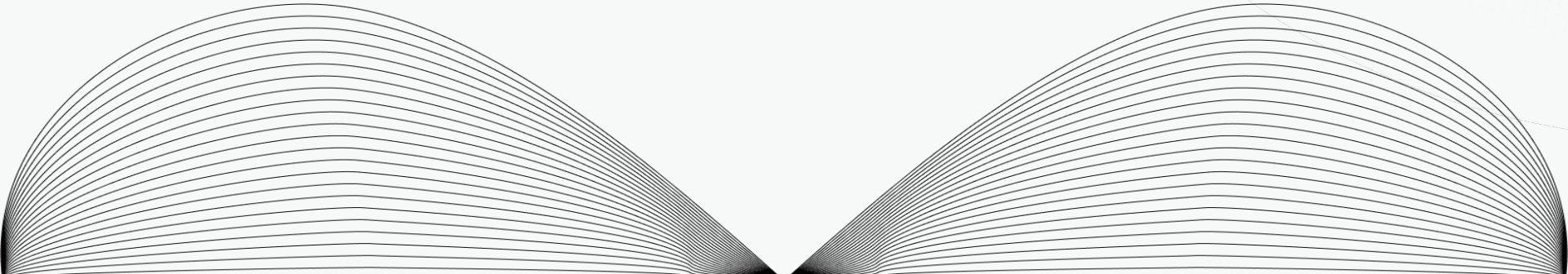
Building on that exchange, the session will move into a collaborative discussion of potential models for partnership. This will include possible technical pilots, integration opportunities, and pathways to joint engagement around crypto market infrastructure. We will also share illustrative examples of how Lagrange has structured similar relationships in the past, while remaining flexible to shape an approach that best aligns with your context.

Finally, the meeting will conclude with a consolidation of key points of alignment, an outline of potential next steps, and the assignment of follow-up actions. Our aim is to ensure that both sides leave the session with a clear understanding of where collaboration might be most impactful and how to carry the conversation forward in a concrete way.

The future of privacy is ZK.
The future of ZK is Lagrange

Ismael Hishon-Rezaizadeh
Co-Founder & CEO of Lagrange

You cannot trust what you cannot **verify**



(Q) How can we trust AI?

As AI becomes increasingly embedded into our everyday lives, we must be able to **prove** that AI models are producing results according to their expected functions. Trust in AI can only come through cryptographic verification.

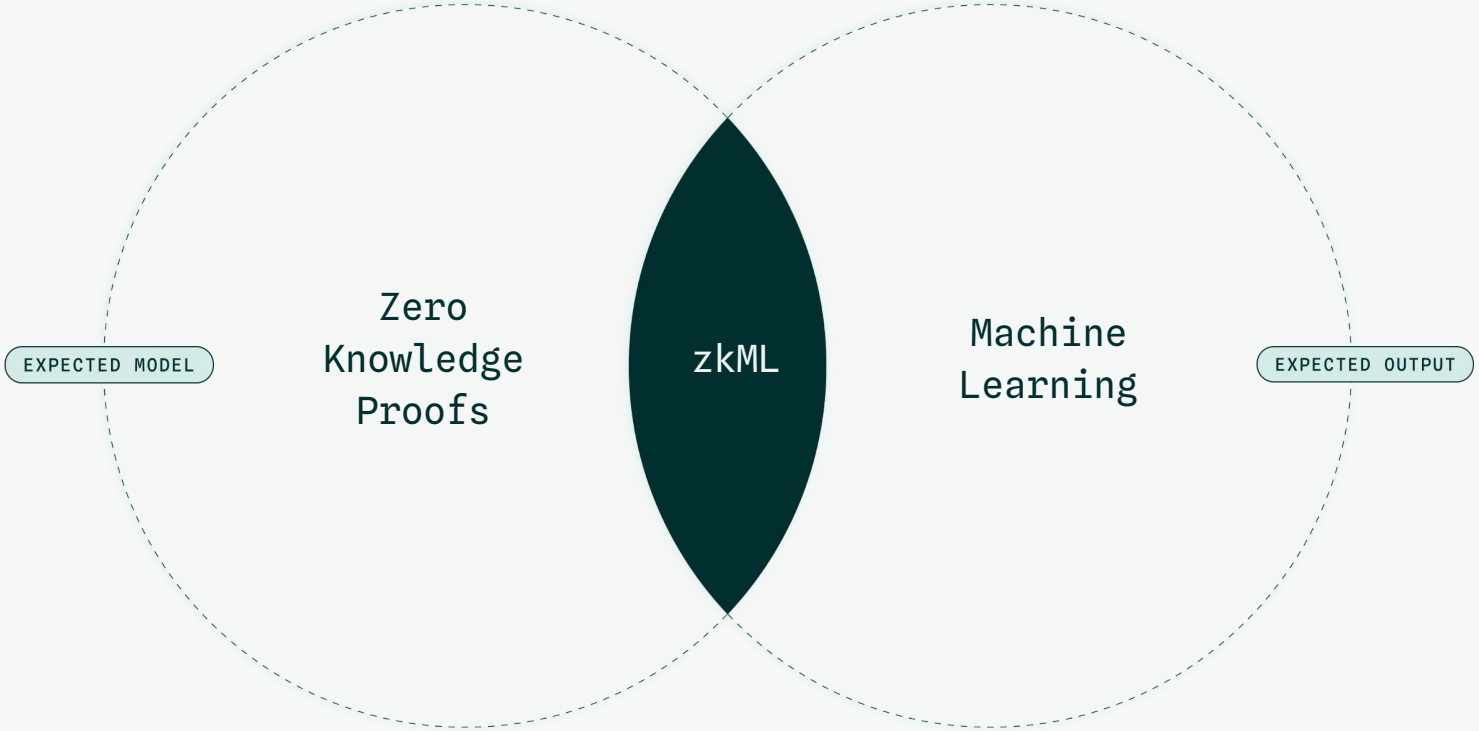
(A) Lagrange

Lagrange's DeepProve—the leading zkML library for machine learning inferences—makes verifiable AI faster and more scalable than ever before, **supporting popular LLMs like OpenAI's GPT-2, LLAMA, and Gemma.** With ZK proofs, DeepProve verifies that AI systems a) run the correct models and b) issue accurate results.

Lagrange Enables Safe, Private Compliance

Business Model

Lagrange's DeepProve enables both **bespoke and generic** models through self-service hosting and querying.



