Stablecoin Privacy

Balancing Privacy and Risk Through Permissionless
Private Stablecoin Infrastructure

Authors:

Yaya J. Fanusie — Global Head of Policy - Aleo

Valerie-Leila Jaber — Senior Advisor - Crypto Council for Innovation

Matthew Green — Scientist - Forte Labs

Aleo

Stablecoin Privacy:
Balancing Privacy & Risk Through Permissionless Private Stablecoin Infrastructure

Acknowledgements

Content contibutors

Yaya J. Fanusie

Valerie-Leila Jaber

Matthew Green

Curators and editors

John Reynolds

Roy Rotstein

Kari Zeni

Leena Im

Designer

Yuji Heid

Table of Contents

Abstract

The widespread adoption of stablecoins anticipated under the GENIUS Act risks being constrained by a fundamental architectural problem: public blockchains expose every transaction to anyone on the internet, permanently. This paper presents a solution — a permissionless private stablecoin architecture built on the Aleo network using zero-knowledge proof technology and programmable smart contracts — where financial privacy and institutional risk management are not in tension but are built from the same set of foundational components. Three interlocking building blocks give regulated institutions the tools to meet their compliance obligations without making every transaction visible to the world. The paper walks through how the system works in practice, how risk oversight is maintained throughout, and how the architecture holds up across real-world use cases, before closing with recommendations for issuers, regulators, and the broader ecosystem. Privacy-preserving stablecoin infrastructure is not a niche application or a regulatory workaround — it is the missing layer that makes public blockchain payment rails viable for mainstream commercial use.

I. The Privacy Challenge of Stablecoins

Lack of financial privacy

Public blockchains' most elegant features–their transparency and full tracability–actually hinder their commercial use for consumer and business transactions. Most blockchains, by design, offer little privacy. The confidentiality offered by a pseudonymous alphanumeric address is easily undermined due to the exposure of the full transactional history and ongoing activity of that address as well as the trackability of all its interactions. Whilst the transparency and immutability of public distributed ledger technology supports auditability and can bolster regulatory enforcement, the widespread adoption of stablecoins expected in the wake of the GENIUS Act[1] risks being stunted by the practical limitations for commercial and personal use of digital assets when their transactions are visible to anyone on the internet, forever.

In theory, public stablecoins should be the 'killer app' that brings digital assets to mainstream payments usage. Public stablecoins solve for the volatility and price fluctuations inherent in most crypto assets and can be utilized across varying use cases, including: Treasury re-balancing, settlements, vendor payments, payroll, donations, remittances, and individual retail purchases. Indeed the use of public stablecoins such as USDC and USDT has skyrocketed in recent years, and now exceeds $300 billion, up from $30 billion in 2020, primarily driven by trading volumes and internal flows,[2] rather than consumer payments. One reason stablecoins have not been used much more for payments lies with the architecture itself. Public stablecoins' transparency broadcasts user data leaving it exposed and vulnerable to exploitation, competitive disadvantages, and, increasingly, even physical harm if wallet holders get doxxed through blockchain analytics, dusting attacks and other tactics

[1] GENIUS Act of 2025, S. 1582, 119th Cong. (2025), https://www.congress.gov/bill/119th-congress/senate-bill/1582.
[2] Matt Higginson, "Stablecoins in Payments: What the Raw Transaction Numbers Miss," McKinsey & Company and Artemis Analytics, February 18, 2026, https://www.mckinsey.com/industries/financial-services/our-insights/stablecoins-in-payments-what-the-raw-transaction-numbers-miss.

aimed at breaking the thin barrier of address pseudonymity.

The imperative of financial privacy is not new. It is embedded in the traditional financial system. When a consumer pays a merchant with a credit card, or a company sends a wire transfer to its supplier, only the specific information relevant to that transaction is visible. Account balances, transactional histories and other information on ongoing financial relationships are shielded from view and not relevant or utilized to effectuate those underlying transactions. This is not only well-accepted financial privacy, but expected by institutions and consumers alike. Unfortunately, public blockchains that power public stablecoin use do not enable these basic protections.

Imperfect alternatives to preserve financial privacy on blockchains

Most crypto privacy preserving technologies deployed today may not be compatible with institutional mainstream adoption, due to regulatory risks. These technologies include mixers and privacy coins that obscure transaction histories. However, regulated institutions that are the linchpin to commercial stablecoin growth must comply with sanctions and Anti-Money Laundering (AML) obligations that require due diligence on their customers. Utilizing mixers or privacy coins are a non-starter from a regulatory and reputational perspective without added customer due diligence measures that could prove operationally prohibitive. However, even the U.S. Department of Treasury has acknowledged that consumers using digital assets may want to use blockchain privacy tools for the legitimate purposes of financial privacy.[3] Still, many individuals are likely to hesitate to use certain privacy preserving technologies for lawful, personal transactions due to the stigma associated with potentially commingling their funds with proceeds of illicit activity.

Any financial service, whether traditional finance or crypto-based, centralized, or decentralized, will receive negative law enforcement and regulatory attention if it is discovered to be used significantly for money laundering or sanctions evasion.

[3] U.S. Department of the Treasury, Report to Congress from the Secretary of the Treasury on Innovative Technologies to Counter Illicit Finance Involving Digital Assets, March 2026, https://home.treasury.gov/system/files/246/GENIUS-Act-Illicit-Finance-Innovation-Congressional-Report-March-2026.pdf.

Financial authorities will undoubtedly seek to stop significant illicit usage through civil penalties and enforcement actions, criminal prosecutions, and/or shutting down the service's operations altogether, if technically feasible. If not possible, authorities will try to implement measures to sway the public from using the service, thus isolating it, stunting its liquidity, and making it less attractive for criminal exploitation.[4]

For a privacy preservation tool to be sustainable for both individual and corporate uses, it has to incorporate ways to mitigate the risks of illicit actors who may want to exploit the tool.

