accenture

Response to FDIC Digital Asset Information Request

Accenture Federal Services
Financial Services Sector (FSS)
July 16, 2021

Contents

Introduction

Accenture Federal Services (AFS) is submitting this document in response to the Federal Deposit Insurance Corporation's (FDIC) Request for Information (RFI) and Comment on Digital Assets (RIN 3064-ZA25) regarding insured depository institutions (IDIs) current and potential activities related to digital assets. We are responding to the following question numbers from the RFI: 4, 5, 8, 10, 11, 12, 13, 14, 15 and 17.

Digital asset innovation has created new markets and is disrupting the financial services industry. Some of the key issues financial regulators are facing with the digital asset industry in the United States:

- Lack of transparency
- Threat of market manipulation
- Complexity of underlying technologies
- Rapid pace of industry development

Assisting our financial regulatory clients in responding to these and other challenges they face in the digital asset industry is critical to establishing the United States as a global leader in this growing sector of finance.

AFS approaches digital assets as an opportunity for a more efficient, resilient, transparent, and inclusive financial system. Regulators, such as the FDIC, have the opportunity to enable these benefits by providing clear guidance and rules for entrepreneurs and companies to deliver value through new digital asset products and services.

The opportunity presented by digital asset innovation must be balanced with the proper amount of education, consumer protection, anti-money laundering (AML/BSA), supervision, and monitoring activities. Regulators have the responsibility to produce reasonable frameworks which mitigate bad actors from using digital assets and underlying technologies for nefarious purposes.

Our response is informed by the primary experience areas AFS has with other U.S. Federal financial regulators and agencies. This experience spans across digital asset related IT infrastructure, blockchain data analytics, and advisory services.[1]

Our current view of the digital asset industry, illustrated in Figure 1, is divided into two main areas: assets/infrastructure and supporting services. With the rapid evolution of the industry and its impact to financial services, it is important for FDIC to maintain a holistic awareness of the digital asset industry.

> ***"If they [stablecoins] are going to be a significant part of the payments universe…then we need an appropriate regulatory framework, which frankly we don't have."***
>
> **– Federal Reserve Chair Jerome Powell**

Federal Reserve Chair Jerome Powell recently told the House Financial Services Committee, *"We have a pretty strong regulatory framework around bank deposits, for example, or money market funds. That doesn't exist really for stablecoins…. If [stablecoins] are going to be a significant part of the payments universe -- which we don't think crypto assets will be but stable coins might be -- then we need an appropriate regulatory framework, which frankly we don't have."*[2] **The areas that we recommend FDIC's elevated focus are around stablecoins and CBDC due to their use cases and close relationship to deposits.**