What is zkML?

zkML is a combination of ZKPs and machine learning (ML) that allows computations on ML models to be verified.

How Does DeepProve Work?

MODEL TRAINING

PREPROCESSING

[One time process]

First, a trained ML model is exported as an ONNX file, along with sample inputs.

The ONNX graph is then parsed (prepared for efficient proof generation), the sample inputs are used to compute the quantized version of the model, and prover/verifier keys are generated.

Preprocessing is a one-time step that does not need to be repeated.

PROVING

DeepProve runs the model on a given input and records how each node of the neural network processes data (also known as an "execution trace").

For every node, DeepProve generates a cryptographic proof that the computation was done correctly.

These individual proofs are then aggregated into a single, succinct proof that represents the entire model's correct execution.

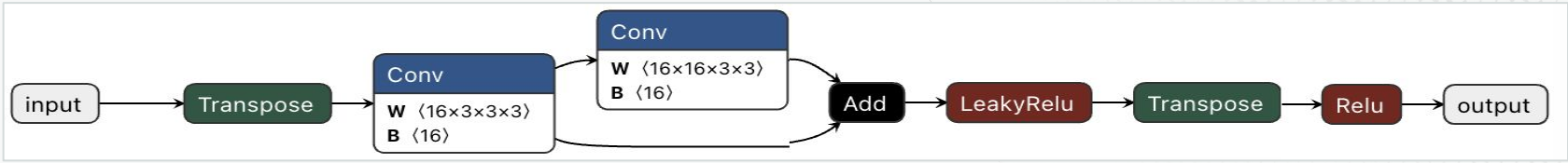
VERIFICATION

Verification is completed using the model's input and output, the model's commitment, and verification keys.

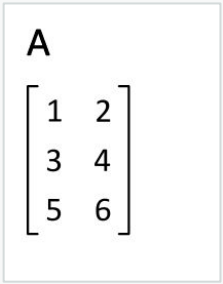
This process confirms that the inference was computed correctly—without ever revealing the input data or the model itself.

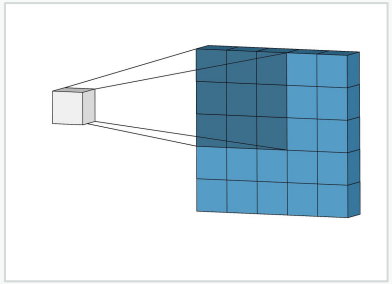
DeepProve: Internals

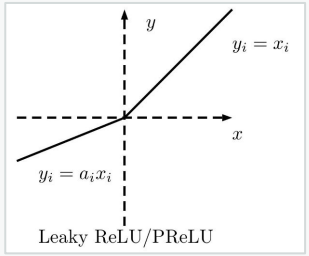
ONNX

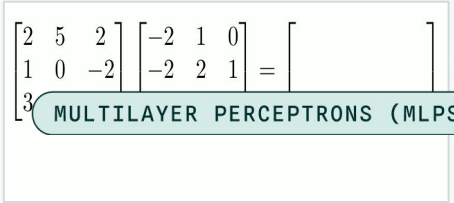


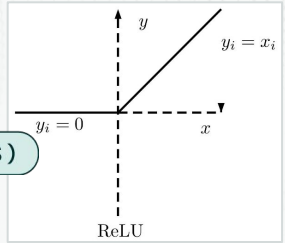
Computation











Cryptography

- Multivariate Polynomial Commitments
- Sum-Check Protocol
- Lookup Arguments

DeepProve Compared to baseline

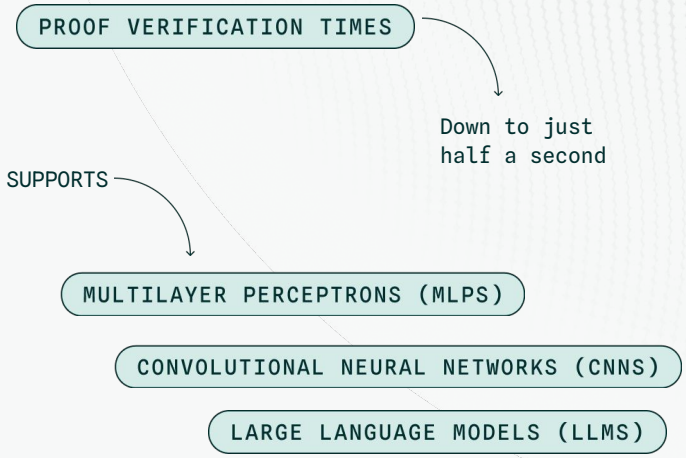
VERIFICATION PROOF UP TO

1150x
FASTER

AT ONE TIME SETUP
THAN BASELINE

1000x
FASTER

AT **AI PROOF GENERATION** ON
GPU THAN THE BASELINE



DeepProve is the fastest and most scalable zkML library to date.

DeepProve becomes proportionately faster as parameter count increases.

Executive Team

Ismael Hishon-Rezaizadeh

Founder and CEO

Formerly: VC, Head of Data at Renegade Partners, Crypto Engineer at John Hancock

Omar Yehia

Chief Strategy Officer

Formerly: Head of Investments at Matter Labs

Amir Rezaizadeh

Chief Operations Officer

Formerly: Harvard Law School

Charalampos (Babis) Papamanthou

Chief Scientist

Co-Chair of Applied Cryptography Dept at Yale University

Research Team

Nicolas Gailly, PhD in Applied Cryptography

Research Engineer in Cryptography & Distributed Systems

→ 12 publications, 3,978 citations

Franklin Delehelle, PhD in CS

Head of Engineering in High Performance Computing & ML

→ 124 citations

Zachary Youell, PhD in Algebraic Number Theory

Research Engineer in Proof Systems for Non-Linear ML

Dimitris Papadopoulos, Associate Professor at HKUST

Research Scientist in ZK Protocols, Verifiable ML, and Cloud Systems.

→ 43 publications, 1,646 citations

Shravan Srinivasan, PhD in Applied Cryptography

Research Scientist in Verifiable Computation & zkML

→ 234 citations

Nicholas Mainardi, PhD in Applied Cryptography

Research Engineer in ZK Systems and Privacy-Preserving AI

→ 13 publications, 75 citations

Research in verifiable computation, zero-knowledge proof systems, and privacy-preserving AI.

