ANCHORAGE DIGITAL

One Embarcadero Center #2623
San Francisco, CA 94126

July 16, 2021

James P. Sheesley,
Assistant Executive Secretary,
Attention: Comments-RIN 3064- ZA25,
Federal Deposit Insurance Corporation,
550 17th Street N.W.,
Washington, D.C. 20429

> "Your Government does not intend that the history of the past few years shall be repeated. We do not want and will not have another epidemic of bank failures."
>
> -President Franklin D. Roosevelt, March 12, 1933[1]

In the late 1920s and 1930s, the financial world was in crisis and the American banking system was not spared. Following a decade of expansion, the stock market crash of 1929 triggered a series of cascading events that have come to be known collectively as the Great Depression. Among these events were bank runs of unprecedented scale and intensity, skyrocketing unemployment, plummeting industrial production and GDP, and a wave of foreclosures leaving people on the streets and banks saddled with unsaleable assets.[2] In the years between 1929 and 1933, nearly 4,000 commercial banks failed in the United States, forcing depositors to suffer losses amounting to a figure approximating $1.3 billion[3]—the equivalent of more than $27 billion today.

Perhaps needless to say, consumer confidence in the banking system bottomed out during this time frame. Money itself was so scarce that bartering became a common form of exchange.[4] Recognizing the gravity of the moment, newly-elected President Franklin D. Roosevelt hit pause on the system as a whole, declaring a bank holiday that temporarily closed every bank in the United States.

"It needs no prophet to tell you that when the people find that they can get their money—that they can get it when they want it for all legitimate purposes—the phantom of fear will soon be laid," said Roosevelt, in an address to the American public around the bank holiday and the larger banking crisis.[5] "The success of our whole great national program depends, of course, upon the cooperation of the public—on its intelligent support and use of a reliable system."[6]

---

[1] https://www.fdic.gov/about/history/3-12-33transcript.html
[2] https://www.fdic.gov/about/history/timeline/1930s.html
[3] Ibid.
[4] Ibid.
[5] https://www.fdic.gov/about/history/3-12-33transcript.html
[6] https://www.fdic.gov/about/history/3-12-33transcript.html

In the following years, Roosevelt and others in government leadership would put a concerted effort into reform, developing safeguards that would ultimately contribute to growing consumer support and the financial system's improved reliability. The FDIC was one of them. Originally introduced as a temporary government corporation under authorization by the Banking Act of 1933, the FDIC was given authority to provide banks with deposit insurance, funded by an initial loan of $289 million through the U.S. Treasury and the Federal Reserve Board.[7]

Over time, the FDIC as an organization alongside broader investment in banking safeguards and initiatives to boost consumer confidence have been remarkably effective, with the number of banks in operation remaining essentially stable from 1935—two years after the FDIC was established—through the 1980s.[8] The FDIC has and continues to play a pivotal role in ensuring consumer confidence in the financial system during times of relative uncertainty, and in the everyday operations of the American banking system.

At first glance, it may not seem like the FDIC and cryptocurrency as an asset class have much in common, but in a way, they share something of a common origin story. Bitcoin, like the FDIC, came into existence as a response to financial crisis, some 80 years after the crash that caused the Great Depression. Having lost a substantial amount of trust in institutions deemed "too big to fail," Bitcoin adopters see in it a rule-based, technological solution to many perceived problems of the financial system past and present, namely the risk of inflation associated with what some consider an overreliance on central bank stimulus policies, and the danger centralization can pose to the entire financial system when central players fail. Of course, while cryptocurrency is much more than Bitcoin, and the broader ecosystem itself is still largely in its infancy, there is a clear and growing demand for exposure to this asset class from consumers and institutions alike.

