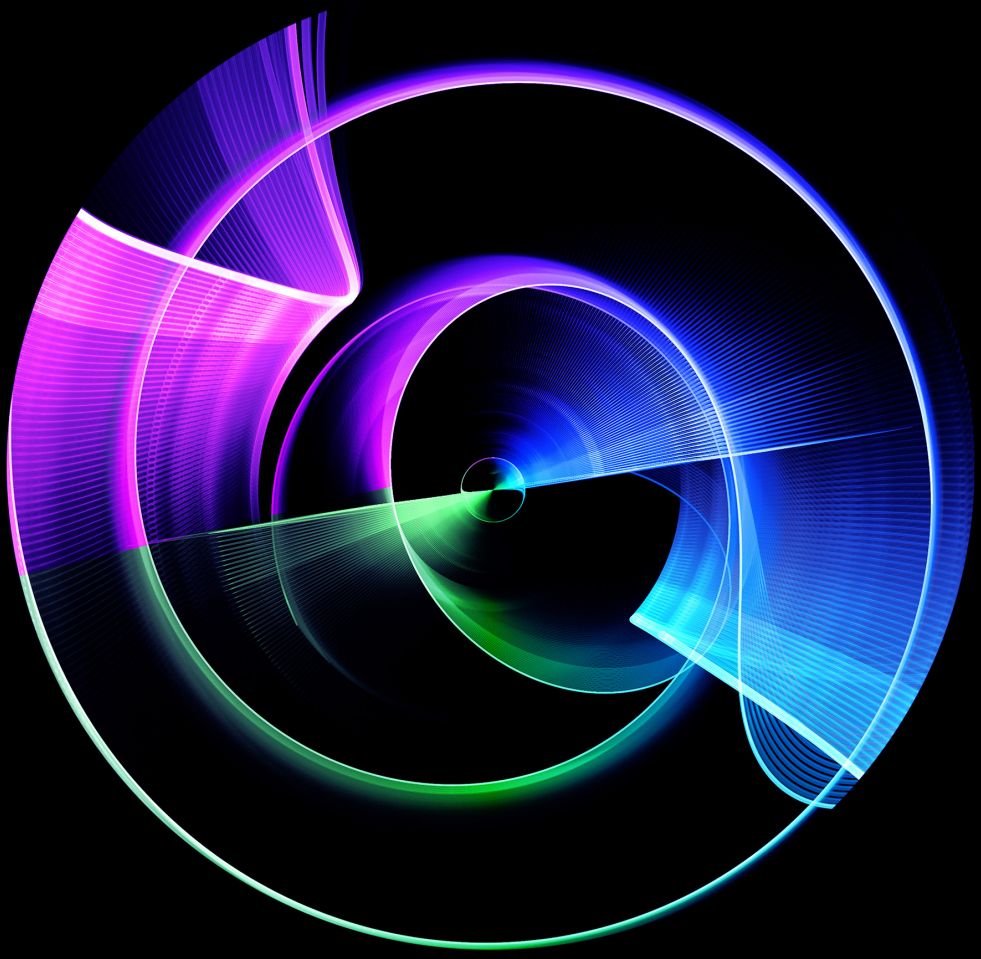
Deloitte.



