MEMORANDUM

To: Crypto Task Force Meeting Log
From: Crypto Task Force Staff
Re: Meeting with Representatives of Phase Labs Technologies Limited

On May 7, 2025, Crypto Task Force Staff met with representatives from Phase Labs Technologies Limited.

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

Proposed Attendees:

- SEC Representatives from the **Crypto Task Force** and **ETF Division**
- **Brandon Geraldi** – CEO, Phase Labs Technologies Limited
- **Dan Dubokovič** - CFO, Phase Labs Technologies Limited
- **Jeff Newman** – Head of Product, Phase Labs Technologies Limited
- **Gabriel Hicks** – VP of Engineering, Phase Labs Technologies Limited

Phase Labs Technologies ("**Phase Labs**") is a Staking Service Provider ("**SSP**") that operates a high-performance validator and stake pool with over 700,000 SOL combined stake (~$100M at current prices). We focus on risk mitigation with technical expertise in validator performance, and institutional-grade validator management to ensure exceptional uptime and reliability.

Key Points for Discussion:

1. **Reiterate the Importance of Staking SOL in ETPs to Protect Investors:**
   - Solana is a **delegated proof-of-stake (dPoS) network**, meaning SOL holders must **stake their assets** to avoid inflationary dilution.
   - Without staking, an ETP holding SOL would be **passively losing value**, as newly minted tokens reward only active participants in the network's security. Staking is an essential part of any PoS/dPoS blockchain and is an inherent feature of any native token of such a network.
   - Including staking aligns ETF investors with **native yield opportunities**, mirroring how other income-generating assets (e.g., bonds, real estate) operate.
   - Staking helps secure the network by participating in the consensus mechanism, which is the core value proposition of the underlying asset.

2. **Why Stake Decentralization is Essential to Protect the Underlying Asset:**
   - **Stake centralization** refers to a small set of validators controlling a large proportion of the total staked assets of the network.
   - In the case of Solana, stake centralization threatens Solana's Byzantine Fault Tolerance (BFT) by increasing the risk of a small validator set controlling ≥33% of total stake. This could enable **censorship, block reordering (MEV exploitation), or even halt consensus** by preventing the required 2/3+ supermajority for finalization.
   - Stake centralization exposes ETP stakers to a higher risk of targeted **DDoS** (Distributed Denial-of-Service) attacks, which have **adverse economic effects** to stakers.
   - By staking to a larger set of validators, ETPs would uphold the **ethos** of the decentralized blockchain network, upon which the **core value proposition of Proof-Of-Stake assets** is built.

3. **How can we Mitigate the Risks of Decentralized Staking:**
   ○ While we are underscoring the need for decentralizing the staking of the ETP assets, we acknowledge the perceived **security concerns** of staking with a large validator set.
   ○ We note that the "**Native staking**" smart contract for Solana was developed by **Solana Labs**, the developer of the Solana blockchain and is thus considered extremely safe from "**smart contract risk**". Our model of ETP staking would be Non-Custodial and use Native Staking.
   ○ We propose **SOC2 and ISO 27001** as the core safety standards to be followed by the industry, as requirements for inclusion in the validator set.
   ○ These standards are intended to remedy the residual cyber-security risks that come up with Native Staking.
   ○ The standards are not cost-prohibitive and allow more validators to join the validator set.
   ○ We are asking for clarity on the **legal & regulatory requirements for including a Validator Service Provider** in the validator set of an ETP.

4. **Ensuring Competitive Market Access for Staking Service Providers:**
   ○ Competitive staking markets will lead to **lower fee rates** for investors.
   ○ A competitive market is a **pre-requisite for stake decentralisation** and **risk mitigation**.
   ○ A competitive market is **not synonymous with lower security** and operational standards.
   ○ Compliance with regulations and industry best-practices does not have to be burdensome or cost prohibitive.
   ○ A competitive market will **spur innovation**.

Agenda for the Meeting:

1. **Introduction** (5 min)
   ○ Overview of **Phase Labs Technologies & Validator Operations**
2. **Reiterating the Need for Staking in the ETPs** (10 min)
   ○ How non-staked SOL **dilutes ETP investors**
   ○ Staking as a **yield-generating mechanism** for ETP shareholders
   ○ Makes ETPs an attractive alternative to holding spot SOL
3. **Why Stake Decentralization is Essential to Protect the Underlying Asset (**15 min)
   ○ Share arguments for the issue of stake decentralization and protecting SOL ETPs investors
   ○ Broadening the landscape for small players, decreasing the barriers to entry
   ○ Increasing the level of access for small companies - Dan/Jeff
4. **How can We Mitigate the Risks of Decentralized Staking** (15 min)
   ○ Addressing the perceived security risks of including more Staking Service Providers

