Request for Information and Comment on Digital Assets (RIN 3064-ZA25)

Executive Summary:

The cryptocurrency marketplace transacts several billions of dollars every day with non-bank participants on exchanges not regulated by the OCC, Federal Reserve, or FDIC with assets that have limited clarity on the source of funds. While U.S. banks consider permissible activities based on the OCC's Interpretive Letters 1170, 1172 and 1174 and as the regulators wisely discuss a joint approach to how cryptocurrency should be part of the business of banking, there is a heightened need for a proper framework.

VaultLink's Platform As A Service (PaaS) offering enables insured depository institutions (IDI) to offer cryptocurrency services and real-time payments to its customers all within a walled-off garden of predefined compliance and reporting that can exist within the banking system. All cryptocurrencies coming from a permissionless blockchain are validated via a proprietary gatekeeper to reduce the source of funds risk similar to wire transfers. Cryptocurrency services offered to banks by VaultLink include custody, staking, buying/selling, and tokenization of assets. Real-time payments 24/7/365 are performed via a closed-loop stablecoin with a 1:1 dollar relationship. All payments and value transfers are required to pass VaultLink's money servicing controls gatekeeper before anything can be transferred between bank customers. It is impossible for value to be transferred to a device and circumvent transfer controls or regulatory audit.

A bank's existing infrastructure easily integrates with VaultLink's blockchain-enabled technology. VaultLink's technology stack is designed for ease of system integration via web socket secure and native API's. The core engine and technology that supports VaultLink currently powers over 40 regulated institutional customers including several of the largest equity and cryptocurrency exchanges in the United States and Canada. VaultLink's walled-off garden approach ensures proper regulatory oversight and adherence, as well as future-proofing our financial institutions for digital asset tokenization.

Our team includes leaders who previously worked at the largest blockchain company in the world and have years of expertise within both banking and blockchain. VaultLink appreciates the opportunity to comment on the FDIC's Request For Information on Digital Assets and is happy to provide subject matter expertise to assist both banks and regulators adopt this emerging marketplace in a safe and sound manner.

Questions Regarding Digital Asset Use Cases

2. *What, if any, activities or use cases related to digital assets are IDIs currently engaging in or considering? Please explain, including the nature and scope of the activity. More specifically:*

a) *What, if any, types of specific products or services related to digital assets are IDIs currently offering or considering offering to consumers?*

VaultLink's Platform As A Servce (PaaS) offering helps banks to offer cryptocurrency services and real-time payments via a closed-loop stablecoin to its customers while staying within the same walled-off garden of predefined compliance of the existing banking system. Existing bank customers that have gone through the banks' KYC/AML processes can custody cryptocurrencies, stake cryptocurrencies, buy/sell/transfer cryptocurrencies, and make payments in real-time with controls the same as checks for dollar movement within the bank's platform.

b) *To what extent are IDIs engaging in or considering engaging in activities or providing services related to digital assets that are custodial in nature, and what are the scope of those activities? To what extent are such IDIs engaging in or considering secondary lending?*

Many banks are exploring how they can custody digital assets either internally or within a sub-custodial nature. Given the limited insurance coverage of "mainstream" crypto-custodians, banks are exploring direct insurance coverage for theft.

As stated earlier, crypto activities include staking cryptocurrencies, buying/selling/transferring cryptocurrencies, and making payments in real-time with controls the same as the checks-for-dollar movement.

Secondary lending of is being considered by some IDIs that are looking to explore the cryptocurrency marketplace. It is crucial these IDIs consider the source of the assets and the counterparties' creditworthiness given the extreme volatility of cryptocurrencies.

c) *To what extent are IDIs engaging in or considering activities or providing services related to digital assets that have direct balance sheet impacts?*

Today, cryptocurrencies are not contemplated as on-balance sheet assets and as these types of digital assets are not insured by the FDIC as the US dollar, it would harm the integrity of the banking system if a bank were to lose a customer's cryptocurrency assets. Digital assets should be held in 'cold storage', similar to an electronic vault that represents a customer's safe deposit box. The digital assets could be tokenized in a private chain so that the tracking of transfers can be the same as the existing banking framework of controls.