Mixers

The first attempt to bring privacy to blockchain transactions emerged through mixers, using different technical methods to obscure the history of users' funds. These privacy-preserving applications such as Tornado Cash, Wasabi Wallet, or CryptoMixer have been used by lawful privacy-seekers, but they have also been exploited significantly by illicit actors because the tools lack strong risk mitigation features. Such mixing tools from a practical perspective do not offer a scalable commercial solution for mainstream crypto adoption. It is well-documented that these obfuscation tools may be highly attractive to use by illicit actors and consequently vulnerable to law enforcement targeting, take-down, or sanction.[5]

While there are legitimate uses for mixers, the multi-layered no-due diligence asset flows they provide are by design not readily mitigated. One new technology aiming to support privacy from mixers while preventing commingling with illicit funds is Privacy Pools, developed out of a white paper coauthored by Vitalik Buterin and privacy-

[4] In some cases, major legal disputes arise over the validity of specific government actions, especially in light of the U.S. Constitution's protections for personal privacy and free speech. Measures currently being proposed in Congressional legislation seek to protect software developers from unfair prosecutions. See Senate Banking Committee, Draft Amendment to the Digital Asset Market Clarity Act, https://www.banking.senate.gov/imo/media/doc/ehf26374.pdf. Even when such disputes are resolved in favor of defendants, the threat of platform stigmatization remains, according to a clear formula: permissionless access combined with anonymization or obfuscation and high transaction volume inevitably attracts illicit actors seeking to launder funds, which in turn invites law enforcement scrutiny and government efforts to shut down the service.

[5] See, e.g., U.S. Department of the Treasury, Office of Foreign Assets Control, designation of Blender.io (May 2022) and designation of Sinbad.io (November 2023); U.S. Department of Justice, indictment of the founders of Samourai Wallet (2024), resulting in convictions (2025).

focused Ethereum developers.[6] Privacy Pools are a smart contract protocol where users can generate proofs showing that their funds have not been associated with a specific set of illicit addresses.

The innovation of Privacy Pools represents a meaningful advance over mixers. Legitimate users have both the ability and incentive to disassociate from illicit deposits, and the separating equilibrium it creates is a genuine contribution to the risk based-privacy design space. However, the approach still depends on deposit-layer transparency: compliance parties must have visibility into deposit information in advance for association sets to function, which constrains the privacy guarantee. Privacy Pools are best understood as a promising step toward reconciling privacy and compliance on public blockchains — but one that stops short of the confidentiality needed for large scale payment infrastructure to move onchain.

Privacy Coins

Privacy coins should be understood as critical options in the digital financial ecosystem, particularly to give individuals the potential to make some transactions that are fully and uncompromisingly private. The regulatory approach to such technology should be to manage the illicit finance risks of private transactions, not eliminate their existence, similar to the risk-based AML approach to physical cash in the economy.

Recent reports have documented the increasing use of privacy coins. According to TRM Labs, Monero usage has grown materially since 2020 with transaction volumes in 2024-2025 significantly higher than in 2020-2021.[7] This resilient growth is all the more striking considering that Monero is restricted or has been delisted from key global exchanges.[8] Zcash saw a 25 percent increase in its shielded supply in 2025,[9] becoming one of that year's best performing digital assets.

[6] Vitalik Buterin, Jacob Illum, Matthias Nadler, Fabian Schär, and Ameen Soleimani, "Blockchain Privacy and Regulatory Compliance: Toward a Practical Equilibrium" (2023), https://privacy-pools-website.vercel.app/whitepaper.pdf.
[7] TRM Labs, "Monero in 2025: Persistent Use and Emerging Network Layer Insights," February 13, 2026, https://www.trmlabs.com/resources/blog/monero-in-2025-persistent-use-and-emerging-network-layer-insights.
[8] See TRM Monero Report.
[9] Daniel Kuhn, "From Aztec to Zcash: The Year Pragmatic Privacy Took Root," The Block, December 26, 2025, updated February 9, 2026, https://www.theblock.co/post/383680/aztec-zcash-year-pragmatic-privacy-root.

These increases underscore the urgency of solving the financial privacy challenge in a manner that does not subject users to value fluctuations and liquidity constraints. But, as with mixers, privacy coins have often been associated with potential increased illicit activity. This is particularly true for privacy coins that do not have features to unshield their transactions for risk mitigation measures, as found with Aleo and Zcash. According to TRM Labs, there has been a structural shift to Monero-only darknet marketplaces, citing that in 2025 nearly half (48 percent) of newly launched darknet sites only supported Monero.[10]

However, even with inevitable illicit usage, fully end-to-end private transactions are necessary in a free society and should not be abandoned or banned by regulation, just as cash transactions remain legal and available despite the anonymity they provide and their exploitation by bad actors. For widescale, mainstream use new approaches are needed to balance risk and privacy with digital assets. The potential exposure to and association with illicit activity, varying valuations, together with constrained liquidity makes the use of privacy coins for widescale institutional and commercial use difficult in the current regulatory environment.

Permissioned Networks

A permissioned network, or walled garden, can provide utility for specific use cases amongst known and vetted counterparties. It is essentially similar to an intranet, which limits access and transactional activity based on pre-set rules or conditions. Such permissioning comes at significant operational and infrastructure costs associated with vetting, granting and revoking counterparty access, and maintaining, modifying or canceling the rules and/or conditions set for the bespoke network.

Although permissioned networks can support confidential transactions with counterparties vetted through traditional finance level due diligence obligations, their narrow utility could disincentivize developers from building on such networks and stunt innovative solutions that would otherwise widen the aperture of this technology. Moreover, the tokens issued for transactions within a Walled Garden would have significantly restricted liquidity, making them unattractive for widescale merchant

[10] See TRM Monero Report

acceptance. These limitations hinder scalability as well as composability, both of which are required to offer financial rails that can truly drive global commerce and bring crypto adoption to the next level. A more durable, stable solution is necessary to ensure financial privacy within a permissionless ecosystem. That solution is a permissionless, private stablecoin that possesses risk mitigation programmability.

