FI RFPs

- Fidelity International (Due @October 16, 2025), source
- PJ Lhullier (Cebuana) (no due date, but ASAP)
  - ▼ Email

    Good morning!

    As requested, creating this new email thread.

    As mentioned in my previous email, we've recently received feedback from our central bank (Bangko Sentral ng Pilipinas, BSP) for our Sandbox application. As we write our response, we would appreciate it if you can endorse us to someone from your team who can help us provide more context on the tech side Solana.

    BSP: *A risk assessment covering concentration risks from reliance on Solana as a single point of failure, with corresponding impact analysis, mitigation measures, fallback procedures, and clear activation authority and escalation paths. The assessment should also address broader risk domains, including custody and physical gold risks, liquidity and redemption risks, operational and human error risks, AML/CFT vulnerabilities (particularly if tokens are moved to non-custodial wallets), consumer protection risks such as mis-selling or fraud, and vendor dependency risks.*

    In your submitted Application – Innovative Characteristics, PJLI highlights the use of the Solana blockchain and Fireblocks Console for token issuance, custody, and lifecycle management. PJLI must justify this choice and outline contingency measures such as fallback procedures, manual settlement protocols, or portability to alternative chains.

    - Solana as a critical service provider, we'd like to request if you can share your standard backup plan in case of extended downtime and what safeguards exist against insider collusion or mismanagement. Additionally, any documentation which entails your recourse mechanisms, including whether insurance, refunds, or recovery processes apply if users lose tokens due to scams, hacks, or wallet compromises, or whether such risks remain solely with customers. And if you could share who within the Solana Foundation or your development ecosystem is responsible for declaring a service disruption and authorizing the activation of these pre-defined fallback or contingency measures.

- On the second point, how does the Solana ledger guarantee the accuracy of data (and backup) on all four token states (Minted, Issued to PDAX, Redeemed, and Burned) throughout the token lifecycle? Beyond speed and cost, would it be possible to share the specific features of the Solana architecture (Proof of History, Sealevel, etc.) which provide superior auditability, security, and integrity that make it the optimal choice for a highly regulated financial product like CEB-T? Lastly, given the regulatory necessity to address technology concentration risk, could you please provide the technical and governance process for portability to alternative chains in the event of a significant service disruption?

If this is readily available in your website, we'd appreciate it if you can share a direct link.

Thank you!

ANGELI K. SOLANA

FOREX Officer

Treasury - Finance Group

P.J. Lhuillier, Inc.

1782 N. Garcia cor. Candelaria Sts., Makati City

(02) 7759-9888 / (02) 8779-9888 Local 1505

Mobile: +63926 065 4660

- Solana as a critical service provider, we'd like to request if you can share your standard backup plan in case of extended downtime and what safeguards exist against insider collusion or mismanagement. Additionally, any documentation which entails your recourse mechanisms, including whether insurance, refunds, or recovery processes apply if users lose tokens due to scams, hacks, or wallet compromises, or whether such risks remain solely with customers. And if you could share who within the Solana Foundation or your development ecosystem is responsible for declaring a service disruption and authorizing the activation of these pre-defined fallback or contingency measures.

    - **Business Continuity and Backup Planning**

      Solana's network is designed for **decentralized fault tolerance**, not centralized restart. Every validator maintains a **complete, cryptographically verified copy of the ledger**, and the network can recover from local or regional outages without coordination from a central party.

      Key continuity mechanisms:

        - **Ledger Replication:**

          Each validator independently stores the full ledger and regularly generates **snapshot checkpoints**. In case of downtime, any validator can replay from the most recent finalized slot to fully restore state.

        - **Distributed Resilience:**

          With ~1,000 validators across 40+ countries, there is **no single point of failure**. Even during regional outages or datacenter failures, block production continues globally.

        - **Extended Downtime Recovery:**

If the majority of stake-weighted validators become unavailable or desynchronized, the network follows a **coordinated restart procedure**.

    - Validators replay the last finalized snapshot.
    - The new leader schedule is derived deterministically from the existing ledger.
    - Restart coordination is handled via signed consensus messages in public validator channels (Discord, mailing list).
    - **No user funds are altered or rolled back.**

- **Insider Collusion and Governance Safeguards**

  Foundation / Core Contributor Controls:

    - The **Solana Foundation** has *no ability to unilaterally alter ledger state or seize assets*. In fact, the Solana Foundation does not operate any validators on Solana mainnet-beta.
    - Core development organizations (e.g., **Anza**, **Jito**, **Jump/Firedancer**) operate under **independent governance and code-review pipelines**.
    - All releases are **open-source, peer-reviewed, and signed** before deployment; no single individual can push unverified code to production.
    - Foundation-delegated stake is distributed across hundreds of independent validators to prevent concentration, and is never deployed to the superminority of validators.
    - Multi-signature access controls are used for all treasury, grant, and key infrastructure operations.

- **Community Oversight:**

  Critical changes (e.g., protocol upgrades or coordinated restarts) require **super-majority validator adoption (>80 % stake weight)** and are transparently discussed in public release channels.

- Solana is a **public, non-custodial blockchain**, so **user custody and transaction signing remain the responsibility of the wallet or custodian**.

  The Solana Foundation does **not hold user funds** and therefore **cannot issue refunds or restitution** for scams, private-key compromises, or third-party hacks.

