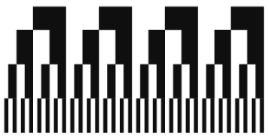
Aleo Network Foundation | www.Aleo.org | 510 LaGuardia Pl 5th Floor
New York, NY 10012



October 17, 2025

Julie Lascar
Director
Office of Strategic Policy, Terrorist Financing and Financial Crimes
U.S. Department of the Treasury

Re: Aleo Network Foundation's Response to Treasury's Request for Comment on Innovative Methods to Detect Illicit Activity Involving Digital Assets, Document No. 2025- 15697

Dear Director Lascar:

The Aleo Network Foundation (the "Foundation") appreciates the opportunity to submit comments in response to the request for comment (RFC) by the U.S. Department of the Treasury ("Treasury") on Innovative Methods to Detect Illicit Activity Involving Digital Assets. The request fulfills the first of many regulatory obligations required under the Guiding and Establishing National Innovation for U.S. Stablecoins Act (GENIUS Act) that will cement U.S. leadership in the global payment stablecoin ecosystem and innovation more broadly.

The Aleo Network ("Aleo") is the first ever Layer-1 blockchain with programmable privacy built into its infrastructure. The Foundation is a 501(c)(4) corporation that provides grants and other ancillary support to builders and developers on Aleo and the broader ecosystem, specifically focused on the potential of applied cryptography and zero-knowledge proofs in the context of decentralized technologies like the internet. The Foundation's leadership team includes former personnel who have served in U.S. Military Special Operations Forces, the U.S. intelligence community, financial regulators, and large technology and payments firms.

At its core, Aleo is powered by zero-knowledge cryptography, combining privacy preserving features with smart contract programmability. By embedding privacy features into Aleo's infrastructure from the outset, Aleo ushers in a new era for decentralized, privacy-preserving computing that can change the internet by protecting user data and enabling a secure experience online with broad applicability to the emerging stablecoin ecosystem. Born from the pages of a 2018 zero-knowledge smart contract project, Zexe[1](co-authored by Howard Wu, Aleo's co-founder), Aleo's genesis block was released in 2024[2], enabling private-by-default functionality and applications combined with secure and confidential user experiences that bridge programmability, risk management, and privacy. Since then, the Foundation has established partnerships with several industry leaders and consortiums including, Request

---

[1] Zexe: Enabling Decentralized Private Computation, Cryptology ePrint Archive, October 2018. Available at: https://eprint.iacr.org/2018/962. At present, Zexe is the only zero-knowledge private smart contract project with a peer-reviewed paper and published in the top computer science security conference.

[2] Aleo announced several upgrades since the launch of mainnet, including a July 2025 update that can be viewed here: https://aleo.org/post/announcing-snarkOS-v4.0.0/. This is all part of the Aleo roadmap, with implementation timelines extending through and beyond 2025. Available here: https://aleo.org/roadmap/

Finance,[3] the Global Dollar Network,[4] Google Cloud,[5] and Revolut,[6] enabling built-in privacy and risk management tools for the next evolution of on-chain finance.

Treasury's Request

Treasury's recent request for comment touches on several key aspects to which the Foundation and the Aleo community is deeply committed. The Foundation is encouraged to see that Treasury will engage, through the Financial Crimes Enforcement Network (FinCEN), on research that explores the potential benefits that blockchain technology can provide to address illicit finance risks. The Foundation is especially focused on the use of emergent technology for digital identity verification and the protection of sensitive information. In particular, the Foundation is responding to the RFC's Question 6 given the widespread benefits that privacy enhancing tools, such as zero-knowledge proofs (ZKPs), will play as the U.S. and global financial services ecosystem increasingly moves on-chain:

> *What innovative or novel methods, techniques, or strategies related to any other innovative technologies such as cryptographic protocols and other privacy-enhancing tools, cloud-based solutions, on-chain compliance tools, oracles, or new verification tools for smart contracts are financial institutions using to detect illicit activity and mitigate illicit finance risks involving digital assets?*

The Foundation believes that advancing zero-knowledge proofs and other privacy preserving technology is critical to the United States remaining at the cutting edge of innovation and protecting everyday people's and companies' data. As our lives become more digital, much more of our personal data is collected online, providing honeypots for hackers and fraudsters. Moreover, the Foundation and builders in the broader Aleo ecosystem are focused on how technology can protect private data even after it is collected by necessity, from being misused by illicit actors. Aleo's ZKP architecture enables new functionalities and techniques to mitigate illicit finance threats involving digital assets. These methods will become even critical for regulators to understand and examine as more of the digital asset ecosystem evolves under a regulatory perimeter that covers traditional finance while allowing for innovation. As Treasury moves forward on its research of innovative approaches to manage illicit finance risks, we look forward to engaging with Treasury and FinCEN in providing additional clarity, examples of, and support for the use of zero-knowledge proofs in delivering built-in privacy to the on-chain ecosystem.