While not an IDI ourselves, as the first and only currently operating federally-chartered digital asset bank in the United States, we feel we are uniquely situated to provide comment on concerns related to the overlap between the legacy banking system and the emerging digital asset space. The demand for cryptocurrency services among consumers is undeniable, and we applaud the FDIC for having the foresight to consider the impact of holding and transacting in this new asset class on end consumers. We believe it is important to allow enough space for innovation to occur in the wider financial system, for consumers to be granted the opportunity to participate in new and emerging asset classes, and for the appropriate oversight to be in place so as to engender the kind of trust in the broader financial system that is necessary to its sound functioning.

Questions Regarding Current and Potential Use Cases

[7] https://www.fdic.gov/about/history/timeline/1930s.html
[8] Ibid.

ANCHORAGE DIGITAL

One Embarcadero Center #2623
San Francisco, CA 94126

1. In addition to the broad categories of digital assets and related activities described above, are there any additional or alternative categories or subcategories that IDIs are engaged in or exploring?

At present, the categories the FDIC included in the Request for Information and Comment on Digital Assets appear exhaustive in a broad sense. That said, the space itself is quickly evolving, and it's extremely likely that IDIs, like other financial institutions, will be exploring ways to best position themselves and best meet the growing digital asset needs of their customers and clients as the market changes. For example, we understand that some community IDIs are beginning to explore offering custodial services for digital assets, but remain cautious about adopting these kinds of services due to a variety of risk mitigation and regulatory concerns.

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?
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?
c. To what extent are IDIs engaging in or considering activities or providing services related to digital assets that have direct balance sheet impacts?
d. To what extent are IDIs engaging in or considering activities related to digital assets for other purposes, such as to facilitate internal operations?

To the best of our knowledge, IDIs are not presently accepting deposits in cryptocurrency. Instead, legacy IDIs are opting to rely on partnerships and third party service providers to sub-custody digital assets. "Banking" for crypto assets, then, is essentially defined as providing custody services, as well as support for crypto-native, on-chain participatory mechanisms like staking and governance. Some IDIs may also be exploring the custody of reserves for the issuance of stablecoins by certain issuers and the use of stablecoins as settlement infrastructure, as expressly permitted by the OCC in Interpretive Letters #1170 and #1174.[9] IDIs will likely play an important and growing role in providing fiat loans to customers who post digital assets as collateral, as well as deposit account and related fiat services (e.g. ACH) to companies in the digital asset space.

While there may be some degree of risk involved in exposure to digital assets themselves, the same is also true of other assets held in custody, be they commodities, securities, and so forth. We believe that, while the mission of the FDIC is to "maintain stability and public confidence in the nation's financial system," that doesn't mean to remove all elements of risk involved in participating in financial markets, particularly emerging markets.

---

[9] https://www.occ.gov/topics/charters-and-licensing/interpretations-and-actions/2020/int1170.pdf; https://www.occ.gov/news-issuances/news-releases/2021/nr-occ-2021-2a.pdf

For the immediate future, we are of the opinion that the best way for IDIs to handle digital assets is to make exceedingly clear the risks of participation through explicit disclosures to that effect, and to hold all digital assets not as deposits, but under custody, at least until the markets mature to the point where they are denominated in cryptoassets. In this way, would-be builders in the digital asset space are allowed to experiment in a way that fosters innovation, consumers can gain the exposure to a new asset class they demand, and the financial system itself is largely shielded from the kind of structural risk that might accompany taking crypto as deposits in the present phase of market development.

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?

It cannot be stressed enough that the digital asset marketplace is still very much in its early days. At present, legacy IDIs are beginning to recognize both consumer and institutional demand for exposure to digital assets. As long-trusted financial partners, IDIs are now exploring ways to meet this demand.

As a federally-chartered trust bank, Anchorage Digital Bank has seen a huge uptick in demand for digital asset services beyond the original class of crypto funds. More and more traditional financial institutions are looking for ways to both gain exposure to the asset class themselves, as well as provide crypto-native services to end consumers. It is our sense that no single phenomenon is driving demand, but a confluence of factors—improving infrastructure and crypto-native service providers, increased regulatory clarity, and a growing sense that crypto is becoming mainstream—is driving increased demand for crypto services across the board.