  However, user protection is reinforced at the ecosystem level:

  - **Custodial partners** (Anchorage, Coinbase Custody, Fireblocks, BitGo) maintain **regulated insurance coverage** for assets held under their control.
  - **Stablecoin issuers** (e.g., Circle for USDC) provide contractual redemption rights for verified holders.
  - **Ecosystem risk disclosures** are published at solana.com/security.
  - The **Foundation bug bounty program (via Immunefi)** compensates ethical disclosures of security issues up to **USD $1 million,** and any Agave-related security vulnerabilities are subject to rewards: https://github.com/anza-xyz/agave/security

  In all other cases, **self-custody risk rests with users or their custodians**, consistent with open-blockchain principles.

- On the second point, how does the Solana ledger guarantee the accuracy of data (and backup) on all four token states (Minted, Issued to PDAX, Redeemed, and Burned) throughout the token lifecycle? Beyond speed and cost, would it be possible to share the specific features of the Solana architecture (Proof of History, Sealevel, etc.) which provide superior auditability, security, and integrity that make it the optimal choice for a highly regulated financial product like CEB-T? Lastly, given the regulatory necessity to address technology concentration risk, could you please provide the technical and governance process for portability to alternative chains in the event of a significant service disruption?

  - **Data Accuracy and Lifecycle Integrity**

    Solana guarantees the accuracy and immutability of all token lifecycle events — *Minted, Issued, Redeemed, and Burned* — through its

account-based model, **cryptographic signatures**, and **deterministic ledger validation**.

Mechanisms ensuring data fidelity:

- **Atomic state transitions:**

  Each token event (mint, transfer, burn) is represented as an atomic, signed transaction referencing specific accounts. Either the entire transaction executes successfully, or it fails entirely — preventing partial or inconsistent state changes.

- **Deterministic ledger replication:**

  Every validator maintains a full copy of the ledger and independently verifies every signature, instruction, and account mutation before appending to the chain.

  Consensus ensures that all honest validators record *identical* token states.

- **On-chain program invariants:**

  SPL Token (and Token-2022) programs enforce strict invariants — total minted = circulating + burned.

  Mint authorities and freeze authorities are publicly visible, ensuring each state change can be reconciled cryptographically.

This makes Solana a **source of record** for the full lifecycle of any regulated token (including asset-backed or stablecoin issuances like *CEB-T*), guaranteeing ledger-wide consistency and auditability.

- **Architectural Features Enabling Auditability, Security, and Integrity**

Architectural Feature	Function	Benefit to Regulated Products
Proof of History (PoH)	Cryptographic timestamping of every event via a verifiable SHA-256 sequence	Creates an immutable time-ordered audit trail for every token action
Tower BFT (PoS Consensus)	Stake-weighted voting ensures ≥ ⅔ of validators confirm each block	Guarantees data finality and tamper resistance

Architectural Feature	Function	Benefit to Regulated Products
Sealevel Runtime	Parallel transaction execution with declared account access lists	Prevents double-spending and enforces deterministic replay
Account Model (vs. UTXO)	Explicit account ownership and state tracking	Enables continuous reconciliation of minted, issued, and burned balances
Verified Builds + Open Source	Every core program's binary is verifiable from source	Ensures public auditability and prevents hidden logic changes
Confidential Transfers (Token-2022)	Encrypted balances with auditor keys	Enables privacy for counterparties while maintaining regulatory audit rights

- **Technology Concentration Risk and Chain Portability**

Solana's governance and open-source model explicitly address **portability and resilience**, ensuring issuers are not locked into a single operator or chain.

Governance and portability process:

1. **Open-source standard compliance:**

   Solana's token programs (SPL / Token-2022) are open and portable; the same token schema can be redeployed on alternative chains (e.g., other SVM or EVM environments) without proprietary dependencies.

2. **Bridging and escrow frameworks:**

   Assets can be migrated using audited cross-chain bridges (e.g., Wormhole, Circle CCTP, Axelar) by freezing mint authority on Solana and issuing equivalent supply on a secondary chain, maintaining 1:1 audit reconciliation.

3. **Regulated issuer controls:**

Mint authority always resides with the regulated entity (e.g., PDAX or an appointed custodian). Should Solana experience sustained service disruption, the issuer can deterministically reconstruct balances and reissue tokens elsewhere using on-chain state proofs.

4. **Validator and governance coordination:**

   Any coordinated network restart or migration would be declared publicly by the **Solana Foundation Incident Response Group**, with input from **Anza**, **core validators**, and the **issuer's own governance body** to ensure transparent and regulator-notified execution.

- Mercari (due @October 24, 2025), source
  - What are the transaction processing capability (TPS) , transaction time, transaction fees(gas fees) of your chain?
  - Please tell us about the developer environment and support system. For example, are technical documentation, SDKs, testnets, and support contacts well-provided?
  - Please share your future technology roadmap and new feature plans. In particular, please let us know if there are any updates planned that would be relevant to our use case (global wholesale market using NFTs).
  - What is the current ecosystem size of your chain (e.g., number of users, number of transactions, number of major applications)?
    - Also, could you tell us about your future growth prospects?"
  - What are the ways to appeal to users within the chain's ecosystem when launching a new DApp (e.g., announcements on social media/blogs, DApp display on Wallet App, etc.)?
  - What support can your chain provide, such as marketing support for new projects and funding from the ecosystem fund?
  - Is there any room for support that would contribute to the growth of the RWA marketplace we are considering, such as: providing a track record of bridging with DApps on the chain, or introducing IP holders of the assets to be tokenized?

    - In addition, could you please tell us about any other noteworthy strengths or selling points of your chain?
- Nasdaq
- Business case for rent reduction