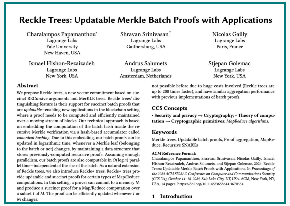
Lagrange's Science

Lagrange's research team is composed of **cryptography leaders** advancing the frontier of verifiable computation and zero-knowledge proofs.

Lagrange has already authored four papers in novel zero-knowledge proof schemes—Reckle Trees and Dynamic zk-SNARKs were both accepted into the **Science of Blockchain Conference (SBC)** in 2023 and 2025.

- Two leading cryptography professors
- Seven PhD researchers
- Over 22,000 combined citations
- Backgrounds from Yale, HKUST, EPFL, and UMD
- Lagrange's Chief Scientist, Babis Papamanthou, chairs the Applied Cryptography department at Yale University.

Reckle Trees



Reckle Trees: Updatable Merkle Batch Proofs with Applications

Charalampos Papamanthou*, Lagrange Labs, Yale University, New Haven, USA
Shravan Srinivasan†, Lagrange Labs, Gaithersburg, USA
Nicolas Gailly, Lagrange Labs, Paris, France
Ismael Hishon-Rezaizadeh, Lagrange Labs, New York, USA
Andrus Salumets, Lagrange Labs, Amsterdam, Netherlands
Stjepan Golemac, Lagrange Labs, New York, USA

Abstract

We propose Reckle trees, a new vector commitment based on succinct RECursive arguments and MerKLE trees. Reckle trees' distinguishing feature is their support for succinct batch proofs that are *updatable*—enabling new applications in the blockchain setting where a proof needs to be computed and efficiently maintained over a moving stream of blocks. Our technical approach is based on embedding the computation of the batch hash inside the recursive Merkle verification via a hash-based accumulator called *canonical hashing*. Due to this embedding, our batch proofs can be updated in logarithmic time, whenever a Merkle leaf (belonging to the batch or not) changes, by maintaining a data structure that stores previously-computed recursive proofs. Assuming enough parallelism, our batch proofs are also computable in $O(\log n)$ parallel time—independent of the size of the batch. As a natural extension of Reckle trees, we also introduce Reckle+ trees. Reckle+ trees provide updatable and succinct proofs for certain types of Map/Reduce computations. In this setting, a prover can commit to a memory M and produce a succinct proof for a Map/Reduce computation over a subset I of M. The proof can be efficiently updated whenever I or M changes. This was not possible before due to huge costs involved (Reckle trees are up to 200 times faster), and have similar aggregation performance with previous implementations of batch proofs.

CCS Concepts

• **Security and privacy → Cryptography**; • **Theory of computation → Cryptographic primitives**; *MapReduce algorithms*.

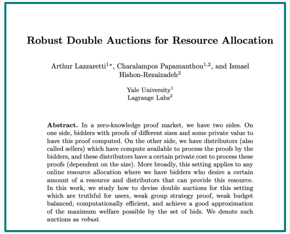
Keywords

Merkle trees, Updatable batch proofs, Proof aggregation, MapReduce, Recursive SNARKs

ACM Reference Format:
Charalampos Papamanthou, Shravan Srinivasan, Nicolas Gailly, Ismael Hishon-Rezaizadeh, Andrus Salumets, and Stjepan Golemac. 2024. Reckle Trees: Updatable Merkle Batch Proofs with Applications. In *Proceedings of the 2024 ACM SIGSAC Conference on Computer and Communications Security (CCS '24), October 14–18, 2024, Salt Lake City, UT, USA*. ACM, New York, NY, USA, 14 pages. https://doi.org/10.1145/3658644.3670354

1 Introduction

DARA



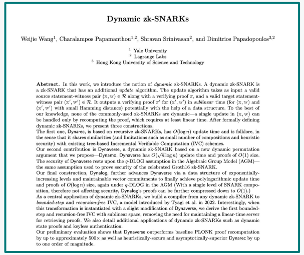
Robust Double Auctions for Resource Allocation

Arthur Lazzaretti[1*], Charalampos Papamanthou[1,2], and Ismael Hishon-Rezaizadeh[2]

Yale University[1]
Lagrange Labs[2]

Abstract. In a zero-knowledge proof market, we have two sides. On one side, bidders with proofs of different sizes and some private value to have this proof computed. On the other side, we have distributors (also called sellers) which have compute available to process the proofs by the bidders, and these distributors have a certain private cost to process these proofs (dependent on the size). More broadly, this setting applies to any online resource allocation where we have bidders who desire a certain amount of a resource and distributors that can provide this resource. In this work, we study how to devise double auctions for this setting which are truthful for users, weak group strategy proof, weak budget balanced, computationally efficient, and achieve a good approximation of the maximum welfare possible by the set of bids. We denote such auctions as *robust*.