Questions Regarding Risk and Compliance Management

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?

As the first and only currently operating federally-chartered digital asset bank, we have a unique insight into exactly the kinds of controls required by the Office of the Comptroller of the Currency (OCC) to custody digital assets, as well as participate in crypto-native on-chain activities like governance and staking. While there is not exactly a 1:1 comparison between existing risk and compliance management frameworks designed to identify, measure, monitor, and control the risks associated with operating in the legacy financial markets and those associated with operating in the digital asset space, existing frameworks for operating a federally-chartered trust bank that can competently service digital assets are very much in the spirit of tested banking frameworks.

For instance, the OCC takes a holistic approach to assessing and managing banking risk, requiring the banks under its purview to maintain the "three lines of defense": a series of overlapping protocols, policies, and personnel intended to identify, measure, and mitigate a wide range of possible risks, both internal and external.

The first line of defense—the "operators"—includes all personnel responsible for the bank's everyday operations and its guiding controls. These individuals receive all appropriate training and certification to perform their roles and maintain a superior level of expertise in the operations of a digital asset bank.

Fully independent from the operators, the second line of defense, is a dedicated compliance and risk management team responsible for guiding the bank in terms of how it can best operate in a way that mitigates or entirely avoids a wide range of risk factors.

The third line of defense consists of an additional audit function that monitors the first two lines of defense (operators and compliance team). While this audit function may be either internal or external, it is critical for it to operate independently from the other two lines of defense, and report directly to the board overseeing the bank.

While perhaps slightly different in expression in a digital asset bank, these "three lines of defense" are typical of risk and compliance management in legacy banking. Taken together, they help to insulate the bank itself against mismanagement, a wide range of potential risks, and the kinds of single points of failure that can exist in their absence.[10]

To be clear, the above are a few examples of the ways IDIs can leverage largely existing risk frameworks to provide services for digital assets. Were an IDI to begin taking cryptoassets as true deposits, we are of the opinion that banks should then be subject to providing a similar kind of insurance as cash deposits, denominated in the asset being deposited. Put differently, if cash in a checking account is FDIC insured to no limit, and each IDI is responsible for putting a reasonable sum into insurance, the same policy should apply to banks taking deposits in Bitcoin, or Ethereum, or Stellar Lumens, or any number of other assets: if the bank is truly taking deposits and not holding assets under custody on behalf of clients, they should be subject to a similar insurance requirement, denominated in the asset deposited.

In terms of other use cases, some, like crypto-backed lending, have some corollary in the world of legacy finance and can similarly lean on existing risk and compliance management frameworks. Other, emerging use cases such as those that exist in decentralized finance may require an entirely new or materially different risk and compliance management framework.

---

[10] OCC, Comptroller's Handbook, Corporate and Risk Governance, pg 42; https://www.occ.treas.gov/publications-and-resources/publications/comptrollers-handbook/files/corporaterisk-governance/pub-ch-corporate-risk.pdf

ANCHORAGE DIGITAL

One Embarcadero Center #2623
San Francisco, CA 94126

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?

The custody and servicing of digital assets is, technologically speaking, wholly different from the custody and servicing of legacy financial instruments. We will address some of the most key differences among the asset classes as well as some of the necessary and unique controls and processes crypto requires in our response to question #12 below. For now, suffice it to say that the blockchain's immutable nature (the fact that transactions are permanent with no central authority to reverse transactions made in error), the fact of existing as a centralized service provider in a larger decentralized system, and the kind of asset volatility that comes with an industry still yet to reach maturity are among the key risks and challenges necessary to measure, monitor, and control for in each and every one of the various digital asset use cases cited in the FDIC's RFI.[11]

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

Despite the technical complexity of transacting in cryptocurrency and otherwise managing blockchain operations, the digital asset ecosystem brings along with it a number of clear and undeniable improvements to financial infrastructure. Consumers have already begun to see them for themselves, and IDIs are finding their own as they investigate support for digital assets in earnest.