- How Non-Custodial Native Staking protects investors and addresses Smart Contract risk
- Share perspective on addressing residual cyber-security risks with SOC 2 & ISO 27001 certifications
- Clarity on other requirements for Phase Labs to be considered as a compliant staking partner

5. **Ensuring Competitive Market Access for Staking Service Providers** (5 min)
   - Achieving investor protection through adherence to robust, but financially and practically attainable security and operational standards that promotes broad market participation.
6. **Closing Thoughts** (10 min)
   - How to best align with institutional expectations
   - **Follow-up discussions & data-sharing process**

To: Securities and Exchange Commission (SEC) Crypto Task Force
From: Phase Labs Technologies Limited
Re: Request for Regulatory Clarity Regarding Staking Services for Exchange-Traded Products (ETPs)

Dear Members of the Crypto Task Force,

Phase Labs Technologies Limited ("**Phase Labs**") respectfully submits this letter to seek regulatory clarity regarding the provision of staking services for Exchange-Traded Products ("**ETPs**"), particularly in connection with pending Solana ("**SOL**") ETP applications submitted by Grayscale, VanEck, 21Shares, and other market participants.

As a Staking Service Provider ("**SSP**"), Phase Labs operates a high-performance validator infrastructure and stake pool with an aggregate stake of over 700,000 SOL, approximately $100 million at current market prices. Our expertise lies in institutional-grade validator management, risk mitigation, and technical optimization, ensuring high availability and network reliability.

This letter represents only a brief overview of the topics Phase Labs would like to engage in with the SEC. For more detailed and technical argumentation of the herein stated, we cordially invite you to read the Research Module available in the **Appendix 1** to this letter.

Background and Request for Engagement

Phase Labs seeks to build upon prior discussions, including those held with Jito and Multicoin, which underscored the importance of integrating staking within Solana-based ETPs. Additionally, we refer to the February 21st statement by Commissioner Hester M. Peirce, wherein staking-related regulatory considerations were identified as a high priority for the Commission.

We emphasize that staking SOL within ETPs serves the following fundamental purposes:

- **Investor Protection Against Token Inflation:** Staking mitigates dilution risks arising from token supply inflation by generating staking rewards, which may otherwise be unavailable to passive holders.
- **Network Security and Stability:** Participation in the Solana consensus mechanism strengthens network security, thereby reinforcing the intrinsic value proposition of the underlying digital asset.
- **Enhancing ETP Market Appeal:** Staking-enabled ETPs present an attractive alternative to direct spot SOL holdings on unregulated trading platforms, offering institutional investors enhanced regulatory oversight and risk management.

Despite the importance of these factors, there remains a significant lack of regulatory clarity concerning the legal, technical, and compliance frameworks governing SSPs that seek to engage with ETP issuers and custodians. Given our expertise in staking and validator operations, we seek guidance

on the applicable regulatory requirements necessary to facilitate compliant participation in the staking economy.

Key Issues for Discussion

Phase Labs respectfully requests the opportunity to engage with the SEC Crypto Task Force to address the following key regulatory considerations:

1. **Necessity of Broad Stake Decentralization for Security and Asset Integrity**

We urge the SEC to prioritize broad stake distribution as a critical security measure in SOL staking within ETP structures. Excessive concentration of staked assets within a few large validators poses systemic risks, including increased downtime, monopoly power, censorship, and transaction manipulation (e.g., Maximal Extractable Value "**MEV**" exploitation). It also heightens the risk of consensus halts, threatening network stability.

Decentralization is a core value proposition of the network, essential for security and fairness. ETPs have the ability to attract outsized amounts of capital and acquire a significant percentage of circulating supply of SOL tokens, which if all staked with a small number of validators would pose a serious threat to the core value propositions. A diverse validator set enhances resilience, is consistent with the ethos of blockchain technology and prevents undue influence over network operations.

Accordingly, we advocate for a regulatory framework that promotes participation in staking services, ensuring accessibility for a diverse range of providers rather than consolidating staking power within a limited number of large entities.

2. **Cybersecurity Framework and Compliance for Staking Services**

We acknowledge that increasing decentralization necessitates the involvement of multiple staking service providers, which may be perceived as an operational risk. To mitigate these concerns, we propose the establishment of a robust, but financially and practically attainable, cybersecurity framework and compliance tailored for SSPs seeking to support ETP issuers.

Specifically, we recommend that the SEC recognize industry-standard security protocols, including:

- **System and Organization Controls (SOC) 2, and**
- **ISO 27001 Certification.**

These security frameworks provide verifiable assurance of robust operational controls, risk mitigation strategies, and regulatory compliance best practices.

Furthermore, we highlight the distinction between custodial and non-custodial staking. Unlike custodial staking—where assets are transferred to a third party—native staking on Solana enables

users to retain full ownership and control over their tokens at all times, thereby mitigating counterparty risk. While residual cybersecurity risks exist, adherence to SOC 2 and ISO 27001 standards would substantially address these concerns.

