Federal Deposit Insurance Corporation
New York Regional Office
350 Fifth Avenue, Suite 1200, New York, New York 10118

January 5, 2023

[redacted]
President and Chief Executive Officer
[redacted]

Subject: [redacted]

Dear [redacted]

On September 14, 2022, the FDIC met with you and other members of management to discuss the bank's proposed [redacted] product and pilot launch. In our letter to you on March 25, 2022, we stated we had a number of questions based on the discussion and information provided to date. The September 14, 2022 meeting and additional comments received on September 20, 2022 and October 31, 2022, provided some useful additional information. During the meeting and in follow-up correspondence you expressed a desire to begin providing the product to [redacted]

We recognize the efforts by your institution to develop the [redacted] product. We also recognize that emerging crypto-related activities may present potential opportunities for financial institutions; however, these nascent activities also introduce significant safety and soundness risks for banking organizations and their customers, and may present potential systemic risk to the U.S. financial system. As discussed with you previously, the proposed [redacted] product raises several novel and complex considerations related to safety and soundness risks. Matters presenting significant risks include, but are not limited to: the use of a decentralized public blockchain; the financial institution operating as and relying on third-party nodes; and bank ownership, use, and holding of crypto-assets.

One area of particular concern related to [redacted] is the bank's ability to quantify, monitor, and control risk related to operating on the public [redacted]. The software runs across a decentralized, open network without customary governance mechanisms; importantly, there are no owners or board of directors/trustees with fiduciary responsibilities related to the network. Also, the bank would not be able to have a contract with [redacted]. Contracts are a critical tool for managing third-party risk as they establish and document specific expectations and obligations of both the financial institution and their technology service providers on a range of issues. For example, without a contract the bank may not be able to fully understand: (1) the responsibilities

regarding business continuity and may not have sufficient detail to manage that risk; (2) the responsibilities regarding network security such as software code security and incident notification to the bank, regulators, or law enforcement; and (3) the recourse available to the bank should service be disrupted. It is not clear how the bank's internal audit system could provide for adequate testing and review of such an information system.[1]

The bank's reliance on third parties for validation of customer entries on a decentralized public blockchain to support its books and records is not only novel, it also raises critical questions regarding the safety and soundness of the proposal, including the adequacy of management information systems, internal controls, and information security.[2] For example, information security standards state that an institution's information security program shall be designed to ensure the security and confidentiality of customer information and protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer. In contrast, a central element of the proposal is publication of customer transactions on a public blockchain, with those transactions validated by third-party nodes. Although you have explained the bank would have the ability through the current operating rules of the public to vet node operators that would validate its transactions, these node operators would not be operating under a service agreement or contract with the bank. Additionally, the bank has not thoroughly identified controls to mitigate the risk of unintended centralities.

Finally, the proposal contemplates the bank serving as a node on the public . Node operators, including the bank, would be required to purchase crypto-assets to operate on the public and would receive crypto-assets for their validation services. In response to our questions regarding the safety and soundness of holding such assets on the bank's books, you have emphasized that the amount would be small, as have a minimal value. That may be the case at present, but it may not be in the future. As a class, crypto-assets have demonstrated significant volatility and have no intrinsic value, raising significant safety and soundness concerns as to their appropriateness as a bankable asset. Further, the bank has not addressed the legal permissibility of holding crypto-assets on its books, in any amount, under federal and state law.[3] The bank's legal opinion did not specifically discuss the permissibility regarding the use of a public blockchain; the financial institution operating as and relying on third party nodes; or the bank's ownership, use, and holding of crypto-assets.

For the reasons outlined above, we are unable to determine that the bank has the ability to conduct the proposed product or pilot in a safe and sound manner.

---

[1] See Appendix A to Part 364 of the FDIC's Rules and Regulations, Interagency Guidelines Establishing Standards for Safety and Soundness.
[2] See Appendices A and B to Part 364 of the FDIC's Rules and Regulations, Interagency Guidelines Establishing Standards for Safety and Soundness and Interagency Guidelines Establishing Standards for Information Security.
[3] See Part 362 of the FDIC's Rules and Regulations, Activities of Insured State Banks and Insured Savings Associations.

[redacted]

This letter and its contents are confidential and intended only for the bank's internal use. The disclosure of such confidential supervisory information is governed by Part 309 of the FDIC Rules and Regulations.

Should you have any questions regarding this request please contact Assistant Regional Director Steven P. Slovinski at [redacted].

Sincerely,
Frank R. Hughes
Regional Director

cc: [redacted]