---

[3] Aleo x Request Finance: Private payments made possible, September 4, 2025. Available at: https://aleo.org/post/aleo-request-finance-private-payments-partnership/

[4] Aleo Joins The Global Dollar Network to Advance Privacy-Preserving Stablecoin Infrastructure, August 28, 2025. Available at: https://aleo.org/post/aleo-joins-global-dollar-network-private-stablecoin/. The stablecoin consortium, founded by Paxos, supports various distributors of the USDG stablecoin and includes other members like Robinhood, Worldpay, Standard Chartered, Kraken, and Anchorage Digital.

[5] Aleo collaborates with Google Cloud to advance privacy-preserving computing, February 27, 2025. Available at: https://aleo.org/post/aleo-google-cloud-privacy-preserving-computing/

[6] Aleo announces Partnership with Fintech Unicorn Revolut, August 12, 2025. Available at: https://aleo.org/post/aleo token-revolut-listing/

Finance On-Chain Needs Confidential Transactions

The Foundation commends ongoing efforts by the Trump Administration and Congress to develop agile and effective regulatory guardrails for the digital asset ecosystem. The strong bipartisan votes in the House of Representatives on the GENIUS Act and the CLARITY Act further demonstrates the policy wherewithal in developing a foundation by which the U.S. can become the 'Crypto Capital of the World', including a broader willingness to rethink and shape the next century of financial markets.

However, the systems and applications that we are currently building and deploying on-chain for mass adoption lack basic privacy protections inherent in traditional infrastructures. Transparency and immutability are core building blocks of the digital asset ecosystem, providing enhanced traceability of funds within architectures that support pseudonymity. The industry has for years striven to develop an ecosystem that supports decentralized money, programmable contracts, and global accessibility, and yet in the rush to construct decentralized, global infrastructures we're still building the needed confidentiality functionality to protect personal and other sensitive data.

Today, most blockchain infrastructures deployed expose users by default. This falls short of the confidentiality norms of the traditional banking system and the privacy most consumers have learned to expect. While modern cryptography can address these privacy gaps, many blockchain "privacy" solutions introduce challenges for illicit finance prevention. Aleo's solution bridges this divide; it provides robust privacy for the general public while enabling functionality for appropriate visibility and enforceable controls over on-chain funds. Programmability allows us to address illicit finance risks proactively, instead of relying on tools after-the-fact.

Alternative Approaches to Illicit Finance Risk Management

Zero knowledge proofs are a powerful tool that can be used both by traditional banking systems and with emergent technology participants. New advances in privacy-preserving cryptography, decentralized identity credentials, and risk-based guidelines for cross-chain transfers provide a set of tools that can also be used to support AML/CFT and sanctions compliance by traditional financial institutions and to minimize illicit flows in truly decentralized networks. The following are examples where Aleo's infrastructure advances innovative illicit finance risk management:

Due Diligence and Identity Verification:

- **zPass[7]:** This decentralized credential system allows a user to submit a 'proof' of verified data, like passport information, eliminating the need to share the actual underlying document's data, keeping personal identity information safe from hacks, thefts, and forgeries. The verified credential proof is stored on the Aleo blockchain, but can be accessed online by anyone the user gives permission to view, giving people control over their personal digital data. This approach reduces the regulatory burden and cybersecurity risk of online services storing that data themselves. Users can create these proofs without requiring modification from, or coordination with, identity issuing

---

[7]Introducing zPass: Aleo's pioneering step toward privacy-preserving digital identity, October 2023. Available at: https://aleo.org/post/introducing-zpass-aleos-pioneering-step-toward-privacy-preserving-digital/

authorities. This allows for greater composability and selective attribute disclosure so users can be more selective about how much information they share and with whom, keeping them from exposing any more personal data than is necessary for verification.

- For example, if FinCEN issues guidance that financial institutions can accept decentralized identity credentials to augment their due diligence processes, zPass could be used to support the goals of AML/CFT risk management and sanctions compliance for banks and money service businesses. Notably, zPass has already been used successfully in other non-financial contexts, such as a pilot program for age verification to protect children using online services.[8] Many U.S. states are seeking ways to improve online age verification practices.[9]
- Fully decentralized applications can also be programmed to accept zPass credentials configured for a range of parameters. For example, blockchain software developers could choose to create a decentralized exchange that only allows users to withdraw assets if their zPass credential shows that they are not on the OFAC Specially Designated Nationals list. zPass technology allows developers to further modulate the parameters to include other sanctions lists from the United Kingdom, European Union, etc., as appropriate.