3.   Ensuring Competitive Market Access for Staking Service Providers

We believe that access to staking service provision for ETPs should be broad-based and inclusive of smaller, highly secure SSPs. Establishing a fair and competitive market would mitigate risks associated with stake centralization while upholding rigorous investor protection and security standards.

To that end, we propose collaborative engagement with the SEC to develop a comprehensive, but non-burdensome, regulatory framework that ensures:

- Investor protection through adherence to robust, but financially and practically attainable security and operational standards;
- Fair market participation, allowing diverse staking entities to contribute to ETPs;
- Preservation of Solana's decentralized architecture and network security.

Conclusion

This was just a brief overview of the topics Phase Labs looks forward to engaging in with the SEC Crypto Task Force. For further detailed explanation, we respectfully invite you to read the Research Module available as **Appendix 1** to this letter. Phase Labs Technologies looks forward to engaging in meaningful discussions with the SEC Crypto Task Force to provide clarity on the regulatory path for staking services in the ETP ecosystem. We seek to contribute to a framework that balances investor protection, network decentralization, and market competitiveness.

We appreciate your time and consideration and welcome the opportunity to further discuss these matters at your convenience.

Sincerely,
Brandon Robert Geraldi
CEO
Phase Labs Technologies Limited

_____

Appendixes:
   -   **Appendix 1:** Research Module
_____

Appendix 1: Research Module

Solana's security model is directly tied to its decentralized validator set. Without sufficient distribution of stake, systemic risks increase, leading to investor exposure. This paper outlines why decentralized staking mitigates such risks.

1. Decentralization as a Risk Mitigation Strategy

Ensuring that Solana ETPs stake to a **decentralized set of validators** is not just an ideological preference—it is a necessary safeguard to mitigate systemic risks to the network and, by extension, the value of **SOL as an asset.**

When too much stake is concentrated in a small number of large validators, the network becomes **more vulnerable** to disruptions caused by validator failures, operational errors, or targeted attacks. Unlike traditional financial markets, where liquidity providers and market makers can step in to absorb shocks, **blockchain networks rely entirely on validator stability** to maintain uptime and security.

---

2. Single Validator Failures Can Disrupt the Entire Solana Network

Due to the nature of **Solana's high-performance architecture**, stake centralization creates an **inherent risk** of network-wide performance degradation if a single highly staked validator goes offline.

When a validator holding a **disproportionate share of stake** experiences an outage—whether due to a **technical issue, software misconfiguration, or DDoS attack**—it can lead to:

- **Block production delays and increased transaction failures.**
- **Validators relying on confirmations from large-staked validators lagging behind, slowing consensus.**
- **A network-wide performance decline, increasing transaction finalization times and reducing reliability.**

Solana's proof-of-stake model depends on **continuous validator participation** to maintain efficiency. If stake is too concentrated, the **failure of a single large validator** can have an outsized effect, causing cascading slowdowns that degrade the **stability and usability of the network.**

These risks highlight the **fragility of stake centralization** and why decentralizing stake across **a broader validator set** is essential for protecting the Solana network and SOL ETP investors.

---

3. How Decentralized Stake Protects the Solana Asset Class

A decentralized validator set is **not just a network philosophy** — it is a **fundamental risk management mechanism** that prevents single points of failure, strengthens economic security, and **preserves investor confidence** in SOL as an institutionally viable asset.

A well-balanced stake distribution directly **addresses key risks** to the network and asset class:

1. Reducing the Risk of Critical Failures

- Concentrating stake in a **small number of large validators** creates **systemic risk.**
- If a single dominant validator experiences an outage, misconfiguration, or attack, it can degrade network performance or, in extreme cases, threaten **network finality.**
- A broader validator set ensures that **no single entity holds enough stake** to jeopardize the **network's stability.**

2. Enhancing Network Resilience

- A **well-distributed** validator set **prevents disruptions from cascading** across the network.
- If one validator fails, the **overall staking infrastructure remains robust,** ensuring uninterrupted transaction processing.
- This mitigates potential **investor losses** tied to network instability.