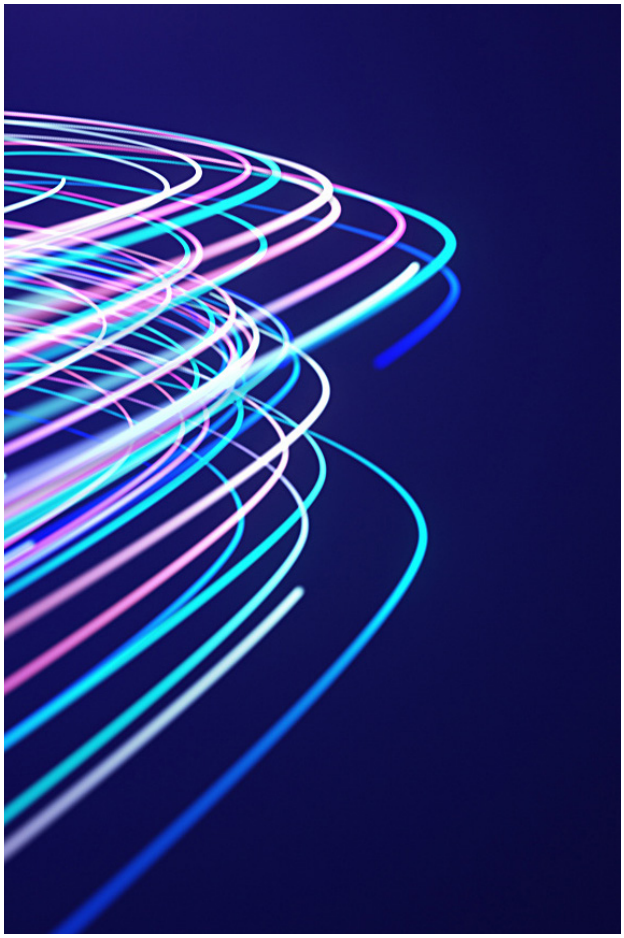
Market Integrity Considerations for Digital Assets

December 2021

MAKING AN IMPACT THAT MATTERS since 1845

"[Digital assets are] rife with fraud, scams and abuses in certain applications. There's a great deal of hype and spin about how crypto assets work. In many cases, investors aren't able to get rigorous, balanced, and complete information."

—Gary Gensler, Chairman of the US Securities and Exchange Commission[1]



The institutional and retail demand for cryptocurrencies continues to grow in parallel with their overall market capitalization and tightening regulatory landscape. Yet, the markets are considered susceptible to manipulation and market participants are uncomfortable with the potential of being exploited. This growing trend was highlighted in the recent meme coin "rug pull" scandal[2,3] which dominated market headlines in early November 2021. Within a week of its introduction, the meme coin soared more than 310,000% in value, hitting an all-time high of $2,861. Twenty-four hours later, the meme coin crashed 99.99% to $.001 leaving investors empty handed, as they were unable to sell their tokens due to an anti-dumping mechanism imposed by the developers. Per reports, the developers absconded with an estimated $3.3 million and erased all traces of the meme coin's existence from social media platforms.

Following this high-profile incident, Securities Exchange Commission (SEC) Chair, Gary Gensler, provided prepared remarks at the Securities Enforcement Forum[4] on November 4, 2021, stressing the importance of stamping out fraud, manipulation, and abuse to instill investors' trust in the digital asset marketplace.

As discussed in our previous articles[5,6], the broad and widespread access and availability of digital asset platforms across the globe and unique operational characteristics, coupled with patchy regulatory guidance, renders the space highly susceptible to investor abuse. This article will focus primarily on market manipulation risks witnessed within the digital asset marketplace, and regulatory and control considerations specific to digital assets that organizations can deploy to effectively manage market conduct risk.

What are key significant manipulative behaviors recently observed in the digital asset marketplace?

Dissemination of false or misleading market information is one of the most prevalent manipulative behaviors in "traditional markets" that has also garnered regulatory attention within the digital asset space. For instance, the SEC penalized a financial technology company for making false and misleading statements related to an unregistered offer and sale of digital asset securities[7]. According to the SEC's order, the company raised more than $16 million after distributing misleading marketing information to investors.

Further demonstrating the applicability of traditional market abuse behaviors in the digital asset marketplace, regulators have already identified instances of ***pump and dump*** manipulative schemes. On March 5, 2021, the CFTC imposed the first *pump and dump*[8] enforcement action related to digital assets, by charging two individuals with multi-million-dollar fines. In this instance, the two individuals secretly accumulated positions in multiple digital coins and deceptively promoted the coins through various social media outlets as valuable long-term investments. They then sold their holdings as prices surged, resulting in profits in excess of $2 million. This case is still pending results, with regulators seeking disgorgement, civil monetary penalties, permanent trading and registration bans, and a permanent injunction.