Without FDIC insurance coverage, it is imperative that the banks, if they choose a sub-

custodian relationship, consider not just the technology holding the assets but also the insurance coverage of the sub custodian. Currently the market capitalization of the crypto marketplace is approximately $1.5 Trillion with only $5 Billion of insurance coverage. Many mainstream sub-custodians range in the 300:1 assets-to-coverage ratio. The VaultLink platform integrates with multiple sub-custodians and has created a framework for each bank to obtain direct insurance coverage at a lower assets-to-coverage ratio.

d) *To what extent are IDIs engaging in or considering activities related to digital assets for other purposes, such as to facilitate internal operations?*

VaultLink has observed IDIs engaging in or consideration other activities including:

i. Real-time transfer of tokenized USD between different internal business units.
ii. Real-time transfer of tokenized USD between counterparties within a closed-loop network.
iii. Balance sheet optimization via tokenization of loans and investments.
iv. Accounting for tokenized USD assets and liabilities using distributed ledger technology.
v. Tracking of suspicious activity via connecting the public blockchain wallets to the names of bank accounts. The blockchain represents every transaction from day 0 to present and then can be continually tracked for better surveillance controls.

3. In terms of the marketplace, where do IDIs see the greatest demand for digital asset-related services, and who are the largest drivers for such services?

The greatest demand for digital asset-related services are split between (1) traditional investment funds, pension funds, asset managers, and sovereign wealth funds, and (2) retail/consumers. The largest drivers for these services include custody, staking, buy/sell/hold and real-time payments.

Questions Regarding Risk and Compliance Management of Digital Assets

4. *To what extent are IDIs' existing risk and compliance management frameworks designed to identify, measure, monitor, and control risks associated with the various digital asset use cases? Do some use cases more easily align with existing risk and compliance management frameworks compared to others? Do, or would, some use cases result in IDIs' developing entirely new or materially different risk and compliance management frameworks?*

Blockchain assets should not be held to any different standard than what we currently use within our banking system. If assets come into the IDI, the source of funds and the transfers should all be monitored. There are different tools to assist this, such as tracking wallet activity on the public blockchain. Once inside the IDI, movement should be in tokenized form rather

than the native cryptocurrency so that controls can be in place, gas or transfer costs can be minimized, and value transfer controls can be utilized.

VaultLink's walled-off garden approach ensures proper regulatory oversight and adherence, as well as future-proofing our financial institutions for digital asset tokenization.

VaultLink provides comprehensive and customizable reporting of digital asset transactions and balances along with full audit traceability in order to ensure that these movements can be incorporated into an IDI's existing risk and compliance framework. In addition to generating reports, all of the associated data can be exposed via the VaultLink APIs for those IDIs that would like to integrate the data directly into their existing applications and tools.

VaultLink provides integrated tooling designed to extend traditional KYC and AML processes to cover the unique characteristics of digital assets. A key component of this is to identify the source of digital assets and to ensure that the regulated banking system has minimal exposure to illicit activity facilitated by digital assets.

Compliance with BSA, KYC, and AML regulations becomes significantly more difficult for assets transacted on the public blockchain as opposed to transactions involving tokenized assets on a closed loop network offered by VaultLink's PaaS model.

5. What unique or particular risks are challenging to measure, monitor, and control for the various digital asset use cases? What unique controls or processes are or could be implemented to address such risks?

Some of the biggest risks are how individuals may manipulate digital assets for regulatory evasion outside the banking system, money laundering, and theft of bearer assets. Regulatory evasion and money laundering concerns are high because several cryptocurrency exchanges validate USD yet do not track the provenance of the crypto asset. These exchanges may have strong AML/KYC policies that comply with BSA laws and be registered as MSB's under FinCEN; yet they are not regulated by the OCC, FDIC, or the FRB. The risk of an IDI directly interfacing with a cryptocurrency exchange to facilitate or coordinate activities exposes the banking network to cryptocurrencies without necessary validation of the digital assets.

Thus, the uniqueness of the need to complete KYC on customers and properly validate the cryptocurrencies themselves have not originated from a malicious user, creates a challenge that requires sophisticated platform software and expertise to support an IDI's exposure to this type of business.