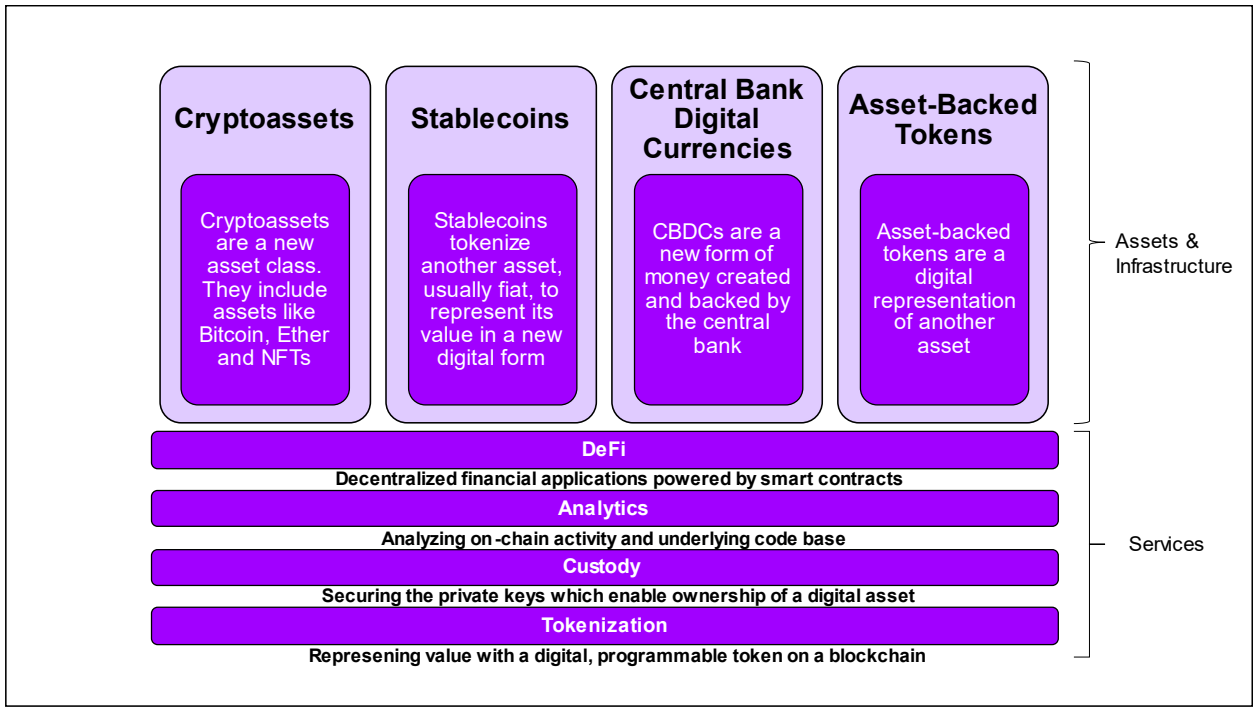

Figure 1 – Current State Overview of Digital Assets

[1] https://www.accenture.com/us-en/insights/us-federal-government/future-digital-currency

[2] https://www.bloomberg.com/news/articles/2021-07-14/powell-says-stable-coins-need-regulation-to-protect-u-s-public

Responses to Questions

In response to FDIC's request about IDIs current and potential activities related to digital assets, we have structured feedback around the areas of Risk and Compliance Management; Supervision and Activities; Deposit Insurance and Resolution; and Additional Considerations. Our feedback includes recommendations for FDIC's consideration featured throughout our response as call out boxes on the right-hand side of the page.

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?

Certain digital asset use cases could require new or materially different risk and compliance frameworks. Different digital asset use cases will require different underlying blockchains or DLT technologies. Different blockchain and DLT systems have different underlying design patterns, standards and interfaces, make tradeoffs to optimize for certain use cases, and have different environmental, social and governance (ESG) profiles. It is possible that IDIs could adopt current risk and compliance (i.e., AML/BSA) standards, then add new standards for operational, technological and other nuanced risk considerations specific to digital assets.

Use cases which include the use of permissionless blockchain networks (i.e., Bitcoin, Ethereum) require frameworks for the operational and technological risks of a global, open source network, which is maintained by distributed developers and secured by distributed miners/validators. Because these network's actors are not all known, IDIs should prioritize fraud mitigation in their risk frameworks. Appropriate cybersecurity is required for the custody of private keys, which enable ownership of assets on these permissionless networks. Depending on the design and deployment patterns of assets, if the private keys of certain assets are compromised or lost, then these assets could be stolen or rendered permanently inaccessible. Furthermore, risks around enterprise data security, including information leakage linking customers and their assets, should be included in risk and compliance management frameworks.

Use cases, which include permissioned blockchain and DLT networks, require appropriate cybersecurity controls at both the private key custody level and the underlying node environment. Because permissioned networks assume that all actors participating in a network are known and approved by other members, a heavy trust reliance is made on identity and membership service providers that could result in external provider risks. Fundamentally, these permissioned networks tend to have different risk profiles than permissionless networks, therefore, regulatory frameworks should be designed with these differences in mind.