Dynamic zk-SNARKS



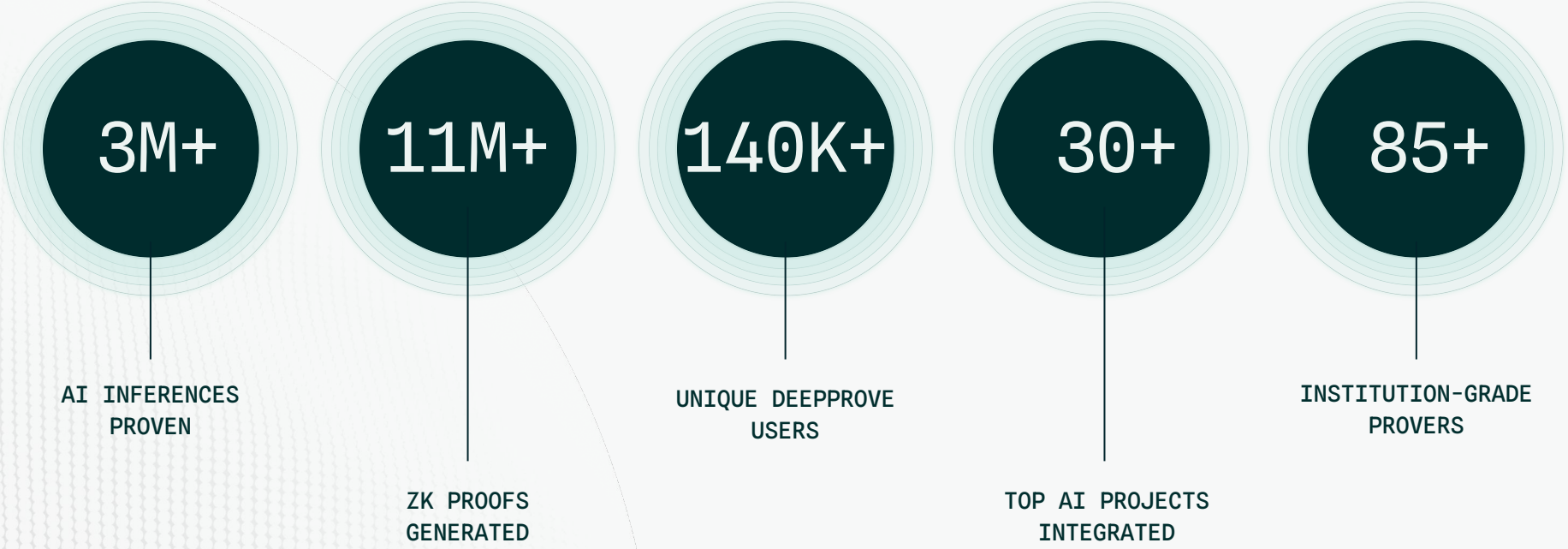
Dynamic zk-SNARKs

Weijie Wang[1], Charalampos Papamanthou[1,2], Shravan Srinivasan[2], and Dimitrios Papadopoulos[3,2]

[1] Yale University
[2] Lagrange Labs
[3] Hong Kong University of Science and Technology

Abstract. In this work, we introduce the notion of *dynamic* zk-SNARKs. A dynamic zk-SNARK is a zk-SNARK that has an additional *update* algorithm. The update algorithm takes as input a valid source statement-witness pair $(x, w) \in \mathcal{R}$ along with a verifying proof π, and a valid target statement-witness pair $(x', w') \in \mathcal{R}$. It outputs a verifying proof π' for (x', w') in *sublinear* time (for (x, w) and (x', w') with small Hamming distance) potentially with the help of a data structure. To the best of our knowledge, none of the commonly-used zk-SNARKs are dynamic—a single update in (x, w) can be handled only by recomputing the proof, which requires at least linear time. After formally defining dynamic zk-SNARKs, we present three constructions.
The first one, Dynarec, is based on recursive zk-SNARKs, has $O(\log n)$ update time and is folklore, in the sense that it shares similarities (and limitations such as small number of compositions and heuristic security) with existing tree-based Incremental Verifiable Computation (IVC) schemes.
Our second contribution is Dynaverse, a dynamic zk-SNARK based on a new dynamic permutation argument that we propose—Dynamo. Dynaverse has $O(\sqrt{n}\log n)$ update time and proofs of $O(1)$ size. The security of Dynaverse rests upon the q-DLOG assumption in the Algebraic Group Model (AGM)—the same assumption used to prove security of the celebrated Groth16 zk-SNARK.
Our final construction, Dynalog, further advances Dynaverse via a data structure of exponentially-increasing levels and maintainable vector commitments to finally achieve polylogarithmic update time and proofs of $O(\log n)$ size, again under q-DLOG in the AGM (With a single level of SNARK composition, therefore not affecting security, Dynalog's proofs can be further compressed down to $O(1)$.)
As a central application of dynamic zk-SNARKs, we build a compiler from any dynamic zk-SNARK to *bounded-step* and *recursion-free* IVC, a model introduced by Tyagi et al. in 2022. Interestingly, when this transformation is instantiated with a slight modification of Dynaverse, we derive the first bounded-step and recursion-free IVC with sublinear space, removing the need for maintaining a linear-time server for retrieving proofs. We also detail additional applications of dynamic zk-SNARKs such as dynamic state proofs and keyless authentication.
Our preliminary evaluation shows that Dynaverse outperforms baseline PLONK proof recomputation by up to approximately 500× as well as heuristically-secure and asymptotically-superior Dynarec by up to one order of magnitude.

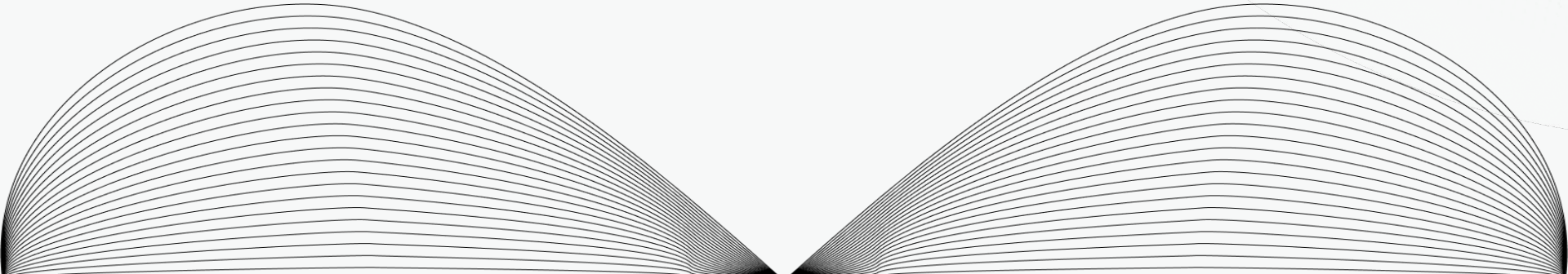
Traction


3M+
AI INFERENCES PROVEN
11M+
ZK PROOFS GENERATED
140K+
UNIQUE DEEPPROVE USERS
30+
TOP AI PROJECTS INTEGRATED
85+
INSTITUTION-GRADE PROVERS

Real-World Use Cases

- Verifiable smart contract AI integrations
- Deep Fake Detection
- KYC and Compliance
- AI-generated NFT provenance verification
- Private AI inferences for finance and healthcare
- Defense and cybersecurity AI compliance verification

SEC Sandbox Proposal



SEC Sandbox Proposal

The SEC seeks to balance the oversight and enforcement of digital assets with the highest possible preservation of privacy.

Lagrange Labs proposes a regulatory sandbox to enable the evaluation of DeepProve — a zero-knowledge proof system producing verifiable, privacy-preserving evidence of compliance.

Sandbox Overview

Why a Sandbox?