II. The Viability of Permissionless Private Stablecoins

Permissionless Private Stablecoins Offer Financial Privacy at Scale

Aleo's private stablecoin architecture is built on zero knowledge proof technology combined with smart contract programmability, and derived from the 2018 academic paper Zexe: Enabling Decentralized Private Computation.[11] Unlike most crypto whitepapers, the Zexe paper was peer-reviewed and published in a leading computer science academic journal. The research originated a cryptographic primitive enabling private smart contract applications at scale and even envisioned the use case of "regulation-friendly stablecoins." Three of the coauthors of the paper also co-wrote the 2014 paper Zerocash: Decentralized Anonymous Payments from Bitcoin, which laid the architecture for the Zcash privacy coin.[12] One of the coauthors went on to co-found the Aleo network.

Aleo's Underlying Tech

Encryption, programmable transactions, zero-knowledge proofs, and selective disclosure are the key components to Aleo's general functionality. Validators[13] of the Aleo blockchain see a hash that reveals nothing about the underlying transactions. In Aleo's base layer architecture, private data can only be decrypted by its owner using a view key to see the details of their commitments. The computations of

[11] Sean Bowe, Alessandro Chiesa, Matthew Green, Ian Miers, Pratyush Mishra, and Howard Wu, "Zexe: Enabling Decentralized Private Computation," Cryptology ePrint Archive, Paper 2018/962 (2018), published in Proceedings of the IEEE Symposium on Security and Privacy (IEEE S&P 2020), https://eprint.iacr.org/2018/962.pdf.
[12] Eli Ben-Sasson, Alessandro Chiesa, Christina Garman, Matthew Green, Ian Miers, Eran Tromer, and Madars Virza, "Zerocash: Decentralized Anonymous Payments from Bitcoin," in Proceedings of the 2014 IEEE Symposium on Security and Privacy (San Jose: IEEE, 2014), 459–474, https://ieeexplore.ieee.org/document/6956581.
[13] On the Aleo blockchain, validators are nodes that produce blocks, verify zero-knowledge proofs, and support the network's consensus mechanism. They do not have custody or control of underlying assets; rather, validators support the verification process critical to the security and integrity of the network.

transactions occur offchain, and only the proof is posted to the public chain, allowing all commitments of transactions to be confirmed in milliseconds, no matter the size or complexity of the transaction computation. By keeping transaction computation offchain, institutional-scale transactions can still be easily represented in an encrypted record, giving large transactions the same privacy guarantees as small ones.

Programmability enables customization within the network. All records have a birth predicate (creation rules) and a death predicate (spending conditions), which allows developers to create rules for various transaction types, amounts, and participants. This is a key distinction from previous privacy coins because rules can be enforced cryptographically.

Zero-knowledge proofs make the high throughput possible. When users transact, they generate a zero-knowledge proof stating "I satisfied all predicates." The proof does not reveal the amount, addresses, or what predicates were triggered, but confirms that the mathematics are valid. Validators verify the proof in milliseconds–regardless of transaction complexity–and update the blockchain ledger with the encrypted commitments.[14]

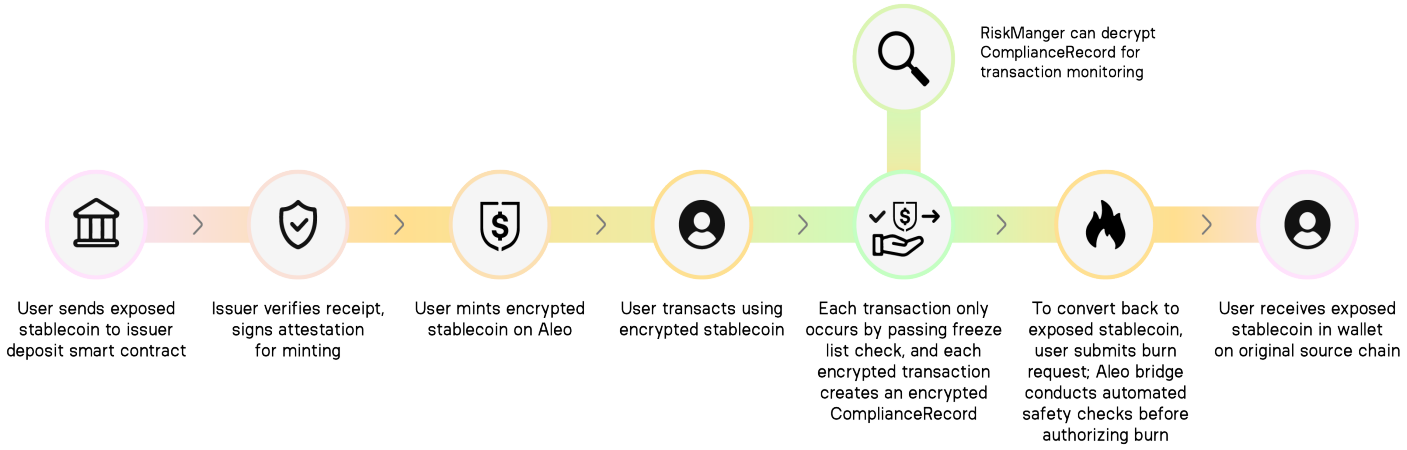
Selective disclosure is a complementary and equally critical component of zero knowledge architecture and consists of both a Transaction View Key and an Account View Key. More specifically, each Aleo transaction emits a read-only Transaction View Key to the two wallets associated with the transfer. The wallet holder can share the view key to allow someone to view the addresses and amounts of the transaction. Also, every address has a read-only Account View Key which, if shared, allows someone to decrypt and view all the transactions of that address. This selective disclosure mechanism allows shielding and unshielding of transactions on the Aleo Network. Adapting this architecture for private stablecoins requires implementing risk mitigation that can address both the public and private states.

[14] Aleo Network Foundation, "Provably Private and Performant Payments Paradigm: Response to DARPA Request for Information (SN-26-23)," February 13, 2026, https://aleo.org/post/response-to-darpa/.

Going from Exposed Stablecoin to Private Stablecoin

This private stablecoin program on Aleo is the actual token contract that keeps track of balances (public) and token records (private). Moving from an "exposed stablecoin" into the Aleo private stablecoin environment requires that the regulated stablecoin issuer[15] provide basic infrastructure and integration with the Aleo network for minting and redeeming the private stablecoin. Below are the general user steps for the minting and burning process.