First of all is the complete transparency of blockchain ledgers. While digital assets are often panned in the media as "anonymous," a more accurate description is "pseudonymous," whereby each and every transaction is recorded on a fully transparent distributed ledger. This kind of record-keeping in an already heavily rule-based system has real implications for curtailing financial crimes and preventing the misuse of financial institutions that have cast a shadow over certain periods of American financial history.

Also among the benefits is the global scale of decentralized networks, and the improved efficiency in terms of both transaction times and cost. Blockchain infrastructure has the potential to improve upon centralized settlement processes and procedures, as well as lower transfer costs for end users around the world. Utilizing stablecoins as part of settlement infrastructure also has the potential to eliminate the costly and time consuming step of converting between fiat currency and digital assets when transacting in digital assets, improving efficiency for participants in crypto markets.

7. How are IDIs integrating, or how would IDIs integrate operations related to digital assets with legacy banking systems?

[11] https://www.fdic.gov/news/press-releases/2021/pr21046a.pdf

While some IDIs will undoubtedly attempt to build their own bespoke tools for the secure custody and servicing of cryptoassets, the far more common method to date has been for legacy banks to offer their clients digital asset services by forming partnerships and/or sub-custody arrangements with crypto-native technology and financial services providers.

Legacy IDIs must be able to compete in what is a quickly evolving financial ecosystem. To continue to be seen as trusted financial partners, it is imperative that they offer all of the financial services that their clients demand, including services surrounding digital assets. These kinds of partnerships and sub-custody arrangements can and do take many forms, from direct API integrations with crypto technology platforms like Anchorage Digital, to partnerships whereby the seriously technical work of digital asset custody services are delegated to a regulated, qualified custodian like Anchorage Digital Bank and client financial reporting and other such services remain under the IDI, to full sub-custody arrangements.

8. Please identify any potential benefits, and any unique risks, of particular digital asset product offerings or services to IDI customers.

Beyond the benefits to IDIs outlined above—benefits that also largely transfer to end consumers—the fact of IDIs offering digital asset product offerings or services to IDI customers is a benefit in and of itself. In their early days, crypto markets operated in some of the lesser traversed corners of the Internet. While today, a number of digital asset exchanges and service providers have come to prominence for their ability to provide consumers with the exposure to crypto they demand, a non-trivial portion of the population will likely stay on the digital asset sidelines until they're able to participate in crypto markets through the banking providers they best understand—the ones they have grown accustomed to, and associate part and parcel with the totality of their financial lives. IDIs offering digital asset products and services to consumers is in effect a benefit itself, because it would allow consumers to access this emerging asset class through a clearly regulated bank.

In terms of risk, beyond the price volatility associated with any emerging market, digital assets carry a number of unique risks associated with what they are from a technological standpoint. Handling, custodying, and otherwise servicing digital assets takes a wholly different technical set to do securely and efficiently, meaning digital assets essentially come with a set of risks not shared with legacy financial instruments. We address the most notable risks as well as appropriate controls in our response to question #12.

9. How are IDIs integrating these new technologies into their existing cybersecurity functions?

Just as there are varied approaches to the custody and servicing of digital assets, the way that IDIs choose to integrate any number of a wide range of technologies associated with digital assets into their existing cybersecurity functions varies according to a number of factors, among them the use case the given IDI is attempting to facilitate, the value of the assets being

safeguarded, and so on. While we cannot speak exhaustively of the tactics being used by IDIs to integrate crypto services across the entire industry, we can speak to the trends that we see ourselves, as an organization that offers banking, infrastructure, and technology solutions for institutions operating in the digital asset space.