Insider trading is another well-known traditional market abuse scheme that has always been a major area of concern for regulators. Per a recent news report[9], US regulators are looking into a cryptocurrency exchange company for a potential *insider trading* instance, following allegations that the crypto exchange exploited its access to customer order data on millions of transactions.

With regulators taking measures to preserve market integrity and protect market participants, it is critical to identify and understand the novel risks and manipulative practices emerging out of the digital asset landscape.

A newly identified and well-publicized behavior is the ***rug pull***, which was discussed through the meme coin example[2,3] referenced earlier in this article. A *rug pull* maneuver is where developers tend to pull the plug on a hyped-up digital asset project and then flee with money they accumulated from investors. As of July 2021[10], *rug pull* related incidents have contributed to losses of $113 million in the decentralized finance (DeFi) sector.

Another example of an emerging manipulative practice is ***stop hunting***, which involves potential market movers, popularly known as crypto whales, that hold large amounts of a particular cryptocurrency. Here, crypto whales artificially infuse liquidity by dumping large volumes of their holdings, driving down the price of the coins. This creates a sizeable supply of sellers due to the triggering of stop-loss orders, which further drives the price downward. This allows crypto whales to strengthen their position in the asset through low-priced repurchases. While this behavior has been observed in the foreign exchange market in the past, *stop hunting* is becoming a more lucrative scheme in the digital asset marketspace.

How are regulators addressing market integrity concerns in this space?

The examples highlighted in this article emphasize the need to safeguard market integrity in the rapidly evolving digital asset ecosystem. Various regulatory bodies across the globe are taking notice and stepping up their focus on shaping the regulatory environment.

The European Union (EU) is in the process of negotiating the regulation on Markets in Crypto Assets (MiCA)[11], which extends the regulatory perimeter into crypto assets. The proposed regulation sets out a comprehensive framework covering issuance, trading, financial stability and market integrity. As per the regulation, authorized crypto service providers are required to comply with general and specific requirements related to consumer protection and market integrity, organizational requirements around ownership, cybersecurity, monitoring of market abuse, safeguarding of crypto-assets, and the operation of trading platforms.

Similarly, in the US, regulators have started to recalibrate and develop guidance around proper governance of risks introduced by digital assets and its market participants. For instance, the Digital Asset Market Structure and Investor Protection Act[6,12], introduced in July 2021, aims to provide legal and regulatory clarity on digital assets along with fundamental investor protection.

In addition to developing regulatory frameworks to control digital asset markets, regulators are actively involved in enforcing regulatory guidelines. The US SEC Chair, Gary Gensler, has stated that enforcement is one of the fundamental pillars in achieving the SEC's mission[4] and it will continue to pursue misconduct wherever they find it, including crypto assets. On similar lines, Rostin Behnam, the acting head of the CFTC, recently announced his intentions to aggressively police the cryptocurrency markets. Furthermore, on November 12, 2021, the SEC has once again voiced its doubts over exchange-traded funds (ETFs) in digital assets by rejecting the VanEck proposed bitcoin ETF, stating its concerns around investor protection and lack of manipulation prevention in the market[13].

While regulators are in the process of addressing the fragmented regulatory landscape, there is also an argument for the industry to focus on building capabilities in order to effectively manage risks related to digital assets.

What can firms do to prevent and detect market abuse for digital assets?

Today, firms are required to have robust internal risk and control frameworks in place for traditional financial assets and their associated market abuse risks, which is supplemented by the regulatory surveillance. However, as it relates to digital assets, a key challenge is the lack of adequate market infrastructure and technology providers to enable digital-asset trading with the same efficiency, reliability, and speed as they do for traditional asset classes such as equities, options, and fixed income. Registrants that have requirements for risk assessment and mitigation (e.g., swap dealers) must apply those requirements to cryptocurrencies as well. Additionally, the National Futures Association (NFA)[14] has separate requirements for all its registrants with regards to the treatment of cryptocurrencies.