Acquiring, Transferring and Burning Private Stablecoins on Aleo



Minting Process

- User deposits the exposed stablecoin into a deposit smart contract maintained by the stablecoin issuer on the source chain (e.g., Ethereum, Solana, or another supported network where the exposed stablecoin natively exists).
    - Note: The exposed stablecoin can be acquired directly from the stablecoin issuer or a regulated exchange so that the user has undergone a due diligence process or it can come from peer-to-peer or over-the-counter trading or decentralized exchanges (DEXs) where due diligence is not necessarily associated with the stablecoin acquisition.
- The stablecoin issuer's attester (an automated mechanism) detects the source chain deposit, validates the request for minting, and produces a signed attestation authorizing the minting instructions.
- After the source chain deposit is confirmed, the attester publishes a signed attestation. The user (or a relayer acting on their behalf) fetches the attestation from the issuer's API and submits it to the Aleo bridge program.
- The bridge program verifies the signature and allows the user to mint the private stablecoin to the user, backed 1:1 by the exposed stablecoin locked in the deposit contract on the source chain.
- Minting can either be completed into the public or private state.

[15] The term 'issuer' as used throughout this paper refers to the regulated entity that issues the original fiat-backed stablecoin on the source blockchain.

- Private minting also emits an encrypted ComplianceRecord[16] owned by the RISKMANAGER_ADDRESS address. The "RiskManager" can decrypt the ComplianceRecord for risk monitoring (These features are discussed below under risk mitigation measures).

Burning Process

- If the user holds the stablecoin in private state, they must first convert it to public state before initiating a burn.
- The user submits a burn request to the Aleo bridge contract, specifying the amount and the destination address on the source chain that will receive the released stablecoin.
- The bridge contract on Aleo enforces basic safety checks before finalizing. The bridge must not be paused, the amount must be above the minimum threshold, and the sender's address must not be frozen.
- If all checks pass, the bridge contract invokes the stablecoin program's burn_public function, which reduces the sender's balance and decreases the total token supply on Aleo by the corresponding amount redeemed. The burn transaction is fully public and serves as on-chain verification.
- The attestation mechanism detects the burn, validates it, and publishes a signed attestation authorizing release of the underlying exposed stablecoin on the source chain.
- Once the burn is finalized on Aleo, the user (or a relayer acting on their behalf) submits the burn proof to the issuer's contract on the source chain, which verifies it and releases the exposed stablecoin 1:1 to the native recipient address specified at burn time.

Risk Mitigation Measures as part of Architectural Design

Aleo's private stablecoin environment has three layers of risk mitigation: the asset view key, freeze list capacity, and bridge controls. By integrating with this environment, a regulated stablecoin issuer can enable holders of its stablecoin to transact privately without abandoning risk-based safeguards.

As discussed above, the stablecoin program outputs a ComplianceRecord that enables a predetermined address (RISKMANAGER_ADDRESS) to hold an "Asset View Key" that can decrypt all ComplianceRecords and view the sender address, recipient address, and amount for all flows in the program. This enables the Asset View Key holder to monitor private transactions and conduct risk analysis. There is no personal identification information intrinsically attached to the transactions. However, because the RiskManager can link newly minted private stablecoins to their corresponding

[16] The term "ComplianceRecord" refers to the encrypted transaction receipt emitted by the Aleo network stablecoin program for private-relevant flows, decryptable only by the designated RiskManager. The label reflects the record's intended function as a foundational building block for institutional compliance programs, providing the transactional visibility that regulated institutions and developers can adapt to meet their applicable legal obligations. Program developers and regulated institutions deploying private stablecoin infrastructure may need to assess and implement additional controls as required by applicable law.

exposed tokens in the deposit smart contract, the RiskManager can also continuously monitor the transparent chain transactions to detect if private tokens are illicitly sourced.

Every stablecoin transaction on the Aleo network operates through a public smart contract Freeze List. When a user initiates a transaction to another address, the sender address is checked to determine if it is on the freeze list. Only non-listed addresses can send funds.[17] Addresses can be added to and taken off the list by a designee who has permissions to update the freeze list.

The Asset View Key and the Freeze List are risk mitigation tools built for the regulated stablecoin issuer to implement and operate. The issuer's inhouse personnel can manage these operations or the issuer can hire and oversee third party firms for day-to-day managing, updating, and enforcing of controls, which is common in many financial risk management operations.

Bridge Controls

Bridges are the critical gateway through which private stablecoins enter and exit the Aleo ecosystem, and they function as a layer where off-chain risk management judgments are converted into cryptographically enforced on-chain action. The stablecoin bridge contract on Aleo requires explicit issuer authorization before any minting can occur. Therefore, the bridge would not create tokens unless it receives and verifies a cryptographic approval signal based on the issuer's own risk management directives, meaning the issuer retains direct control over every mint. The bridge also enforces a one-time-use check on each deposit instruction from the user, ensuring the same deposit cannot be processed more than once and preventing double-spending. Before completing any mint, the bridge deterministically checks that the recipient address is not on the freeze list — using a standard check for public mints and a privacy-preserving proof for private mints that confirms non-inclusion without revealing the recipient's identity. On the redemption side, the bridge enforces

[17] As an architectural design choice, the freeze list check is enforced onchain only on the sender to cut transaction time in half rather than checking both sender and recipient. This blocks the address from sending funds, rendering it useless for the user. However, the freeze list is public and wallets can be programmed to enforce freeze list checks on the recipient as well. The issuer can address any law enforcement requests for asset seizure through its policies for the exposed stablecoin on the source chain.

a freeze check on the sender before any burn can complete, making the off-ramp a second hard chokepoint for flagged addresses. A deterministic pause mechanism gives the stablecoin issuer the ability to halt all minting and burning activity in the event of a systemic risk or security incident.

These bridge-level controls are complementary to, and in key respects exceed, the risk management best practices established by the Aleo Network Foundation under ARC-0100, which call for bridge operators across the Aleo ecosystem to implement measures such as transaction screening against sanctioned addresses, real-time monitoring, and geofencing against prohibited jurisdictions.[18] The private stablecoin bridge encodes several of these objectives directly at the program level rather than relying on operator policy alone, giving the risk management framework a harder technical foundation. Taken together with the freeze list and ComplianceRecord monitoring discussed above, bridge risk management controls form the outermost layer of a defense-in-depth architecture: one that screens at entry, monitors throughout, and enforces at exit.