- Overall: experiment to use ZK proofs in place of broader data collection wherever possible
- Legacy compliance tools often don't fit blockchain environments
- Broad data collection creates privacy risks, legal exposure, and operational burden
- A sandbox enables the SEC to test modern methods in a controlled environment

Objectives:

- Protect investor privacy: proofs replace data exposure
- Ensure accountability: tamper-evident, time-stamped proofs of compliance
- Strengthen legal defensibility: reproducible, court-ready evidence
- Clarify regulatory gray areas: When are proofs sufficient vs. full disclosures?
- Deliver policy-ready insights for SEC guidance and rulemaking

Use Case 1: Investor Privacy

Use Case: Digital securities purchases require eligibility (e.g. accreditation, residency), which ultimately can expose sensitive personal data.

Challenge: Current methods mainly rely on off-chain attestations and raw data disclosure during inspection and enforcement. Occasionally, on-chain leaks occur (i.e. attestations written on-chain, whitelists with classification metadata, identifying token classes). This creates major privacy risks.

Solution: Transforms eligibility checks into cryptographic proofs — verifiable, privacy-preserving, and enforceable — which can be employed either retroactively or proactively.

Potential Benefits:

1) Investors: Reduced data exposure, elimination of production burden during inspection

2) Issuers: Streamlined procedure, reduced administrative burden, reduced potential liability

3) SEC: Fewer inspections, increased enforcement efficiency, stronger public trust

Use Case 2: Broker-Dealer Auditing

Use Case: Broker-dealers must meet obligations across books and records, custody, best execution, liquidity, and disclosures — typically requiring manual data pulls and broad document sharing.

Challenge: Current oversight depends on large-scale data collection, exposing sensitive information, increasing disputes over accuracy, and placing a heavy burden on both digital firms and regulators.

Solution: Pairs each requirement with a cryptographic proof, enabling verifiable compliance without revealing underlying data. Full records are retained, but proofs act as first-line evidence.

Potential Benefits:

1) Broker-Dealers: Lower operational burden, stronger confidentiality, reduced audit friction

2) Market Integrity: Trustworthy compliance processes, fewer disputes, greater transparency

3) SEC: Streamlined exams, strengthened enforcement actions, reduced administrative burden

Sandbox Phases

1. **Phase 1 (Months 1–2)**: Define objectives, evaluation metrics, and establish a joint working group with SEC staff and other participants.
2. **Phase 2 (Months 3–5)**: Integrate DeepProve into participant workflows within a test environment.
3. **Phase 3 (Months 6–11)**: Pilot onboarding and execution, generating proofs for each relevant scenario.
4. **Phase 4 (Months 12–14)**: Audit proofs for accuracy, conduct mock legal reviews, and test evidentiary sufficiency.
5. **Phase 5 (Months 15–18)**: Publish technical findings, operational results, and policy recommendations.
6. **Phase 6 (18+ months):** Maintain sandbox for ongoing collaboration and explore expanded use cases, ultimately resulting in real-world application.

Goals & Success Metrics

The sandbox will be evaluated based on:

1. **Privacy Preservation**: Success is measured by the reduction in raw data exposure while maintaining and satisfying all oversight and enforcement requirements.
2. **Proof Performance**: Proofs must be generated and verified efficiently at scales consistent with live-market conditions. Reliability, speed, and uptime will be measured across typical regulatory workflows.
3. **Legal Defensibility**: Proofs must meet standards for admissibility in enforcement and litigation contexts. Simulated legal reviews will assess tamper-evidence, reproducibility, and evidentiary strength.
4. **Operational Impact**: Proof-based compliance should streamline regulatory reviews and reduce manual data collection. Feedback from SEC staff will measure usability, integration effort, and long-term adoption potential.

Annex A: Future AI Use Case

Use Case: AI systems used or to be used by the SEC detect suspicious trading activity (insider trading, wash trades, pump-and-dumps), but alerts are difficult to substantiate and often challenged in court.

Challenge: AI-generated surveillance signals are often perceived as lacking interpretability and reliability, leaving them open to dispute and weakening their enforcement value.

Solution: DeepProve pairs AI alerts with cryptographic proofs — verifiable, reproducible, and privacy-preserving — that confirm or disprove violations directly from on-chain activity.

Potential Benefits:

1) SEC: Stronger, faster enforcement with reduced investigation burden

2) Courts: Tamper-proof, objective evidence with higher admissibility

3) Investors: Privacy protection while market manipulation is deterred

[DRAFT] SEC Financial Surveillance and Privacy Sandbox Proposal – Lagrange Labs

Submitted to the U.S. Securities and Exchange Commission

1. Executive Summary

The Crypto Task Force holds a pivotal role in shaping global standards for the integration of artificial intelligence (AI) and cryptography in digital-asset regulation. It is uniquely positioned to set a global precedent for how these advanced technologies can be used to enhance oversight and accountability in the rapidly evolving crypto landscape. However, the application of AI in regulatory frameworks introduces several key challenges that require careful consideration:

- **Privacy Concerns**: AI-driven surveillance could unintentionally intrude on the privacy of lawful U.S. consumer activities, raising significant questions about data protection and individual rights.
- **Opaque Enforcement Decisions**: The use of "black-box" AI systems - where decision-making processes are not fully transparent - poses a risk of challenges in enforcement actions, potentially undermining trust in the regulatory process.
- **Evidentiary Gaps**: In legal proceedings, the reliance on AI-generated evidence may create difficulties in establishing verifiable, transparent, and credible evidence in court, complicating judicial review.

To address these issues, Lagrange Labs proposes the creation of a regulatory sandbox to enable the SEC to test DeepProve, our cutting-edge zero-knowledge proof framework for verifiable AI inference. This solution is specifically designed to mitigate the aforementioned risks in three key areas:

- **Consumer Privacy**: By ensuring that sensitive consumer data remains private while enabling AI-driven analysis and oversight, DeepProve can prevent unnecessary intrusions into personal data.
- **Transparent Enforcement**: The zero-knowledge framework facilitates accountable, transparent AI decision-making processes, ensuring that enforcement actions are both explainable and defendable, even in legal challenges.

- **Evidentiary Integrity**: DeepProve's design allows for the creation of verifiable audit trails and proof of compliance, ensuring that AI-generated evidence holds up to scrutiny in judicial contexts.

Through this sandbox, the SEC will be able to test-pilot DeepProve in real-world environments, producing measurable outcomes and potential policy-ready models for the responsible integration of AI in digital-asset regulation. These programs will serve as a foundation for developing clear, actionable policies that balance innovation with regulatory oversight, helping to foster a more secure, transparent, and equitable digital-asset ecosystem.