On-Chain Risk Management:

- **ViewKey[10]:** Instead of exposing everything by default, every Aleo account comes with cryptographic "windows" that stay sealed unless the user opens them. These are view keys—protocol-native tools for selective disclosure, built directly into the account model. Regulated financial institutions that integrate products or functionalities on Aleo can use this view key functionality to enable compliance checks and transaction auditing for market integrity. Aleo's view key system includes two distinct layers of visibility: the Account View Key and the Transaction View Key, each designed to provide a different level of disclosure. Users can share Account View Keys to give the recipient (such as a financial institution) read-only access to all encrypted transactions of that account. Transaction View Keys give recipients visibility into only the inputs and outputs of a specific transaction. AML and sanctions compliance teams in traditional financial institutions can use this feature to support transaction monitoring, due diligence, and reporting requirements, when appropriate.
- **ARC-100[11]:** To mitigate the misuse of the Aleo Network by illicit actors, the Foundation established ARC-100, a set of best practices and considerations for builders for managing risks with cross-chain bridges. The ARC-100 procedures direct how bridging protocols on the Aleo Network should handle wallet addresses tied to documented bad actors in the ecosystem. The guidelines also set procedures for transaction limits and

---

[8] Developing an age assurance tool that parents can trust, August 15, 2024. Available at: https://www.commonsensemedia.org/kids-action/articles/developing-an-age-assurance-tool-that-parents-can-trust [9] How zero knowledge tools can help us verify age and protect privacy, July 23, 2025. Available at: https://thehill.com/opinion/technology/5414009-zero-knowledge-identity-protocols/

[10] How the view key solves the privacy vs. compliance dilemma, June 20, 2025. Available at: https://aleo.org/post/aleo-view-key-compliance/

[11] ARC-100 sets best practices for cross-chain operations: https://aleo.org/post/arc-100-sets-best-practices-for-cross chain-operations/; *Also See ARC-100 details at* https://vote.aleo.org/p/100

dynamic timelocks, as well as how to limit bridges' exposure to certain prohibited locations. Although this framework is ultimately voluntary, the broader Aleo community of users and developers and the Foundation encourages validators to stay vigilant and take necessary precautions as on-chain risks evolve. The guidelines also can be adapted to the risk environment as bad actors change tactics and different threats to the network emerge.

Stablecoin Integration and Security:

- **Secure Stablecoin Transaction Infrastructure:** Aleo maintains secure infrastructure for stablecoins that can be adopted by any GENIUS Act-compliant payment stablecoin issuer. Aleo's stablecoin functionality ensures that sensitive information such as participant identities and transaction amounts are kept confidential, similar to how online banking and credit card transactions are encrypted and not visible to external parties. Stablecoins are now an important part of the blockchain ecosystem and are beginning to make inroads into traditional finance. Today, their aggregate market cap is roughly $280 billion,[12] and in 2024 alone stablecoin transactions reached $26 trillion.[13] Most stablecoins, however, operate on fully transparent, non-confidential blockchains such as Ethereum, where every transaction is publicly visible—permanently. The Foundation sees Aleo's functionality as the necessary new standard for stablecoin architecture in order for payment stablecoins to be adopted widely by institutions and individuals.

The use of Zero Knowledge Proofs on public blockchains helps to resolve the long-standing tension between permissionless access and the need for risk management by enabling verifiable credentialing with selective disclosure. Zero knowledge cryptography allows users to prove the validity of information - such as identity or solvency - without revealing the underlying data. In practical terms, this means users can support the aims of AML/CFT rules to combat illicit activity without exposing every transaction to the world.

The future of payments demands confidentiality, security, and the management of risk. Without this combination, the U.S.'s ability to become the 'Crypto Capital of the World' will face significant challenges. While an open, transparent, and globally accessible on-chain ecosystem poses considerable opportunities for users and the broader industry, the lack of incorporating privacy at the outset could curtail widespread adoption and pose substantial risks to a user's wellbeing. It is essential that as Treasury and FinCEN undertake research, as required under the GENIUS Act, to understand how regulated financial institutions are using novel and unique methods and technologies to detect illicit finance, that they also consider the role zero knowledge proofs play in developing an on-chain ecosystem that is open, compliant, and respects an individual's right to privacy.

---

[12] Stablecoin market capitalization reaches ATH of $278B in August, October 1, 2025. Available at: https://www.coindesk.com/research/stablecoins-and-cbdcs-report-august-2025

[13] Stablecoins: Five killer tests to gauge their potential, May 2025. Available at: https://media publications.bcg.com/Stablecoins-five-killer-tests-to-gauge-their-potential.pdf

Thank you again for the opportunity to comment and we look forward to engaging with both the Treasury to help support the research effort.

Respectfully,

Kari Zeni
General Counsel
Aleo Network Foundation