Permissionless	Permissioned
• Anyone can have access to the underlying data and transaction history. • All participants in the network are treated as equal, meaning that all users have equal rights to read data and execute transactions. • They are frictionless for anyone to transact on and provide everyone the ability to access a complete copy of the transaction history (ledger).	• One or more organizations control who can have access to the underlying data and transaction history. • User identities are authenticated and known through some type of procedure (e.g. KYC/AML). • Different levels of read and write access can be assigned to participants for various types of data in the distributed ledger. This enables greater control and privacy than permissionless blockchains.

Figure 2 – Permissionless vs Permissioned Blockchain Comparison Tables

It should be of note that permissionless and permissioned networks are not necessarily mutually exclusive and that design patterns could follow a hybrid approach in which certain activities are conducted on a permissionless network and others on a permissioned network.

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?

IDI's participation in blockchain and/or DLT networks will give rise to new risks and challenges.

Depending on what type of blockchain and/or DLT network IDI's are participating in, different technologies and processes will be required to address the unique risks including node infrastructure, software maintenance, security and custody. FDIC should examine the different types of blockchain and DLT networks being used in the market and what people, processes and technology might be required for addressing unique risks of each network.

FDIC should examine the different types of blockchain and DLT networks being used in the market and what people, processes and technology might be required for addressing unique risks of each network.

Blockchains and other DLT systems produce transactional data in a new format which must be collected and analyzed in an appropriate manner. Furthermore, this transactional data might be challenging to trace through and analyze depending on how the network is designed. IDIs should be developing the necessary IT infrastructure, data pipelines and/or node infrastructure for the respective blockchain and/or DLT networks they participate in or interact with.

Many digital asset use cases involve the use of smart contracts. Smart contracts are a new technology which enables the programmability of assets and the development of decentralized applications (DApps) on blockchain networks. IDI's should have a clear methodology for identifying, understanding, measuring, and monitoring smart contract risks such as contagion and composability.

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

We focus on the potential benefits and risks of permissionless blockchain-based stablecoin related product offering and services:

Benefit	Explanation
Increasing financial inclusion	Can be transferred to anyone at any time with an internet connection and digital wallet.
Reducing costs	Can be sent for minimal costs (depending on gas costs of particular network), no matter the amount being sent.
Increasing transparency	Transactions are publicly auditable and traceable.
Increasing resiliency	Run on multiple blockchain networks simultaneously.
Increasing transaction speed	Transactions can be sent, verified by the network and settled within minutes.
Increasing financial participation	Enable users to transact, send value and participate in digital financial services.
Increasing consumer options	Provide new payment rails with additional functionality with smart contracts.
Strengthening law enforcement	Can be programed to freeze and blacklist addresses in the case of law enforcement request.

Figure 3 – Potential Stablecoin Benefits

Risk	Explanation
Blockchain technology	Stablecoins are enabled by blockchains which are still a new and evolving technology. Customers need to understand complex risks around private key infrastructure, digital wallets and irreversible transactions.
Smart contracts	Stablecoins leverage smart contracts to create programable tokens on blockchain networks. Customers to understand complex smart contract risks such as exploits and upgrades.
Contagion	Smart contracts are composable, in that one smart contract might interact with many other smart contracts to build a decentralized application (DApp). Smart contract bugs or exploits could result in a contagion risk.
Funds governance	Underlying collateral management is not always transparent or subject to regulatory standards. Lack of transparency could result in lack of confidence and instability.

Figure 4 – Potential Stablecoin Risks

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?

Market structure of digital assets is significantly different than traditional financial systems. The same asset may trade in multiple venues in multiple jurisdictions with various regulatory standards, as well as being transacted peer to peer or peer to smart contract. This decentralization of market activities could require new supervisory processes and technologies. FDIC should examine the various options for supervision, such as traditional KYC and on-chain monitoring (blockchain analytics).

> ***FDIC should take into account the various options for supervision, such as traditional KYC and on-chain monitoring (blockchain analytics).***

On-chain monitoring involves the analysis of transactional data produced by entities using blockchain and/or DLT networks and smart contracts executing applications. Different blockchain and DLT networks may produce vastly different data types depending on network design. For any off-chain transactions, FDIC cannot rely on blockchain analytics and must work with the centralized IDI entity to understand how funds are handled internally.