At Anchorage Digital, we have long seen the desire on behalf of IDIs to be able to offer digital asset services essentially through the same vehicle as their existing services, at or beyond the same level of security. There is a reason "bank-grade" is used to describe the strength of things like vaults, encryption, and even security more generally. The fact of the matter is that banks have long set the standard for what it means to hold something securely on someone else's behalf. That being the case, we have found IDIs and other banks to be extremely discerning in their decision-making when it comes to digital asset service providers.

Knowing full well the unique security risks associated with digital assets (see #12), IDIs and other banks are opting out of crypto solutions that rely on manual human operations to make transfers, that rely on physical redundancy of private keys, and that rely on largely theoretical mathematical solutions that have themselves resulted in the real-world, practical loss of client funds.

Instead, we see IDIs with a preference for digital asset services that meet or exceed their existing cybersecurity functions. We have seen a preference for tools with strong end-user authentication that doesn't rely on tools like email or SMS for two-factor authentication—tools that can be compromised to the effect of great loss. We have seen a preference for tools that forego the kind of weak authentication a password can give (proving only that a user possesses it) for the kind of strong authentication biometrics can provide (proving who a user is). And we have seen a preference for tools with a long track record of securing private key material. All of these suggest that IDIs, as they look to provide the kinds of digital asset services their clients demand, are treating the task of integrating a technology that is new to them with the due diligence long expected of banks.

In truth, on a macro level, some of the tools that form the foundation of the digital asset ecosystem—private key cryptography, zero knowledge proofs, and strong end-user authentication—stand the chance to vastly improve cybersecurity functions across the financial services industry. We will discuss some of the unique security considerations associated with operating in the digital asset space in our response to question #12.

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?

To the extent that IDIs are holding digital assets under custody and not on balance sheet, we believe that, from a supervisory perspective, there exist no unique aspects of digital asset

activities that the FDIC should take into account. In terms of unique aspects of digital asset activities more generally speaking, from a technical perspective, please see #12.

11. Are there any areas in which the FDIC should clarify or expand existing supervisory guidance to address digital asset activities?

Over the past few years, the digital asset space has benefited from improvements in regulatory clarity. With the OCC publishing a number of interpretive letters clarifying the role that banks are empowered to play in terms of providing digital asset services to consumers, providing banking services to legally operating digital asset businesses, and participating in decentralized networks, interest in the space itself among institutions in legacy banking and finance has only grown. Granting federal trust bank charters to digital asset banks like Anchorage Digital Bank has also had the effect of normalizing digital assets among more traditional financial institutions.

That all said, as with any nascent industry, there is still quite a bit to be desired in terms of regulatory clarity in the digital asset space. Banks want to provide the kind of digital asset services their clients demand, but they want to be sure that they're operating within both the spirit and the letter of existing regulatory frameworks. To the extent that those frameworks can be sharpened, expanded, and clarified to accommodate digital assets and their many use cases, there is certainly a role for the FDIC to play. As the stabilizing force it has been for the American banking system for decades, the FDIC could itself take something of a leadership role in ensuring the financial system remains stable with the addition of digital banking services by publishing a statement confirming the allowance of measured participation in the space by federally-regulated entities. To remain competitive in a quickly changing marketplace, banks need clear guidance around what services they can and cannot provide to end consumers, and what constitutes appropriate partners and controls.

12. In what ways, if any, does custody of digital assets differ from custody of traditional assets?

Digital asset custody and the custody of traditional assets are fundamentally different operations from a technological perspective. This means that an IDIs expertise in holding, securing, or servicing traditional financial instruments has little if any bearing on its ability to hold, secure, or service digital assets.

In practice, the most significant differentiators among digital assets and legacy financial instruments are 1) the blockchain's immutable nature and the irreversibility of transactions, as described above in our response to question #5, and 2) the bearer nature of the assets themselves, where control of private keys essentially equates to control of the associated assets.