2. Objectives of the Sandbox

- **Protect U.S. Consumer Privacy**

  Current surveillance often requires broad access to consumer financial data. This sandbox will test whether cryptographic proofs can replace raw data, allowing for oversight power without unconstitutional or unnecessary collection of personal data.

- **Ensure AI Accountability**

  DeepProve provides reproducible evidence that AI models were executed on the intended datasets. This sandbox will assess whether such proofs meet evidentiary standards in enforcement actions.

- **Strengthen Legal Defensibility**

  Enforcement outcomes must be able to survive litigation. Proof-backed AI alerts will be tested as tamper-proof, admissible evidence.

- **Advance Policy Innovation**

  International sandboxes demonstrate that empirical results inform rulemaking. This sandbox will provide data-driven insights for SEC policymaking on AI, consumer privacy, and blockchain oversight.

3. Technology Overview – DeepProve

AI is already being used to scan blockchain activity, flag suspicious trades, and review disclosures. But these systems face a trust problem: how can regulators, courts, and the public know that an AI's findings are accurate, unbiased, and generated appropriately?

DeepProve solves this by attaching a cryptographic receipt to every AI action. Rather than relying on the model's results alone, regulators receive a proof that the model ran exactly as intended, on the correct data, and without manipulation. This proof can be independently verified by auditors, courts, or regulators, *without* exposing private data used in the process.

In essence, DeepProve turns AI from a “black box” into a “glass box” with privacy curtains. Regulators can verify the actions taken, but consumers’ sensitive data remains shielded. This combination of transparency for oversight and privacy for individuals is ideally suited to the SEC’s mission and a positive public perception into the future.

4. Privacy-Focused Sandbox Use Case

The following proposed sandbox use case demonstrates how the SEC can envision enforcement against illicit activity while protecting consumer privacy - a balance that is essential to maintain public trust and regulatory legitimacy.

Privacy-Preserving Blockchain Surveillance & Model Correctness Validation

Blockchain transactions are inherently transparent, but they also provide a level of pseudonymity. The SEC must monitor blockchain activity to detect illicit actions like money laundering, market manipulation, and fraud while protecting the privacy of non-involved, lawful consumers. This is especially critical as overly broad surveillance could risk the perception of the government infringing on U.S. citizens’ rights.

This use case tests whether DeepProve can ensure that only flagged illicit transactions are ultimately associated with personal data, while lawful consumer activities remain private, achieving a best-of-both-worlds scenario.

Approach:

- **Transaction Monitoring with Privacy Shields**

  The SEC will deploy and/or leverage existing AI models to detect illicit activities such as money laundering, market manipulation, and fraud across exchanges and DeFi protocols. DeepProve will ensure that the AI only links flagged transactions to personal data of suspected illicit actors.

    - In the case of illicit actors, if a suspicious transaction is flagged, the SEC can access identifying information such as wallet addresses and transaction amounts.
    - Otherwise, transactions that are not flagged will be shielded from exposure, ensuring that the privacy of innocent individuals is maintained.

- **Zero-Knowledge Proofs for Privacy-Preserving Validation**

  DeepProve will generate cryptographic proofs to validate that flagged transactions meet the criteria for illicit behavior, without revealing personal details. For example:

    - If a transaction is flagged for money laundering, a zero-knowledge proof will confirm that the transaction meets the illicit behavior criteria, but without revealing the underlying personal data.
    - These cryptographic proofs serve as a transparent and verifiable way to validate the AI model's decision, without exposing unnecessary data.

- **AI Model Correctness and Transparency**

  Every AI-driven decision will be backed by a cryptographic proof, which demonstrates:

    - The AI model ran on the correct dataset.
    - The model was applied correctly to the data.
    - The decision-making process followed the right steps to flag illicit activity.

  This ensures that regulators have clear evidence of the AI model's correctness and transparency, reducing the risk of litigation challenges.

- **Legitimacy and Defensibility of Enforcement Actions**

  DeepProve's cryptographic proofs will ensure that enforcement actions based on AI findings are defensible in court. If a flagged transaction is challenged in a legal setting, regulators can present verifiable evidence that:

    - The model was applied correctly.
    - The flagged transactions were indeed illicit.
    - There was no manipulation in the AI process.

  This ensures that the SEC's enforcement actions are robust and credible, standing up to scrutiny in legal proceedings, which would otherwise have not been possible.

- **Privacy-First Consumer Protection**

The framework ensures that the personal data of law-abiding consumers is shielded from regulators unless their transactions are linked to illicit activity. In practice:

- Privacy is protected for non-involved individuals.
- Only relevant, suspicious data is accessible for enforcement, protecting innocent users from broad surveillance.

Measures of Success:

- **Privacy Protection**: Volume of data shielded compared to traditional surveillance methods, with audits to confirm no unintended exposure of lawful consumer data.
- **AI Accuracy**: Accuracy of flagged transactions in detecting illicit activities, compared to real-world enforcement benchmarks.
- **Proof Validity**: Success of cryptographic proofs in verifying AI model correctness and privacy protections.
- **Enforcement Defensibility**: Rate of success in legal challenges, with mock litigation exercises assessing the admissibility and strength of cryptographic proofs in court.
- **Public Trust**: Surveys and feedback from stakeholders, including auditors and consumers, about the balance between effective surveillance and privacy protection.

Outcome:

This sandbox use case enables the SEC to effectively monitor illicit activity in blockchain transactions while preserving the privacy of law-abiding citizens. By using privacy-preserving cryptographic proofs to validate enforcement actions, the SEC can enhance its credibility and public trust, demonstrating that it can balance privacy protection with regulatory oversight.

5. Sandbox Timeline

Phase 1: Initial Planning & Stakeholder Engagement

Duration: 1–2 months

- **Objective:** Establish groundwork for sandbox, ensure alignment with SEC objectives, and identify key stakeholders.

- **Key Activities:**
  - Form a collaborative working group with SEC officials, privacy advocates, industry experts, and Lagrange team.

    - Conduct risk assessments, privacy impact assessments, and define regulatory goals.
    - Review existing regulatory frameworks and identify/confirm gaps.
    - Finalize agreements on data handling, security, and transparency protocols.