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

Stablecoins – FDIC should consider the following steps:

- Examine the different models of stablecoins which are being issued by private entities
- Define how these stablecoins are used in the market across various use cases
- Clarify guidance related to identified stablecoins being used by IDIs (or other entities providing stablecoin products/services) if appropriate
- Potentially expand existing supervisory guidance to address these stablecoin activities if appropriate

DeFi – FDIC should consider the following steps:

- Examine DeFi as a potential new backend infrastructure for IDIs
- Engage IDIs to gauge interest in using DeFi products/services
- Potentially clarify or expand supervisory guidance to address IDIs use of DeFi if appropriate

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

Custody of digital assets focuses on the security of private keys which determine who owns the ability to interact with a digital asset residing at a certain address or wallet containing multiple addresses. Digital asset custodians must be considerate of the theft, destruction and unauthorize use risks of private keys. Multiple custody models exist for enabling asset owners to interact with their digital assets in a custodial setting.

Custody solutions are available on a range of security levels and models depending on the requirements of the use case. This spectrum of custody solution ranges from "hot wallets", which are directly connected to the internet and ready to execute transactions, to "cold wallets", which are not connected to the internet and could require significant time and approval processes to execute a transaction. FDIC should examine the recommended best practices of custodial risk management frameworks for the different models of custody under different use cases.

> ***FDIC should examine the recommended best practices of custodial risk management frameworks for the different models of custody under different use cases.***

Each blockchain network has its own native wallet infrastructure in which private keys are held. Custody providers should maintain the appropriate node and network participation infrastructure for each blockchain network they support. FDIC should investigate how digital asset custodians segregate individual account funds across different blockchain networks.

> ***FDIC should investigate how digital asset custodians segregate individual account funds across different blockchain networks.***

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 3 See 12 C.F.R. Part 362, subpart A. 7 uncertainty surrounding the permissibility of particular types of digital asset-related activity, in order to support IDIs considering or engaging in such activities?

Participating in blockchain networks could (depending on which blockchain network and what type of participation) result in an IDI receiving the native cryptoasset of a network. FDIC should harmonize with OCC guidance to provide more clarity and certainty for IDIs to participate in blockchain networks.

> ***FDIC should harmonize with OCC guidance to provide more clarity and certainty for IDIs to participate in blockchain networks.***

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?

Digital asset products complexity and marketing could make it difficult for customers to clearly distinguish between uninsured products and insured deposits. There are multiple methods which could be used to help customers distinguish between the different types of products and insured deposits; directly on-chain and off-chain via financial institution disclosures, account structuring or other tagging mechanisms. FDIC should consider the different methods for financial institutions to help customers distinguish between traditional assets and digital assets.

> ***FDIC should consider the different methods for financial institutions to help customers distinguish between traditional assets and digital assets.***

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?

Certain fiat-backed stablecoins might have similarities to stored value products in that one can purchase stablecoins, hold them without market fluctuation in a digital wallet and transact with them for different products/services. Because there are various models for fiat-backed stablecoins, the FDIC should examine these different fiat-backed stablecoin models and potentially produce guidance regarding underlying collateral transparency, usage and proof of reserves.

> ***FDIC should examine these different fiat-backed stablecoin models and potentially produce guidance regarding underlying collateral transparency, usage and proof of reserves.***

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.

FDIC should consider empowering and elevating the FDiTech team to coordinate FDIC's oversight and response to digital asset activities. Other U.S financial regulators such as the SEC, with FinHub, and CFTC, with LabCFTC, have empowered and elevated their Fintech entities within their agencies. Furthermore, we recommend a specific focus of the FDIC to the sector of stablecoins and CBDC due to their rapid development, use cases and close relationship with deposits.

FDIC should consider empowering and elevating the FDiTech team to coordinate FDIC's oversight and response to digital asset activities.