These factors together set the bar for secure custody of digital assets much higher than traditional assets. In this light, we believe the following should be considered baseline

requirements for digital asset custody that is both secure and compliant with existing regulations. It is also worth noting that an IDI could reach this high bar by relying on a sub-custody partner who already satisfies the requirements for providing secure custody in the digital asset space.

Proof of exclusive control and existence

Securities Exchange Act of 1934 §15c3-3(d) ("the Customer Protection Rule") is intended to prevent the delay or inability to return an investor's securities in the event of untimely demise of a custody provider. Toward that end, the Customer Protection Rule requires custody providers to meet certain requirements, including the requirement "to maintain physical possession of or control over customers' fully paid and excess margin securities."[12] While not directly relevant to all IDIs, the rule itself is useful to illustrate both the challenges of digital asset custody, as well as the need for strong consumer protections in that realm.

Private keys are the foundation of the crypto economy. More than that, they are the core tools of cryptography that allow a user access to their digital assets. Essentially, they are software. And like any software, they can be easily copied. This means that it is possible, even likely, for private keys to exist in more than one instance and location. It follows that, even if a custodian can provide proof of holding *a* private key on behalf of an end consumer, they haven't necessarily proven control of *the* private key. In other words, proving control is not the same as proving exclusive control.

It is possible to prove exclusive control over private key material through a combination of software, hardware, and operational processes. That said, custody models that rely on maintaining multiple redundant physical or electronic copies of a private key as part of their security model cannot do so. What's more, the existence of multiple redundant copies of private keys in the hands of a custody provider significantly increases the risk of internal collusion and theft.

Beyond proof of exclusive control, another key difference in digital asset custody is the ability to prove, on a regular basis or as requested by auditors or regulators, that assets held under custody exist. In short, the ability to prove control of private keys, even exclusive control, doesn't much matter if a custody provider can't also prove the existence of the associated assets. The ability to do so is essential, both for consumer protection and to comply with existing requirements related to qualified custody.[13]

Hardware security modules

---

[12] https://www.sec.gov/divisions/enforce/customer-protection-rule-initiative.shtml

[13] Additionally, in a January 18, 2018 Staff letter, the SEC Staff designated the need to validate "existence, exclusive ownership and software functionality of private cryptocurrency keys and other ownership records" as core assessment requirements for registered funds using third party custody providers. The letter is available at https://www.sec.gov/divisions/investment/noaction/2018/cryptocurrency-011818.htm

We are of the opinion that both exclusive control and existence proofing assets on a regular and event-based cadence are best achieved through the use of single-purpose hardware security modules (HSMs) for both key generation and storage. When air-gapped and kept physically separate from public network connectivity, HSMs exceed the security of so-called “cold storage,” because, on top of storing private keys offline, relying on HSMs foregoes private key sharding or any of the kinds of manual human operations that most forms of cold storage rely on—and in so doing eliminates a wide range of operations that can increase the risk of theft, human error, or other compromise that can result in loss.

HSMs are able to both generate and store private key material without that material ever leaving the module itself, thus proving exclusive control. In terms of proving existence, HSM-based architecture allows for easy and nearly instant challenge-response authentication, which is not true of custodial solutions reliant upon private key redundancy in the name of security. What’s more, both clients and third party auditors can easily audit HSMs. We ourselves have had Bishop Fox audit our security claims, Ernst & Young audit our ability to meet stated control objectives, and have helped clients provide similar documentation to their own external auditors.

More than facilitate proof of exclusive control and asset existence, HSMs have the benefit of being long-known, battle-tested technology with existing government standards for private key security. The National Institute of Standards and Technology maintains the Federal Information Processing Standards (FIPS), standards and guidelines approved by the Secretary of Commerce, developed for use by the Federal Government. HSMs rated FIPS 140-2 meet the exacting requirements needed to secure private keys. We feel it is imperative for custody providers in the digital asset space to meet or exceed the standards long-set for private key security. Doing so is in the best interest of consumer protection—and, in turn, trust in the larger financial system.