Below is a step-by-step practical example of how the private stablecoin infrastructure employs these mitigation measures, followed by an overview of the constraints faced by bad actors potentially trying to exploit the ecosystem.

Birthday Gift Scenario

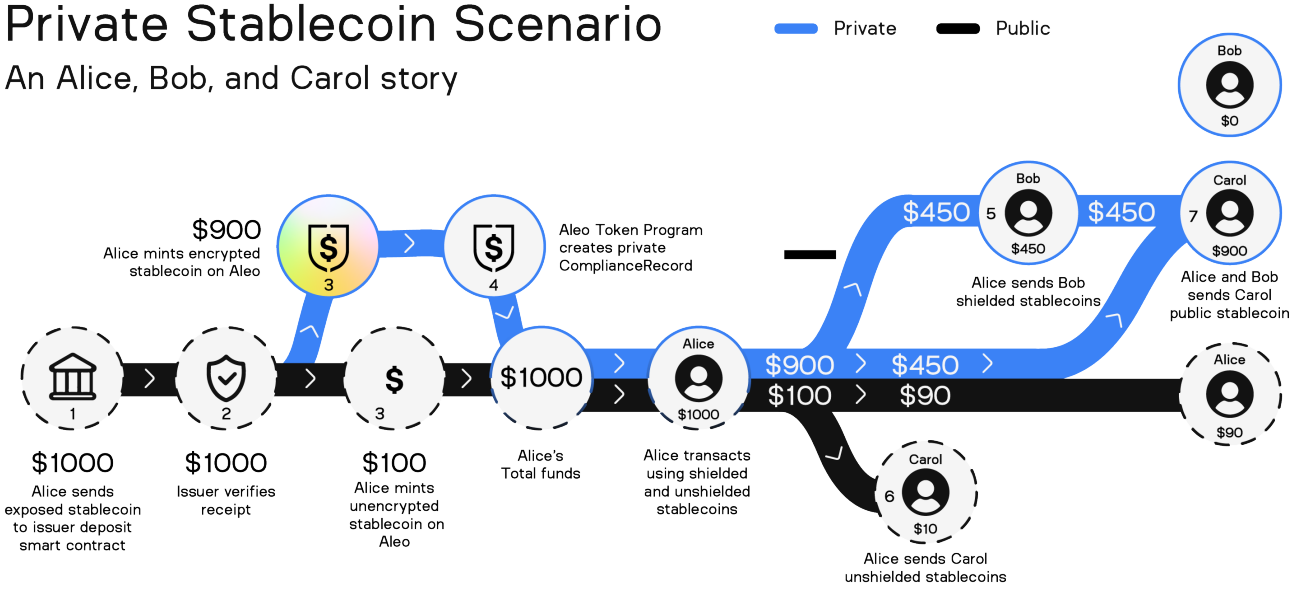
Alice, Bob, and Carol: A Birthday Gift Scenario

Alice, Bob, and Carol are three friends. Alice and Bob want to buy Carol a surprise birthday present. Carol is a crypto enthusiast who only accepts stablecoin funding as a present. She's also a bit obnoxious, but her friends love her. Bob is embarrassed because he has no money to gift Carol. Alice is wealthy. Alice and Bob figure out a way for them both to equally gift Carol, while playing a little joke on her.

[18] Aleo Network Foundation, "ARC-0100: Best Practices for Bridges on Aleo," https://vote.aleo.org/p/arc-0100#best-practices-for-bridges-on-aleo.

Private Stablecoin Scenario

An Alice, Bob, and Carol story



Private Stablecoin Transaction Flow

A demonstration of public and private transaction states on the Aleo network

Public Event Private Event

1

Deposit on Native Chain

Alice sends exposed stablecoin worth $1000 into the stablecoin issuer deposit smart contract address on native chain.

Public Event

2

Screening & Validation

Deposit smart contract operator/attestor (Stablecoin Issuer) does its normal screening (at minimum sanctions/freeze-list policy; possibly additional risk checks off-chain) and does not identify any flags.

Public Event

3

Minting to Aleo

Alice wants $900 minted into the private state and $100 minted into the public state. The bridge tells the Aleo token program to mint $1,000 to Alice's Aleo address according to her preferences; $100 as unshielded/public and $900 as shielded/private. Onchain observers only can see her $100 balance.

Public Event Private Event

4

Private Compliance Record

For the private funds, the Aleo token program creates a private ComplianceRecord which is sent to the RiskManager address. The RiskManager can decrypt this record at any time.

Private Event

5

Private Transfer to Bob

Alice sends $450 private stablecoin to Bob's address. This is a private transaction. Before the transaction is complete, the program checks the freeze list to make sure Bob's address is not on the freeze list, which it is not. Another encrypted ComplianceRecord is sent to the RiskManager address.

Private Event

6

Public Transfer to Carol

On the morning of Carol's birthday, Alice tells Carol she is going to send her a huge birthday present. Carol is excited. Alice sends her $10 of her $100 unshielded (public) stablecoin holdings to Carol's Aleo address. This is a public transaction, but it still is run through the freeze list check for the sender. Alice knows Carol will check the blockchain browser to see how much stablecoin Alice owns. When Carol checks, she sees Alice's public holdings of $100, and notices Alice only sent $10. Carol begins to get upset.

Public Event

7

Private Birthday Surprise

However, Bob calls Carol to tell her there's another surprise and to check her wallet. Bob and Alice then each send Carol $450 in private stablecoin. "We had you fooled!" they tell her. Carol is surprised and laughs – she's happy both her friends sent her so much. And Bob is pleased because Carol can't look at the chain and tell he's broke or that he needed Alice's help; private transfers don't reveal Bob's overall balance publicly, while the RiskManager could still reconstruct what happened later using the ComplianceRecords.