As more firms are exploring avenues to provide digital asset exposure to their institutional and retail clients, they will need to develop a strong understanding of the emerging risks that come with entering this space. Once this has been established, firms should be able to make the appropriate adjustments and enhancements to their surveillance mechanisms. Absence of a surveillance framework can increase exposure to market manipulation, eventually eroding faith in the market.

Specific underlying characteristics of digital assets create additional factors for firms to consider when looking to update their risk and control frameworks, specifically while supervising and surveilling transactions in this space. To first gain access to these markets, firms will need to define their product/service strategy and determine the risks associated with the offerings. It is important to note that the digital asset offerings require firms to access new venues that many of them have had little to no experience in and would require expanding current third party risk management frameworks to conduct due diligence of third-party digital asset exchanges and service provider. This entails implementing a strong venue onboarding process to be able to obtain transaction data, implement cross-market surveillance, and ensure that jurisdictional regulatory requirements are met, among other activities.

Secondly, by engaging in markets that are 24/7/365, firms will need to have continuous, around the clock monitoring and surveillance

Figure 1: Key Factors for Establishing a Digital Asset Surveillance Framework

capabilities. Lastly, firms will need to enhance their anti-money laundering (AML)/know your customer (KYC) procedures to identify the holders of these assets and how funds are being transferred across the digital asset ecosystem. To account for some of the risks noted above, Figure 1 highlights considerations for firms when looking to make enhancements to their risk and control frameworks.

How can customer protection be compromised in digital asset investments?

Market manipulation in digital assets is a big concern when it comes to ***investor protection***, and this concern is further aggravated by the lack of fully vetted suitability and disclosure practices tailored to the needs of digital assets. Given the lack of maturity in this marketplace, many customers—including institutional counterparties—may not have adequate knowledge on the risks associated with investment in these new assets.

Investing in digital asset products does increase the risk for customers to add products to their portfolio that do not align with their financial objectives. This is referred to as *suitability risk* and can be due to several factors including a lack of uniformity in the definition of digital assets across regulatory bodies and the industry as a whole, and inappropriate or inaccurate disclosures provided by issuers of the crypto assets themselves.

Last year, the CFTC charged three individuals and three companies for creating fraudulent marketing materials that promised astronomical profits with no risk of loss. These materials were used to encourage tens of millions of customers and prospective customers to open and fund-off exchange binary options and digital asset trading accounts, resulting in payments of $20 million as commissions[15].

What does customer protection for digital assets look like from a regulatory lens?

Regulators globally have started to opine on a legal framework to ensure protection for customers and counterparties exposed to digital assets. As highlighted in Deloitte's Digital Assets Regulatory Digest[6], regulators will likely expect market participants to focus on attaining increased transparency and taking adequate measures to protect consumers, including appropriate disclosures of digital assets traded or issued, protections to compensate investors, and safeguarding of ownership rights. Currently, there exists an ambiguity with the applicability of existing regulatory frameworks for the digital asset space. Firms should look to existing guidance for suitability and disclosures and do their best to apply it to digital asset products.

In the EU, MiCA[11] expects firms to assess the compatibility of crypto assets with investor needs as well as mitigate the risks of misleading investors through inappropriate disclosures. To address this, MiCA has shared initial guidance requiring crypto issuers to publish a whitepaper on their website ahead of crypto issuances, providing detailed information on the characteristics of the issuance.