3. Protecting Against Economic Manipulation and Fee Exploitation

- Over-centralization of stake allows dominant validators to **exert undue influence** over staking economics, such as:
    - Adjusting **commission rates** to extract **higher fees** from delegators.
    - Prioritizing self-interest over **network health.**
- A **diverse validator ecosystem** prevents scenarios that expose **investors to unnecessary financial risks.**

4. Maintaining the Institutional Integrity of SOL

- The value of SOL as an **institutional asset** is **inherently tied** to the **security and reliability of the network.**
- A more decentralized staking structure prevents:
    - **Censorship vulnerabilities.**
    - **Systemic failures caused by validator concentration.**
    - **Increased exposure to single-entity risks.**
- Ensuring a **decentralized validator set** helps institutional investors engage confidently with **SOL ETPs as a secure and sustainable asset.**

4. Institutional Best Practices for Staking SOL

1. Diversifying Stake Reduces Financial & Network Risks

- Solana **does not slash for downtime**, but an offline validator **earns no staking rewards** while inactive.
- Large institutional stakes **in a single validator** create an **"all-or-nothing" risk.**
- If that validator goes offline, **100% of that stake is unproductive.**
- Solution: **Spreading stake** across multiple validators ensures a stable yield stream, even if one validator encounters downtime.

2. Strengthening Solana's Nakamoto Coefficient

- Solana's **Nakamoto Coefficient** (currently **19**) represents how many validators must collude to **compromise network security.**
- If institutions **concentrate too much stake** in one validator, this **lowers decentralization** and **increases systemic risk.**
- A higher Nakamoto Coefficient ensures **greater resistance** to network capture or failure.

3. Network Decentralization & Stake Distribution

- A single validator with too much stake can **negatively impact Solana's restart times.**
- Spreading stake across **multiple validators strengthens network resilience** by:
  - **Preventing correlated failures** from infrastructure outages (e.g., cloud provider issues).
  - **Supporting client diversity** (e.g., Jito, Firedancer), ensuring a bug in one client doesn't stall the entire chain.

4. Institutional Standards: Security & Compliance

- High-quality validators ensure:
  - **99.99% uptime.**
  - **Fast response times** for updates and network issues.
  - **Redundant infrastructure** across multiple data centers.
- **SOC 2 & ISO 27001 certifications** prove that validators operate with **enterprise-grade security and compliance.**

5. Conclusion: A Balanced Approach to Staking Policy

To **mitigate systemic risk,** Solana ETPs should implement **staking policies that balance performance with decentralization.**

While high-performance, institutional-grade validators play an important role, limiting stake to only a **handful of large operators** introduces unnecessary **vulnerabilities.**

A thoughtfully designed **validator selection process—prioritizing security, compliance (e.g., SOC 2 & ISO 27001 certification), and stake distribution—will create a stronger, more resilient Solana network**, ultimately benefiting both investors and the broader financial ecosystem.

By ensuring that **smaller validators** have the opportunity to participate in **ETP staking**, regulators can foster a network that is:
- **Compliant** and institutionally viable.
- **Secure** and resistant to disruptions.
- **Decentralized**, preserving the long-term value of the SOL asset class.

A **balanced, risk-aware staking strategy** will reinforce Solana's position as a leading blockchain network while **protecting institutional investors** from unnecessary exposure to validator concentration risks.

---

6. SOC 2 and ISO 27001: The Industry Cyber-Security Standards

We have identified **SOC 2** and **ISO 27001** as what we believe to be the most appropriate cyber security standards to tackle the cyber risks associated with providing staking services to ETPs. There is precedent of use with at least 2 industry players, Orangefin and Everstake (a top 10 Solana validator securing over 1B$ in SOL) having both chosen SOC2 and ISO 27001. We have consulted with multiple experts and auditors on the matter and we believe them to be the best path forward.

It should be noted that operating a validator has multiple aspects, both blockchain related and using legacy systems, such as running a server.

As far as blockchain goes, operating the validator does not require you to sign any transactions so you do not have to hold any private keys. The custodian **delegating** to the validator must sign a transaction with their private key. This forms the foundation of Non-Custodial Native Staking on Solana.

The validator operator will mainly be responsible for **securing the server** that is running the "**full node**", which operates the software used to validate and produce blocks on the Solana blockchain.

Security considerations around operating this server infrastructure revolve around the following **key objectives**:

KEY OBJECTIVES	SOC2	ISO27001
Risk Management	Focuses on identifying, monitoring, and mitigating cybersecurity risks.	Implements an ISMS (Information Security Management System) to manage risks systematically.
Data Protection	Ensures data is encrypted, stored, and processed securely.	Requires risk-based controls to protect information assets.
Compliance Monitoring	Requires continuous monitoring and periodic audits of security controls.	Mandates regular internal audits and reviews of security controls.
Cost Effectiveness (Obtaining Certification)	Typically less expensive for smaller organizations, with a focus on existing operational controls.	Higher upfront costs due to extensive documentation and formalized processes but more comprehensive.

We see both standards as **complementary** to each other and Phase Labs Technologies is currently in the process of obtaining a certification for both.

The last point is important, the industry standards **should not be cost prohibitive**, which lets smaller players enter the market and keep stake decentralized. We should work to keep the **up-front capital barriers low and safety standards high**, and we think this framework achieves both of these goals.