In terms of using blockchain technology outside the banking system, the following challenges are unique and create problems for the ways IDIs must manage their risks today. Some of the potential issues are listed in the following areas below:

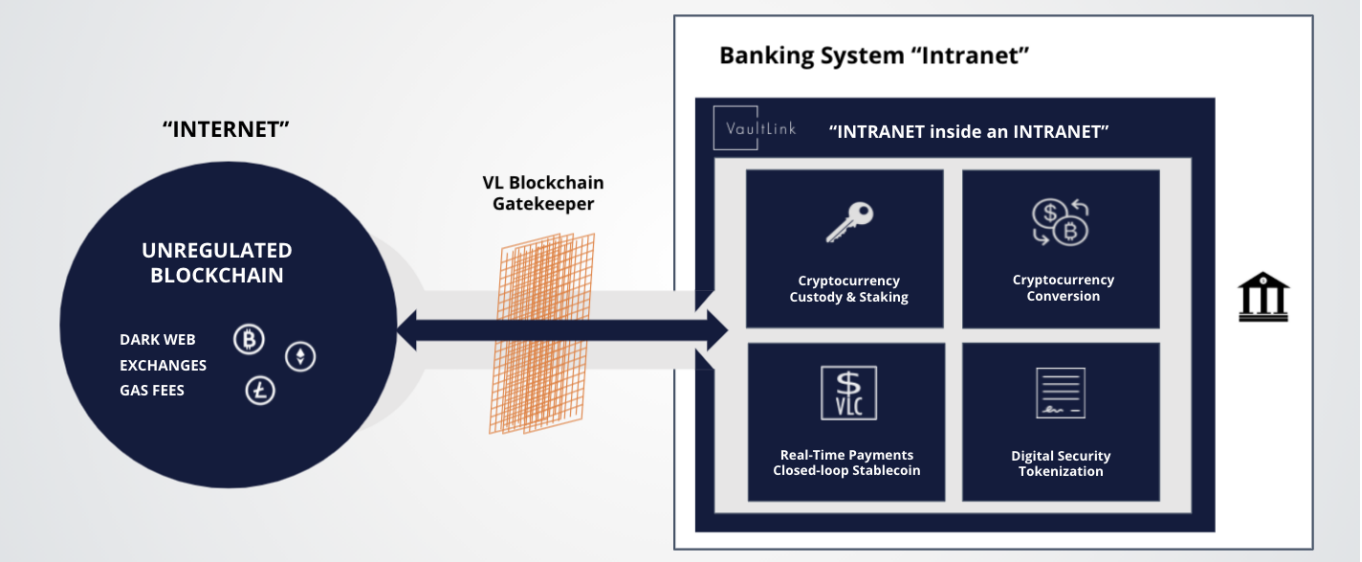
1. Accounts on public blockchain are pseudonymous. There is no authority holding identity

data. The only identifying information is an account number and transaction history.
2. Account creation is completely decentralized, instantaneous, and zero cost.
3. Accounts can therefore be considered both disposable and relatively anonymous.
4. There is no requirement for KYT for blockchain transactions.
5. Mixers, Tumblers, and unregulated exchanges provide further direct and in-direct anonymization of the ultimate owner and source of assets

Ensuring only legitimate, validated and identified assets participate on the VaultLink platform is a key function of the VaultLink Gatekeeper. Once these assets have been validated and accepted into the VaultLink network, these assets can be transacted with the benefit of full KYC transparency.