Phase 2: Framework Development & Testing Preparation

Duration: 2–3 months

- **Objective:** Develop the technical infrastructure for the sandbox and ensure the DeepProve framework meets SEC requirements.

- **Key Activities:**
    - Integrate DeepProve's zero-knowledge proof system into the sandbox environment.
    - Implement data anonymization and privacy-preserving mechanisms to safeguard consumer privacy.
    - Develop transparent AI accountability tools for auditing and reporting AI decisions.
    - Design test scenarios that mirror real-world regulatory challenges (e.g., surveillance, enforcement, evidence gathering).
    - Perform internal testing to validate the effectiveness of the framework in mitigating identified risks.

Phase 3: Pilot Execution (Test Runs)

Duration: 4–6 months

- **Objective:** Launch initial pilot testing with controlled real-world data and activities.

- **Key Activities:**
    - Deploy DeepProve in a live, controlled environment, processing limited but diverse sets of digital-asset transactions.
    - Monitor privacy, security, and compliance with regulatory standards during pilot operations.
    - Conduct test runs simulating different enforcement scenarios (e.g., detecting suspicious financial activity or illegal transactions).
    - Evaluate the transparency of AI decision-making and ensure all actions are traceable and verifiable.
    - Collect feedback from stakeholders, including regulatory bodies, consumer privacy groups, and industry participants.

Phase 4: Performance Evaluation & Refinement

Duration: 2–3 months

- **Objective:** Evaluate the pilot results, identify areas for refinement, and iterate on the system's performance.

- **Key Activities:**
    - Assess the effectiveness of the privacy-preserving mechanisms and AI accountability tools.
    - Review the legal validity and reliability of AI-generated evidence.
    - Analyze feedback and data to optimize the framework's functionality.
    - Refine policies, operational procedures, and regulatory models based on findings.
    - Continue engaging with stakeholders to assess satisfaction and resolve concerns.

Phase 5: Full-Scale Rollout & Policy Recommendations

Duration: 3–4 months

- **Objective:** Finalize recommendations and expand the sandbox to support broader regulatory applications.

- **Key Activities:**
    - Finalize comprehensive policy recommendations for incorporating AI and cryptography into digital-asset oversight.
    - Publish findings and insights from the sandbox pilot, including successes, challenges, and improvements.
    - Submit policy and regulatory guidelines to the SEC for review and potential adoption.
    - Scale the sandbox to include additional scenarios and industry players.
    - Develop a framework for ongoing monitoring and updates as AI and cryptography technologies evolve.

Phase 6: Long-Term Monitoring & Evolution

Duration: Ongoing

- **Objective:** Continuously monitor the effectiveness of the framework, adjust policies, and update the sandbox as needed.

- **Key Activities:**

    - Monitor ongoing usage and performance of the DeepProve framework in real-world applications.
    - Update the framework to adapt to new technological developments, regulatory changes, and emerging risks.
    - Conduct periodic reviews with the SEC to ensure compliance and refine regulatory approaches as necessary.
    - Continue working with industry partners to ensure that DeepProve stays aligned with evolving digital-asset trends.

Summary Timeline

- **Months 1–2**: Initial Planning & Stakeholder Engagement
- **Months 3–5**: Framework Development & Testing Preparation
- **Months 6–11**: Pilot Execution
- **Months 12–14**: Performance Evaluation & Refinement
- **Months 15–18**: Full-Scale Rollout & Policy Recommendations
- **Months 18+**: Long-Term Monitoring & Evolution

This timeline balances thorough development with practical testing, enabling the SEC to evaluate and refine DeepProve in a structured, transparent way while allowing ample time for feedback and iteration. It also sets a clear path to transition from proof of concept to actionable regulatory frameworks.

6. Evaluation Methodology

The value of a sandbox lies not just in experimentation, but in the ability to generate clear, measurable insights that inform policy and enforcement. Without structured evaluation, pilot projects risk becoming isolated experiments with little regulatory impact. This sandbox emphasizes evidence-based assessment, with metrics designed to measure not only technical performance but also fairness, privacy, and legal defensibility.

- **Technical Validity**: The SEC must have confidence that proofs are generated reliably, quickly, and at scale. This measure evaluates success rates, processing latency, and system scalability to ensure oversight can keep pace with market activity.
- **Privacy Protection**: A core purpose of this sandbox is to minimize consumer data exposure. Independent audits will confirm how much less identifiable information is retained under a proof-based system, validating that privacy-by-design has been achieved in practice.
- **Enforcement Defensibility**: For AI-driven enforcement to withstand courtroom challenges, outputs must be reproducible and tamper-proof. Mock litigation exercises will

test whether cryptographic proofs are accepted as admissible evidence and whether they reduce disputes over model reliability.

- **Operational Efficiency**: Technology that improves workflows for SEC staff provides additional value. This measure evaluates whether case triage becomes faster, whether false positives decline, and whether staff find proof-backed AI outputs easier to use than traditional methods.

Together, these evaluation dimensions ensure the sandbox delivers meaningful results that can inform both future policy and day-to-day enforcement practices.

7. Risks and Mitigations

Launching an innovative regulatory sandbox inevitably carries risks, both technical and institutional. Anticipating these challenges, and designing safeguards in advance, will ensure the sandbox strengthens the SEC's oversight rather than undermines it.

One key risk is latency: generating cryptographic proofs can add computational overhead. If proofs are too slow, surveillance or enforcement workflows may lag behind market activity. To mitigate this, Lagrange will employ best-in-class efforts to ensure that proofs are produced quickly and without degrading system performance. Pilot testing in the sandbox will further calibrate acceptable speed thresholds.

Another risk is AI bias, which could lead to unfair outcomes if models systematically misinterpret certain trading patterns or consumer behaviors. Embedding fairness checks directly into the proof system will help mitigate this: DeepProve can prove not only that a model ran correctly, but also that bias-detection routines were applied. This ensures AI oversight remains equitable and not subject to hidden distortions.

A further challenge is judicial skepticism. Courts may initially be hesitant to accept cryptographic proofs as evidence, particularly in complex enforcement cases. To mitigate this, the sandbox will incorporate mock evidentiary hearings and legal stress-tests. These exercises will assess admissibility standards and refine how proofs are presented in litigation, building confidence among judges, prosecutors, and defense counsel alike.