Private Event

RiskManager's View and Actions in the Birthday Gift Scenario

At the start, the RiskManager can see the public, native-chain deposit into the issuer deposit smart contract (the $1,000 going into the deposit address) and can see the Aleo-side mint happen, but what they can directly observe depends on which form was minted. If the mint was public, the RiskManager can see the recipient Aleo address and amount on-chain like any other public balance movement. If the mint was private, the general public can't see "Alice received $1,000," but the token program still emits a ComplianceRecord to the RiskManager address that points to "a mint happened for X amount to Y address," giving the RiskManager a clear risk management trail even when the asset is shielded. In either case, the RiskManager generally still doesn't know "Alice the person" unless that address is linked to an identity off-chain (from the issuer's due diligence relating to the deposit smart contract, information received from law enforcement, etc.), but the RiskManager can do blockchain analysis on the public side (e.g., the native-chain source address and any unshielded Aleo activity) to look for known illicit signals.

When Alice sends $450 privately to Bob and later $450 privately to Carol, the public can't see those private transfers. The RiskManager's visibility comes from the compliance instrumentation in the token program. Private flows (mint_private, burn_private, private transfers, public to private conversions) emit ComplianceRecords that are addressed to the RiskManager. Those records contain the key facts (amount, sender, recipient) in a form intended for risk management review, even when the underlying token movement is private. That's how the RiskManager can learn that "Alice's address sent $450 to Bob" and later "sent $450 to Carol" even if the rest of the network can not.

The ComplianceRecords are the mechanism giving the RiskManager visibility. The Asset View Key allows the RiskManager to review the private activity that the program deliberately reports to the RISKMANAGER_ADDRESS via ComplianceRecords.

Aleo Private Stablecoin Environment: Built-in Deterrent for Exploitation

Aleo's private stablecoin infrastructure has intrinsic risk mitigation measures to disincentivize illicit use of the ecosystem. Access is permissionless, but the freeze list, Asset View key, and bridge controls bring accountability not uniformly present in the broader permissionless environment. Comparing Aleo's infrastructure with the general landscape shows that illicit actors actually would face higher risks by operating in this private stablecoin system.

Although the private stablecoin transactions are hidden from public view, a malicious actor still faces the scrutiny of transaction monitoring (by the RiskManager) and the potential for issuer-directed address freezes built into each transaction pre-computation. Aleo's decentralized bridging guidelines,[19] although voluntary, set illicit finance mitigation standards that are not established in the broader crypto landscape. Alternatively, the bad actor could operate outside the Aleo environment using a self-custodial wallet and have unfettered access to mixers and decentralized exchanges with little risk of freezing. A bad actor entering Aleo's stablecoin program would encounter a privacy environment filled with active measures to discover illicit connections, even absent due diligence or sanctions compliance data.

A Building with Two Doors

Aleo's private stablecoin infrastructure can be understood through a simple analogy. Stablecoin issuers are able to invite the public into a metaphorical building that is open 24/7, but with built-in security features that the issuer oversees. Imagine a building where everyone inside wears a mask — you cannot see their faces or know their names. The building has two entrances. The first is a guarded front door, the approved portal through which users enter by depositing exposed stablecoin through the issuer's intake process. Those who enter this way have been vetted by the bouncer — screened against sanctions lists, cleared by the issuer's attestation process — and carry a lower risk profile as a result. The second is a side door, representing open market or peer-to-peer acquisition. Those who enter this way are also masked, and they haven't been vouched for, so they carry a higher risk profile. But crucially, they are

[19] Aleo Network Foundation, "ARC-0100."

still inside the building. The RiskManager — holding the Asset View Key — can observe what everyone does once inside, regardless of which door they used, and may watch the side-door entrants more closely as a result.

There are also two ways to leave. The approved front door exit is the bridge redemption process, where the bouncer checks you on the way out — freeze list verification, sender screening — before releasing your funds on the native chain. The regulated stablecoin issuer oversees the bouncer and checks your movement through the approved portal. Think of it as handing in your mask and leaving the building. The side exit could be a DEX swap, where you exchange your private stablecoin for another asset and leave — but rather than handing in your mask, you pass it to a stranger on your way out. You've left the building, but the token remains in circulation under a new holder. The RiskManager loses the thread on you specifically, though the freeze list continues to constrain what the new holder can do.

Beyond the door checks, it is worth noting that the freeze list operates continuously throughout a participant's time in the ecosystem — checked on every transaction a participant attempts to execute. An address that entered cleanly can be frozen at any point by the RiskManager or an appointed third-party designee with permissions to update the Freeze List if the RiskManager identifies criminal activity, at which point their funds are effectively immobilized. They can no longer send, and they cannot exit through the approved door. The compliance policy engine infrastructure is not a one-time entry check but an ongoing enforcement environment. The methodology and framework for identifying illicit transactions should be designed and implemented by the stablecoin issuer, in tandem with any third parties such as analytics firms that the issuer hires to support risk management in the specific private stablecoin environment.

For a bad actor, the question is: what does entering this building actually offer? The honest answer is very little, and at considerable cost. Inside the building they are masked from the public but not from the RiskManager, who retains visibility into their activity through ComplianceRecords. They cannot exit cleanly through the approved door without hitting the same freeze list and screening controls as everyone else. And

the alternative — remaining outside in the unregulated ecosystem, using Monero or a variety of DEXs — offers more genuine anonymity with far less risk management tools and infrastructure watching their movements. The building's privacy protects its legitimate occupants from outside surveillance. For bad actors, it is more a potential trap than a refuge.

The above measures are building blocks that come with pilot implementation of the private stablecoin environment. Other risk tools can be added by developers and institutions seeking more fine-tuned risk management or sanctions compliance controls.

Addressing Threat Scenarios

The following are examples of tools and actions to counter exploitation of the private stablecoin ecosystem

Scenario A: Bad Actor Acquires Exposed Stablecoins Illicitly and Mints Private Stablecoin

A bad actor sends public stablecoins (from the exposed chain) into the issuer deposit smart contract to try to convert them into private stablecoins on Aleo. Before anything is minted, the issuer can review the deposit's origin and behavior (sanctions signals, known bad counterparties, wallet clustering, unusual patterns, etc.). If the deposit fails risk management policy, the simplest control is: don't attest it (no signature →the Aleo bridge can't mint).