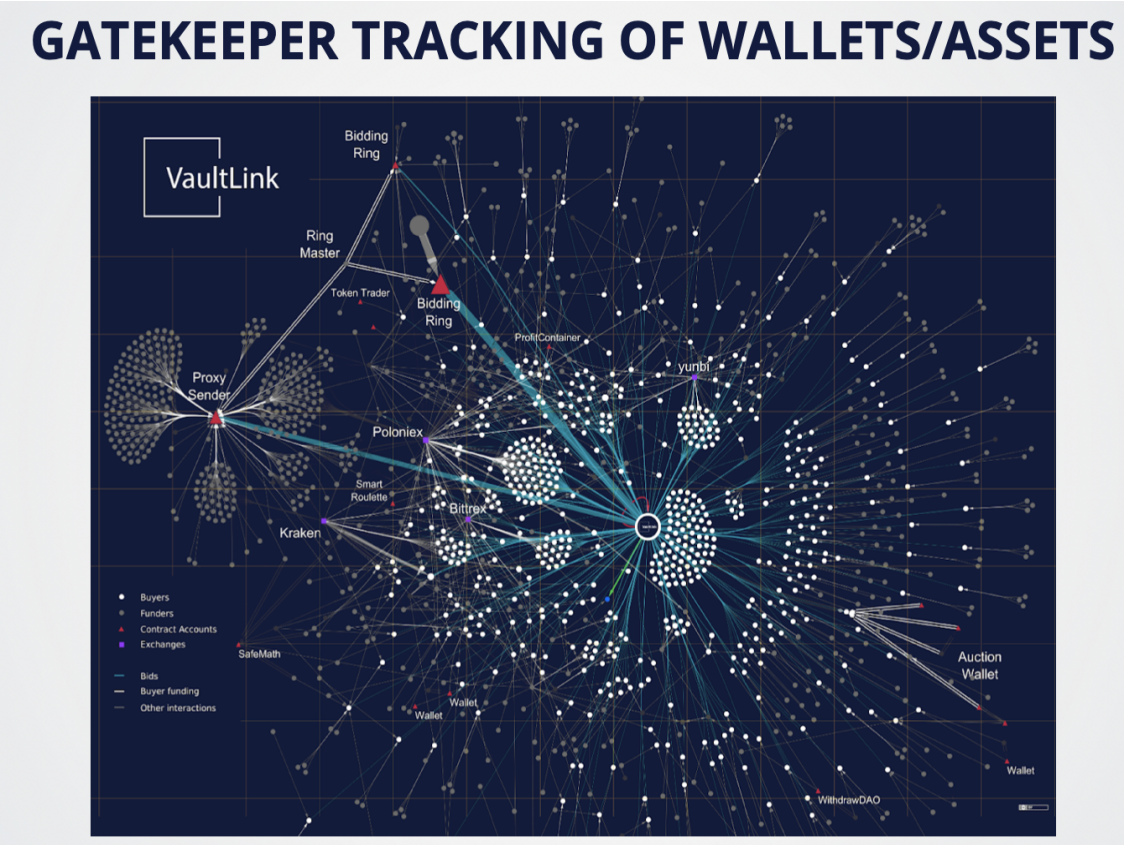
Figure 1 below offers some suggestions for controls include validating the assets prior to coming into and when leaving the IDI.

Figure 1



VaultLink's walled-off garden approach ensures proper regulatory oversight and adherence, as well as future-proofing our financial institutions for digital asset tokenization. Figure 2 below is a pictorial representation of wallets sending value to one investment. Each dot represents a wallet and it is easily seen that clusters are wallets that have some association. If one of the wallets were determined to be a "bad actor" then heightened scrutiny should be applied to associated wallets looking to transfer assets into the IDI.

Figure 2



6. *What unique benefits to operations do IDIs consider as they analyze various digital asset use cases?*

The 'blockchain' implies the possibility of radical change at the settlement layer of the existing infrastructure and how IDIs may hold and secure resources on behalf of customers to reduce cost, friction, and inefficiency.

The advance of this new architecture is heavily mitigated and path dependent because the design of the public permissionless blockchain is fundamentally inconsistent with the pillars of the existing regulatory system.

Still, the obvious benefits inherent to digital assets architecture is in the ability to break down walls between asset classes, institutions and financial behaviors that have to date been held in place by 'ledger silo'. Utility can be extracted by bringing more activity on to a single ledger. Increasing prevalence of cryptocurrency-related architecture and solutions in the global financial system is undeniable and is permeating all levels of the modern financial institutions. Fundamentally, we see a collapse of 'ledger siloes' that have historically separated behaviors in disparate asset classes, regions and institutions.

7. *How are IDIs integrating, or how would IDIs integrate operations related to digital assets with*

legacy banking systems?

Rather than integrate with the public blockchain, which today would be too slow, expensive, and not compliant with existing regulations, IDIs would integrate a wallet infrastructure to help support future services. Current integration would be on a private, permissioned blockchain so as to include all the regulatory oversight and controls necessary.

Questions Regarding Supervision and Activities

10. *Are there any unique aspects of digital asset activities that the FDIC should take into account from a supervisory perspective?*

The public blockchain is an unregulated ecosystem. There is a need to understand and track who is moving value and where that value originated from. VaultLink refers back to its gatekeeper mechanism. The VaultLink gatekeeper tracks what the wallets have done in the past and can be set to alert if a wallet or associated wallet were to be triggered by high-risk scores. We also refer back to our previous comment of making sure that the IDI or sub-custodian has enough insurance coverage for the amount of the crypto assets held.