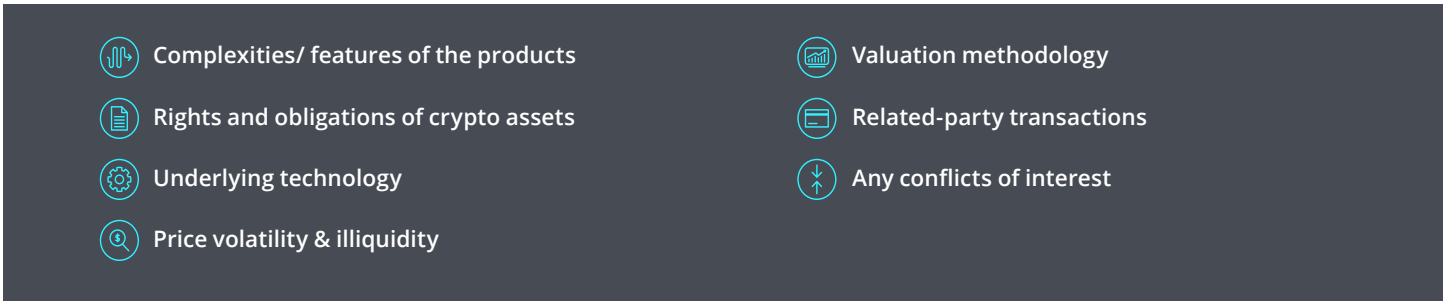
Likewise, in the US, the SEC Division of Examinations issued a risk alert[16] in February 2021 on digital asset securities. The alert emphasized the need to update solicitation documents, marketing materials, regulatory brochures and supplements, and fund documents to take into consideration the specific risks associated with new digital assets issuance. Further, CFTC has issued primers[17] to provide investors with information on emerging concepts in digital assets. NFA has also provided guidance on disclosure requirements for its members that engage in virtual currency activities[14].

It is worth noting that regulators in the US and the UK have shared guidance listing key disclosure topics to be covered by firms (Figure 2), and provide prospective buyers of digital asset products with ample information to help them make informed investment decisions.

What can firms do to protect customers' interest?

While the industry waits for more targeted direction from regulators, firms need to continue to abide by their fiduciary duties and prioritize customer best interest when recommending digital asset investments.

Figure 2: Disclosure Requirements



Additionally, firms can leverage their existing "traditional products" leading practices[18] and tailor them for their digital asset offering, specifically paying attention to three key factors:

Training:

Adequately training employees, particularly in business and internal risk and control functions, on the characteristics of digital asset products and associated risks to promote sound judgment of product suitability for different customer categories.

Accurate disclosures:

Communicating material facts and risks associated with digital assets to ensure enhanced transparency and comply with regulatory expectations, as discussed in the previous section.

Suitability due diligence:

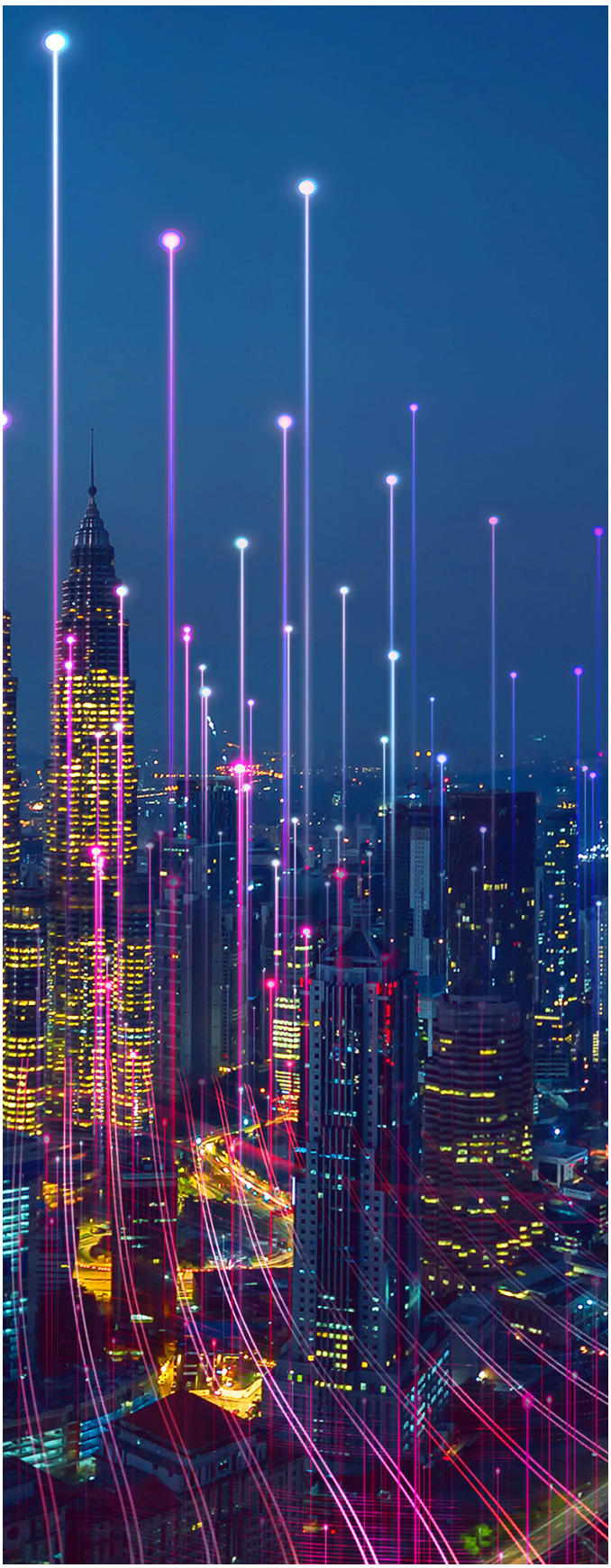
Leveraging suitability due diligence and KYC processes currently in place to adapt to digital asset products by performing ***Know Your Customer (KYC)*** and ***Know Your Product (KYP)*** assessments for classifying customers and products. For instance, existing swap dealer suitability and KYC requirements can be adopted by digital assets investment advisors.

Overall, firms should enhance their existing supervisory frameworks by integrating digital assets related processes, guidance, and controls to enable monitoring of suitability related red flags.

Planning ahead

Rapid growth of digital assets and its adoption across financial markets is paving the way for market evolution and maturity. Most organizations are proactively assessing their existing "traditional asset-focused" monitoring, supervision, and surveillance frameworks to explore opportunities for adoption and integration with digital asset product and service offerings.

On November 23, 2021, the Federal Reserve Board of Governors (FRB), Office of the Comptroller of the Current (OCC) and Federal Deposit Insurance Corporation (FDIC) issued a joint statement on their Crypto-Asset Policy Sprint Initiative and Next Steps[19]. Later that day, the OCC provided an independent statement[20], furthering their stance in previously issued interpretive letters, that banks need to perform certain activities before legally engaging in cryptocurrency-related activities. These letters, which were largely around custody services and stablecoin issuance activities, stated that banks should be able to demonstrate, to the satisfaction of its supervisory office, that they have controls in place to conduct the activities in a safe and sound manner and must receive prior permission from their supervisory officer.