Blockchain monitoring

Today there exist thousands of digital assets, with new ones being developed almost daily, all at different levels of security and soundness. As such, it falls to providers of custody to assess the various blockchains they aim to support. The unique security concerns inherent to the operation of the digital asset space mean that any vulnerability at the protocol level runs the risk of being exploited, and the worst of exploits occur at scale. Given the risks, if a financial institution wishes to custody assets at a level required for sound operation of digital asset markets, we believe they should be required to proactively monitor the blockchains they aim to participate in, and implement clear policies for completing such monitoring at regular intervals.

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?

As FDIC's Part 362 application procedures surround permission "to engage in activities impermissible for a national bank,"[14] we are of the opinion that it is not applicable to federally-chartered trust banks' participation in digital assets. The OCC has made it abundantly clear that banks are fundamentally allowed to participate in the digital asset space. Not only are banks allowed to participate under current guidance, but they must be allowed to participate in financial activities involving digital assets if they are to remain competitive in a fast-evolving marketplace. Ultimately, we believe it is in the best interest of consumer trust in the broader financial system for IDIs, banks, and other regulated financial institutions to participate in the digital asset space with the proper controls in place.

Questions Regarding Deposit Insurance and Resolution

14. Are there any steps the FDIC should consider to ensure customers can distinguish between uninsured digital asset products on the one hand, and insured deposits on the other?

To the extent that digital assets are held under custody, not on balance sheet, the FDIC should follow the same approach that it would in terms of informing customers of the risks of participating in any emerging asset class. More specifically, banks facilitating client participation in digital assets should be required to develop explicit, clear disclosures around the risks of participating in digital assets, including the risk of total loss.

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?

Generally speaking, the analogy 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 sounds reasonable on its face. That said, and the technological differences laid out above in our response to question #12 aside, this area is still very much developing. As it continues to evolve, this area deserves attention and additional exploration.

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?

Without knowing the full scale of the resolution process or receivership, it's not possible to present an exhaustive list of the complexities the FDIC may encounter. Suffice it to say that the valuing, transferring, marketing, operating, and resolving digital asset activity is essentially different in nature than those activities that are considered in the realm of legacy banking. There

[14] https://www.fdic.gov/regulations/applications/resources/part362.html

are literally thousands of digital assets and possible digital asset use cases in an ecosystem that grows almost daily, and complexity increases with the number and variety of assets and use cases a given IDI supports.

In the event that the FDIC were to encounter any of the digital asset use cases set forth in its RFI in the resolution process or in a receivership capacity, the most secure, effective, compliant, and efficient course of action to ensure the orderly wind down of a banking institution and return of assets to consumers would be to engage a federally-regulated qualified custodian with expertise in all aspects of of the digital asset lifecycle. Taking this approach would match the FDIC's unrivaled expertise in resolution and receivership in the broader world of banking with the specific, technical expertise required to handle digital assets in a way that is secure and compliant.

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 President Roosevelt's speech to the American people on the temporary closure of all banks, he made a particularly salient observation—one that still rings true today:

> "After all there is an element in the readjustment of our financial system more important than currency, more important than gold, and that is the confidence of the people. Confidence and courage are the essentials of success in carrying out our plan. You people must have faith; you must not be stampeded by rumors or guesses. Let us unite in banishing fear. We have provided the machinery to restore our financial system; it is up to you to support and make it work. It is your problem no less than it is mine. Together we cannot fail."[15]

We are confident that, with the proper controls, the proper foresight, and the proper technological approach, the American people can participate in the new, emerging asset classes they wish to, while maintaining confidence in the stability of the broader financial system.

[15] https://www.fdic.gov/about/history/3-12-33transcript.html

ANCHORAGE DIGITAL

One Embarcadero Center #2623
San Francisco, CA 94126

Very truly yours,

[redacted]

Nathan McCauley
Co-founder and CEO
Anchorage Digital

[redacted]

Georgia Quinn
General Counsel
Anchorage Digital