More technical to blockchain are the risks of these assets themselves. Considerations such as malicious hacks, bugs, forks, airdrops, and planned protocol changes must be considered. These can all have a direct or indirect impact on digital assets held under custody with an IDI. Similarly, there have been malicious hacks and thefts of blockchain assets in the ecosystem. An IDI should have policies and procedures in place to account for and protect against these events beyond just insurance.

It is important to remember that all digital assets are based on a stack of software. At every layer of this stack from the base protocol up through to the software being used by the IDI, can have defects that could result in a loss of digital assets.

By the very nature of public blockchains, all transactions and holdings are public and visible to any individual that is interested. This presents confidentiality issues for both IDIs and potentially their clients as well.

The decentralized nature of blockchains mean that errors can result in an irretrievable loss of assets with no recourse. These errors could be compounded if they are embedded in the software being run by an institution.

What should the FDIC take into account from a supervisory perspective?

The FDIC should take into an account the novel aspects of how to examine:

a. Private key custody procedures for digital assets.
b. Paying Stakeholder Rewards to the appropriate parties.

13. *FDIC's Part 362 application procedures may apply to certain digital asset activities or investments. Is additional clarity needed? Would any changes to FDIC's regulations or the related application filing procedures be helpful in addressing uncertainty surrounding the permissibility of particular types of digital asset-related activity, in order to support IDIs considering or engaging in such activities?*

Our recommendation is that the custody of digital assets be made explicit within the Part 362 application procedures. Banks must have robust anti-money laundering and know-your-customer compliance and reporting infrastructure to support the unique characteristics of digital assets, including the ability to identify the source and provenance of the digital assets to ensure that the banking system is not subjected to undue risk of illicit activity facilitated by digital assets. Digital assets interact with the public blockchain, which is an unregulated ecosystem where regulatory evasion and money laundering concerns exist and which is subject to malicious hacks, bugs, forks, airdrops, and planned protocol changes. VaultLink also recommends that Part 362 make explicit that the bank maintain appropriate levels of insurance coverage for loss and left of digital assets.

Questions Regarding Deposit Insurance and Resolution

15. *Are there distinctions or similarities between fiat-backed stablecoins and stored value products where the underlying funds are held at IDIs and for which pass-through deposit insurance may be available?*

FIAT-backed stablecoins are store valued products. Any assets that can be moved at will and lack insights into tracking and movement put our banking system at risk. Therefore, stablecoins should not be able to transact outside the banking system in the permissionless blockchain but be within the banking system itself. If dollars and dollar value are being moved inside the banking system, it should have the same tracking systems as exist for U.S. dollars today. Given the capabilities of the technology, a company could 'wrap' a token so that we cannot track their movement.

16. *If the FDIC were to encounter any of the digital assets use cases in the resolution process or in a receivership capacity, what complexities might be encountered in valuing, marketing, transferring, operating, or resolving the digital asset activity? What actions should be considered to overcome the complexities?*

This is dependent on what are the checks and balances of the movement involved for the digital assets. The FDIC should require banks using sub-custodians to have multi-signature authority for spending digital assets, whitelisted addresses, and other size limitations and time limitations for movement. In addition, if a bank is entering into a receivership, cybersecurity protocols would need to be put in place prior to closing the bank that would severely limit what existing employees would be able to do without additional oversight by the FDIC.

Additional Considerations

17. *Comments are invited to address any other digital asset-related information stakeholders*

seek to bring to the FDIC's attention. Comments are also welcome about the digital asset-related activities of uninsured banks and nonbanks.

In summary, VaultLink already has a framework for moving U.S. dollars, and employs stringent checks and balances. The technical capabilities that exist with digital assets to tokenize a dollar and move around the system at will goes straight against the current banking system. Our belief is that if there is a decision to tokenize the dollar and allow this kind of value to move, it should be done within a closed loop system such as VaultLink offers. The banking system itself is a closed loop system, so the VaultLink solution fits neatly into how the current banking system exists today. If we continue to enable dollars to be moved on a permissionless blockchain where there is no ability to track who that value moves from, the level of risk increases to the safety and soundness of the U.S. banking system.