Finally, there is the risk of regulatory over-reliance. If proofs are misunderstood as substitutes for human judgment, important contextual factors might be overlooked. The sandbox mitigates this by ensuring human analysts remain in the loop, using proofs as validation rather than replacement. This balance ensures accountability remains firmly with regulators, not with machines.

Taken together, these mitigations create a controlled environment where risks are addressed proactively, and lessons are codified for long-term regulatory adoption.

8. Participants

- **Lagrange Labs**
  - Ismael Hishon-Rezaizadeh, CEO - Strategic vision & alignment
  - Brian Novell, Esq., Head of Business Development - Policy engagement & legal interface
  - Babis Papamanthou, Chief Scientist - Cryptography & ZK proof architecture

- **SEC Crypto Task Force**
  - To be designated

- **Independent Auditors & Observers**
  - Academic partners (e.g., Yale ACL)
  - Privacy NGOs / External law firms
  - Industry observers (e.g., FINRA, MIT DCI)

9. Expected Outcomes

The ultimate measure of success for this sandbox is not just technical performance, but whether it strengthens the SEC's ability to enforce the law while protecting Americans' rights. The outcomes will be twofold: immediate operational benefits in the form of privacy-preserving, verifiable enforcement tools, and broader policy lessons that inform the Commission's long-term approach to AI and digital assets. By producing concrete data, legal tests, and public reporting, the sandbox will help the SEC move from theory to practice in setting global standards for responsible oversight.

. The expected outcomes from the sandbox will include:

- A blueprint for AI-powered enforcement with privacy-by-design.
- Cryptographic audit standards for AI model outputs in regulation.
- Policy-ready evidence for SEC rulemaking on AI and crypto privacy.
- Evidentiary standards for AI-backed regulatory actions.

10. Conclusion

By addressing key friction points such as privacy protection, transparency, and legal defensibility, this sandbox will strengthen the SEC's ability to enforce the law while protecting consumer rights. Lagrange Labs respectfully requests the SEC's approval to initiate this sandbox and establish the United States as a global leader in verifiable, privacy-preserving oversight of digital assets.

Annex: Additional Potential Use Cases (Beyond Immediate Sandbox Proposal)

While this proposal focuses initially on privacy-preserving use cases, additional sandbox pilots could further strengthen enforcement and accountability. These are not part of the immediate sandbox request but are offered as future options.

Use Case A – Verifiable AI in Insider Trading Enforcement

Enforcement against insider trading in token markets faces two compounding challenges: the speed at which illicit trades occur and the evidentiary weakness of AI-driven alerts. Regulators may detect suspicious trading patterns, but if these alerts are generated by black-box models, defendants can argue they are unreliable or unverifiable. This undermines deterrence and slows down investigations.

Approach

- Apply AI models to detect trading anomalies around token listing announcements or governance votes.
- Use DeepProve to generate proofs of model correctness and dataset integrity.
- Deliver alerts to enforcement teams with cryptographic evidence attached.

Metrics for Success

- Reduction in investigation time compared to baseline.
- Number of AI alerts deemed admissible during mock litigation exercises.
- Degree of reproducibility confirmed by independent SEC staff teams.

This use case would significantly increase the credibility of AI-assisted enforcement in high-stakes insider trading cases. By providing courts with verifiable, tamper-proof evidence, the SEC strengthens its litigation posture while signaling to markets that enforcement tools are both modern and defensible. Public perception would benefit from knowing that the Commission is enhancing fairness and legal integrity, not relying on opaque algorithms.

Use Case B – AI-Powered Disclosure Reviews

The SEC's mandate to review token whitepapers, governance filings, and exchange disclosures is resource-intensive. AI can accelerate this work, but only if findings are provable and resistant to

issuer challenge. By attaching proofs to every AI-assisted review, the SEC can create tamper-proof audit trails that document precisely what disclosures were analyzed and why they were flagged, ensuring enforcement remains credible.

Approach

- Deploy AI to scan disclosures for red-flag patterns (e.g., unsubstantiated revenue claims).
- Generate DeepProve proofs linking inferences directly to the documents reviewed and model parameters.
- Retain immutable records for reproducibility in case of disputes.

Metrics for Success

- Time saved in disclosure audits relative to manual review.
- Detection rate of misstatements compared to baseline.
- Third-party validation of reproducibility from proofs alone.

This use case would expand the SEC's capacity to oversee a rapidly growing volume of disclosures, ensuring efficiency without sacrificing legal rigor. It would improve market integrity while enhancing the Commission’s reputation as a modern regulator able to handle complexity at scale. Public perception would highlight the SEC’s ability to innovate responsibly while maintaining fairness and accountability.

Use Case C – Tamper-Proof Market Surveillance Logs

Crypto markets are fast-moving and prone to manipulation. AI can flag patterns like spoofing or wash trading, but regulators must maintain credibility that these alerts are genuine and not subject to after-the-fact alteration.

Approach

- Deploy AI for detecting manipulation in DeFi and CEX venues.
- Log every inference with a DeepProve proof, creating immutable, verifiable audit trails.
- Enable third parties (courts, auditors) to re-verify alerts independently.

Metrics for Success

- Percentage of alerts successfully verified by third-party auditors.
- Latency impact of proof generation compared to current systems.
- Reduction in evidentiary disputes during mock enforcement trials.

This use case would reinforce the SEC's authority and credibility in market oversight, reducing disputes and ensuring that enforcement actions cannot be challenged on procedural grounds. By pioneering verifiable surveillance logs, the Commission would improve transparency and public trust, reassuring both investors and courts that oversight is impartial and beyond manipulation.

Use Case D – Strengthening Defensibility of AI Outputs

AI-generated outputs are increasingly challenged in enforcement proceedings as opaque, unverifiable, or biased. Unless regulators can demonstrate that results are reproducible and free from tampering, cases risk being undermined.

Approach

- Embed DeepProve proofs with every AI output used in enforcement.
- Demonstrate that each inference is tied to a specific dataset, model, and timestamp.
- Retain immutable, verifiable records of all steps in the AI pipeline.

Metrics for Success

- Percentage of AI-generated outputs verified as reproducible in mock hearings.
- Reduction in challenges to AI evidence during litigation simulations.
- Auditor confirmation that outputs are both correct and unbiased.

This use case would ensure that enforcement actions relying on AI are not only effective but also legally resilient, minimizing risks of dismissal or settlement due to evidentiary weaknesses. It enhances both market integrity and the SEC's credibility in deploying advanced tools.