Matter Labs Technologies, Inc. Comment Letter on File No. 4-927

November 4, 2026

VIA E-MAIL

Vanessa A. Countryman
Secretary, U.S. Securities and Exchange Commission
100 F Street NE
Washington, DC 20549-1090
comments@sec.gov

Re: Order Granting Temporary Conditional Exemptive Relief for Tokenized Securities Venues; Release No. 34-106402; File No. 4-927

Dear Ms. Countryman:

Matter Labs Technologies, Inc. ("Matter Labs US") appreciates the opportunity to respond to the Commission's request for comment on the Innovation Exemption (the "Order"), particularly Requests 1 and 5.

Matter Labs US is a Delaware corporation headquartered in New York. It licenses Prividium, a modular blockchain technology stack built on ZKsync that enables enterprises to launch private, permissioned, and interoperable zero-knowledge chains, to U.S. financial institutions and provides related integration services.

Matter Labs US is a technology provider. It does not intend to operate a Tokenized Securities Venue ("TSV").

We support the Order. We ask the Commission to clarify one condition so that it fully serves the Commission's stated purposes and accommodates a design that may serve those purposes better than fully transparent execution.

1. The Public Ledger Condition and Its Purpose

The Order requires that smart contracts used by a TSV be "auditable, public, and deployed on a public, permissionless distributed ledger," and states that "'[p]ermissionless' generally means that anyone can read or write to the distributed ledger without authorization." The Commission explains that this condition will help TSV Participants "understand how their trades are effected on a TSV" and will empower "participants and third parties to audit and report vulnerabilities."

We agree with these purposes. Publishing code serves them only when participants can be confident that the code published is the code that executed. Validity proofs provide that confidence directly.

2. Validity Proofs Provide a Stronger Form of Auditability

A validity proof (also called a zero-knowledge proof) is a cryptographic proof that a batch of transactions was executed exactly as specified by published code. A smart contract deployed on a public, permissionless ledger can verify the proof, and a state change that fails verification is rejected. Anyone can check the result without relying on the operator.

This allows execution data to remain confidential while the code, the verification logic, and the proofs remain public. A participant or independent third party can confirm that every state change was executed as specified by the published code, without seeing other participants' orders or positions. Access permissioning, which the Order expects a TSV to perform, is applied by the operator outside the proof and disclosed in the TSV's Notice.

This matters for the market the Order contemplates. The Order requires each TSV to describe in its Notice its "procedures and safeguards to protect the confidentiality of TSV Participants' information," and its "policies and procedures designed to address Maximal Extractable Value." Fully transparent execution exposes institutional orders and positions before and after trading, which enables front-running and sandwich attacks that the Order identifies as risks a TSV must disclose. Proven private execution reduces this exposure while preserving what participants and the Commission can verify.

3. What a Proof Does Not Establish, and Accompanying Safeguards

A validity proof establishes that state changes were correct. By itself, it does not establish that transactions were included fairly, that the system cannot be halted, or that the Commission can observe trading activity. In a private execution environment, participants also rely on the operator to include their transactions and to keep the system running. We therefore propose that proof-based designs qualify only when accompanied by the following safeguards:

(a) Public, verifiable code. The application code and the proof verification logic are published, and any person can confirm that the deployed verifier corresponds to the published code.

(b) Proofs settled on a qualifying ledger. Each state change is proven, and the proof is verified by a smart contract deployed on a ledger that satisfies the Commission's public and permissionless standard.

(c) Disclosed control powers. The Notice identifies each person who can upgrade, pause, or override the verifier, the bridge, or the execution environment, and the conditions under which they may do so. The Notice also states whether upgrades

other than emergency security fixes take effect only after a delay and, if so, the length of that delay.

(d) Disclosed exit and continuity arrangements. The Notice states whether and how participants can withdraw their assets if the operator ceases to function or declines to process their transactions, and describes the continuity arrangements that apply in that event, including any transfer of operating keys to a successor operator, and any power of a third party, such as a security council, to override the operator.

(e) No reduction in transparency or recordkeeping. The TSV continues to publish transaction data as required by the Order's transaction transparency condition and provides the Commission full access to its records, consistent with the Order's statement that distributed ledger records satisfy the books and records condition "if they can be readily accessed by the Commission in a human-readable format and a reasonably usable electronic format."

4. Requested Action

We respectfully request that the Commission, through staff responses to frequently asked questions or a modification of the Order:

1. Confirm that the condition that a TSV's smart contracts be "deployed on a public, permissionless distributed ledger" may be satisfied where those contracts execute in an environment whose every state change is proven and verified on a qualifying public, permissionless ledger, subject to safeguards (a) through (e).

2. Clarify the meaning of "public" and "permissionless," and recognize that a TSV's applications may satisfy the condition through validity-proof settlement on a qualifying ledger, without being deployed directly on that ledger.

3. Require that the Notice state the facts on which the TSV relies to conclude that its ledger, or its proof-based settlement, satisfies the condition, and that a material change in those facts trigger a revised Notice.

We would welcome the opportunity to discuss these points with staff of the Division of Trading and Markets and the Crypto Task Force.

Respectfully submitted,

Noah Pravecek

Head of Product, Prividium

Matter Labs Technologies, Inc.