If a deposit is attested and a mint happens, the system still has a strong on-chain lever: the Risk Manager or the issuer's designee for freeze list updating–all under the oversight of the issuer–can add the Aleo address tied to that activity to the freeze list. Once frozen, that address is effectively boxed in: it can't mint again through the bridge, it can't move funds through the token's public transfer paths, and it can't redeem back out through the bridge burn flow (because the bridge checks the freeze list on burns). In practice, freezing stops a known-bad address from using the system further and from exiting back to the native chain.

Redemption restrictions in the code paths can be summarized as follows:

- Freeze list: if an address is frozen, bridge burns/redemptions won't go through.
- Pause: the bridge has a deterministic pause switch that halts minting/burning entirely.
- Issuer attestation gate: even if someone burns, the issuer can apply policy on the native-side release step; and conversely, if the issuer does not want a deposit to mint, it simply would not sign the attestation.

On "monitor private-to-private activity": the public can't see private transfers, but the system is designed so the RiskManager still gets a trail via ComplianceRecords emitted for private actions (private mint/burn and private transfers). That means the RiskManager can review private flows for internal risk monitoring without making them public.

Scenario B: Bad Actor Acquires Private Stablecoin via Open Market and Not Through a Regulated Exchange

It is possible for a bad actor to acquire private stablecoin tokens through a peer-to-peer transfer or decentralized exchange, circumventing the issuer's primary market intake and any associated due diligence process. This is a realistic scenario — secondary market activity is permissionless by design, and no architecture can prevent it entirely without sacrificing the open access that makes the ecosystem viable.

The relevant question is not whether this is possible, but whether the bad actor is better or worse off than with the realistic alternatives. A sophisticated illicit actor who cannot or will not use the primary market already has access to Monero, unregulated decentralized exchanges, and traditional mixing services — none of which have ComplianceRecords, freeze lists, or issuer-controlled off-ramp gates. Entering the Aleo private stablecoin environment instead means accepting a risk mitigation infrastructure that those alternatives lack. The RiskManager retains visibility into all private flows via ComplianceRecords, enabling pattern detection across addresses even without a due diligence or sanctions compliance link to the actor's identity. The freeze list remains fully operative regardless of how tokens were acquired — a frozen address cannot send funds or automatically redeem through the bridge, making the

off-ramp a hard enforcement point that open market acquisition does not bypass. And because the bridge burn requires passing the issuer's freeze list checks, the actor's ultimate exit back to the native chain runs through the same chokepoint as any other user.

The Aleo private stablecoin environment is therefore structurally less hospitable to open-market illicit actors than the permissionless alternatives they would otherwise use — not because it eliminates the risk, but because it introduces accountability mechanisms not included in those alternatives. Issuers and bridge operators seeking additional controls for higher-volume environments, including source-of-funds screening before swaps to other assets or restricting swaps to assets with similar risk-mitigation features, can build on this baseline through the bespoke enhancements discussed below.

Enabling Bespoke Risk Management

The baseline risk mitigation architecture described above — ComplianceRecords, the freeze list, and bridge controls — is designed to function at pilot scale in a permissionless environment without imposing friction that would undermine commercial viability. As private stablecoin adoption grows and transaction volumes increase, stablecoin issuers and developers may find it appropriate to layer additional controls on top of Aleo's permissionless architecture, calibrated to their specific risk profiles and regulatory environments.

Some enhancements sit close to the existing infrastructure and could be implemented without significant external dependencies. Transaction volume and velocity limits — capping the amount a single address can send or receive within a given time window — would increase the friction facing bad actors attempting rapid layering or structuring, while preserving normal commercial use for the vast majority of participants. Similarly, time delays on large transactions above a defined threshold would create interdiction windows that give the RiskManager time to act on suspicious patterns identified through ComplianceRecord monitoring before funds move beyond reach. Both of these controls have precedent in traditional AML frameworks and

have been identified by analysts as promising risk based compensating measures for privacy-preserving blockchain systems.[20]

Other enhancements would require external frameworks or ecosystem-level coordination to implement effectively. Decentralized identity credential support — allowing users to cryptographically attest to verified attributes without revealing underlying personal data — could enable more granular, risk-tiered access without sacrificing the permissionless nature of the ecosystem. Conversion restrictions such as limiting swaps to assets whose issuers maintain comparable risk management standards, would address the cross-asset evasion risk that arises when a user exits the private stablecoin environment through a decentralized exchange. As the building analogy illustrates, passing your mask to a stranger on the way out is the primary vector through which RiskManager visibility breaks down. Closing that gap, however, requires coordination across issuers and platforms that goes beyond what any single deployment can achieve unilaterally, and would involve meaningful tradeoffs in composability and market liquidity that institutions will need to weigh carefully.

None of these enhancements are preconditions for a viable private stablecoin deployment. They represent a menu of options for institutions seeking tighter risk management as the ecosystem matures — building on a foundation that is already more accountable than the unregulated alternatives available today.

Enabling Law Enforcement Outreach

Law enforcement investigations often lead investigators to identify criminal exploitation of all types of payment infrastructure. To effectively curb illicit finance, risk mitigation architecture must have a mechanism for responding to law enforcement requests to stop bad actors in their tracks and curtail illicit activity. Under this framework, the RiskManager is operating on behalf of the stablecoin issuer and has the Asset View Key to monitor both public and private chains, making the RiskManager entity best-placed to respond to law enforcement inquiries relating to private

[20] TRM Labs, “On-Chain Privacy and Financial Compliance,” https://www.trmlabs.com/reports-and-whitepapers/on-chain-privacy-and-financial-compliance.

stablecoin use. In addition, the RiskManager may act upon law enforcement requests or court orders to freeze assets in real-time to prevent further transfers or burning, if appropriate.

The RiskManager does not maintain PII or any due diligence records on private stablecoin users, however, its ability to take real-time action and coordinate with law enforcement is central to the safety of the ecosystem. Necessarily, from a policy perspective, any regulatory safe harbors should be extended to the RiskManager for taking such actions.

Overcoming Adoption Challenges

The private stablecoin architecture described in this paper represents a meaningful advance in financial privacy technology, but its path to mainstream adoption requires navigating several regulatory and institutional challenges that are not yet fully resolved.

Need for Regulatory Clarification and Guidance

The most immediate challenge is classification. Private stablecoin tokens being developed today do not necessarily fit cleanly within the permitted payment stablecoin framework established by the GENIUS Act. Rather than being backed directly by fiat, they are backed by an already-issued stablecoin — a structure that falls outside the current regulatory definition without clearly falling into another. Describing these tokens as derivatives would be imprecise and would import a body of regulatory meaning that does not apply. This is a gap that regulators and industry will need to address together.

A related question concerns secondary market activity. Stablecoin issuers will most likely treat open-market acquisition and peer-to-peer transfers of their wrapped token as secondary market activity — activity connected to their issued token but not the token itself, and generally not involving their direct customers. Treasury's recent proposed rule[21] implementing GENIUS Act AML and sanctions requirements reflects this logic, clarifying that permitted payment stablecoin issuers are not obligated to monitor secondary market transactions or file suspicious activity reports

[21] U.S. Department of the Treasury, "Treasury Proposes Rule to Implement the GENIUS Act's Requirements to Counter Illicit Finance," press release, April 8, 2026, https://home.treasury.gov/news/press-releases/sb0435.

(SARs) on them, in part because other regulated institutions in the flow can fulfill those obligations. In the private stablecoin context, however, the privacy architecture complicates the ability of exchanges and other regulated institutions to identify risks associated with their customers' activity in this ecosystem. New processes and tooling will be needed to fill that gap.

Responsibility and Liability

Finally, the role of the RiskManager — which in this architecture may be held by a third party rather than the issuer itself — raises questions about responsibility allocation that some issuers may find unfamiliar. Third-party compliance arrangements are common in traditional finance, and nothing in the current regulatory framework prohibits this structure. But given the novelty of the architecture, clearer regulatory guidance on who bears compliance responsibility in a tiered, multi-party private stablecoin deployment would benefit both issuers and regulators.

A New Category of Payment Infrastructure

These challenges are real, but they should be understood as the growing pains of a genuinely new category of payment infrastructure rather than fundamental objections to the approach. The private stablecoin ecosystem described here offers something that has not previously existed: permissionless access to a stable, dollar-denominated asset with built-in, programmable risk mitigations that can be customized by the institutions that choose to build on it.

The historical parallel is instructive. The addition of SSL encryption to create HTTPS did not merely make the internet more secure — it made commercial activity on the internet possible at scale. Merchants, consumers, and institutions could engage with the technology with confidence precisely because the underlying infrastructure provided privacy and integrity guarantees that HTTP alone could not. Blockchain payment infrastructure faces the same inflection point. Without privacy, public blockchain rails will remain difficult for the commercial and institutional use cases that would drive mainstream adoption. Private stablecoin infrastructure is not a niche application — it is the missing layer that makes the broader ecosystem viable.

Recommendations

For stablecoin issuers and blockchain developers: Pilot deployments of private stablecoin infrastructure should proceed now. The baseline risk mitigation architecture is sufficiently developed to support responsible experimentation, and real-world deployment experience will generate the operational and regulatory learning that theoretical analysis cannot. Waiting for comprehensive regulatory clarity before experimenting is likely to produce neither the clarity nor the experience needed to move forward.

For financial regulators: The regulatory framework for privacy-preserving payment infrastructure is still forming, and the choices made now will shape the ecosystem for years. Regulators should engage directly with the technical and risk mitigation architecture of private stablecoin deployments rather than applying frameworks designed for transparent chains or for intermediated finance. In comments submitted to the US Office for the Comptroller of the Currency (OCC) on its GENIUS Act proposed rule, the Aleo Network Foundation ("Foundation") identified a structural gap in the proposed rule: by defining distributed ledger data as publicly available information, the rule effectively excludes on-chain transaction data from nonpublic personal information protections — regardless of whether the issuer could have prevented that exposure through privacy-preserving infrastructure.[22] The Foundation recommended that the OCC establish transaction confidentiality as an affirmative data privacy standard, clarify that privacy-preserving architectures satisfy the rule's operational and consumer protection requirements, and recognize selective disclosure mechanisms as sufficient to meet examination and transparency obligations. The Foundation comment letter makes the broader case that federal stablecoin regulation should affirmatively accommodate privacy-preserving blockchain architectures — removing regulatory uncertainty that might otherwise discourage issuers from adopting infrastructure that better protects consumers. Separately, for the Bank Secrecy Act, issues around the Travel Rule — particularly how originator and beneficiary information requirements apply when regulated institutions transact in privacy-preserving environments — warrants dedicated attention and coordination between FinCEN,

[22] Aleo Network Foundation, "Aleo Comment Letter on OCC GENIUS Act Rulemaking," https://aleo.org/post/occ-genius-letter/.

industry, and blockchain analytics providers.

For the broader ecosystem: New risk monitoring infrastructure purpose-built for privacy-preserving blockchain environments will be essential. Existing blockchain analytics tools were designed for transparent chains and require significant rearchitecting to interface meaningfully with private transaction ecosystems. Industry participants are beginning to develop these solutions, and their maturation will be a prerequisite for regulated institutions to participate in private stablecoin markets with confidence. This is not a problem that any single actor can solve unilaterally — it requires coordination across issuers, analytics providers, regulators, and protocol developers.

The technology is ready. The regulatory and institutional infrastructure is catching up. The question is whether the participants in this ecosystem — industry, regulators, and developers alike — will engage with sufficient seriousness and speed to realize the opportunity before it is foreclosed by regulatory inaction or misdirected enforcement.

Acknowledgments

The authors would like to thank John Reynolds, Alex Kim, and Roy Rotstein for their technical input and review of this paper. We also thank Kari Zeni, Kyle Zink, Jun Harada, Leena Im, and Koh Harada for their helpful feedback and edits. Special thanks to Yuji Heid for designing the paper's graphics and layout.