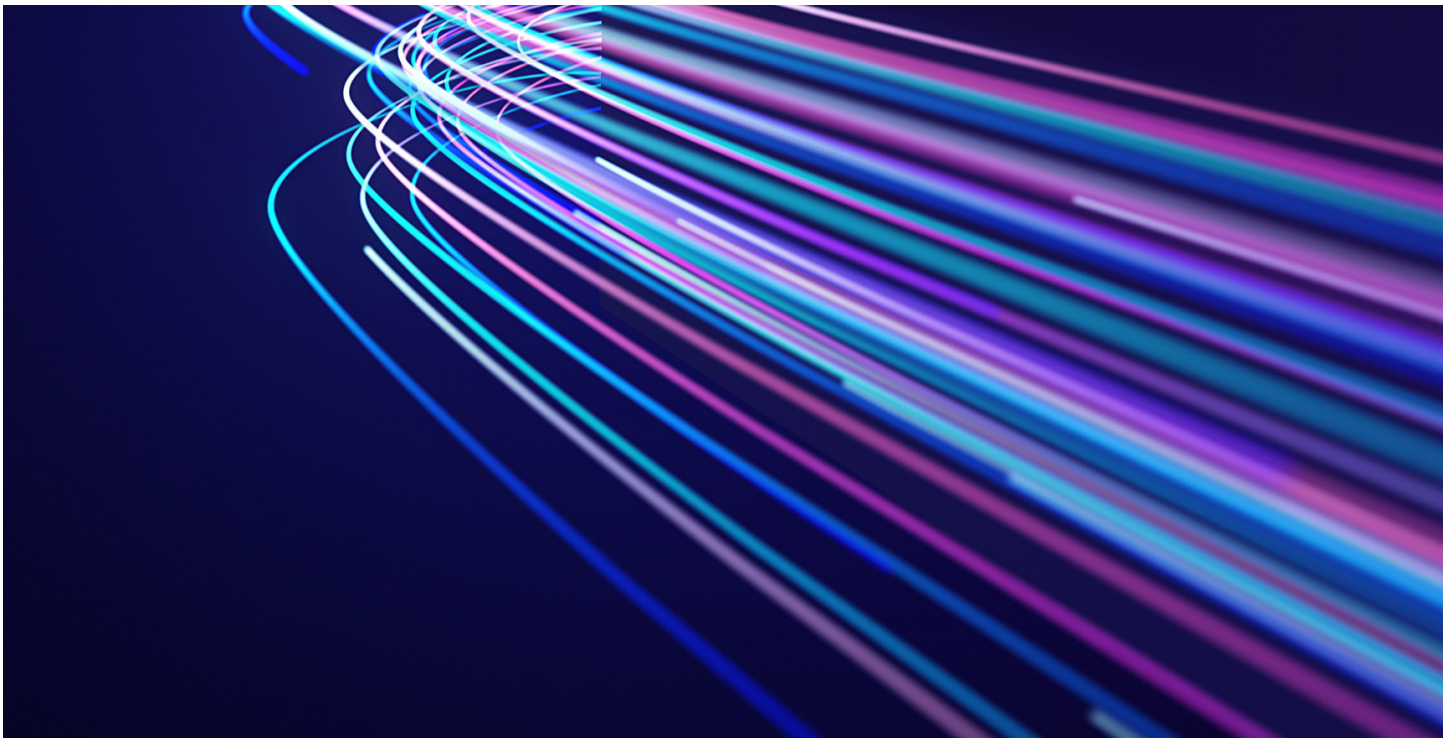
The joint statement indicated that the agencies plan to provide greater clarity on whether sales and trading-related activities related to crypto assets conducted by banking organizations are legally permissible and expectations for safety and soundness, consumer protection, and compliance with existing laws and regulations related to (i) crypto-asset safekeeping and traditional custody services; (ii) ancillary custody services; (iii) facilitation of customer purchases and sales of crypto-assets; (iv) loans collateralized by crypto-assets; (v) issuance and distribution of stablecoins; and (vi) activities involving the holding of crypto-assets on the balance sheet.

The key point for both releases is that financial institutions will need agreement on the permissibility of these assets within the current regulatory framework and the ability to demonstrate that they have established an appropriate governance, risk management and control process for the proposed activities, including having adequate systems in place to identify, measure, monitor, and control the risks of their activities. It is noted that while undertaking digital asset risk and control programs, it is imperative for organizations to adhere to the golden principles of any program implementation. These include governance and oversight, risk-prioritized assessment frameworks, involvement of skilled resources, record-keeping, and escalation protocols. This is specifically important because of the novelty of digital asset product offerings. Additionally, organizations should adopt metrics and reporting to ensure that the framework is robust and effective.

Throughout 2022, regulatory authorities in the US and globally are looking to provide further clarity on whether certain activities related to crypto assets are legally permissible, and appropriately set expectations for safety and soundness, consumer protection, and compliance with existing laws and regulations. Keeping abreast of these developments, Deloitte will refresh this paper in the next few months to provide an enhanced outlook of the regulatory expectations around the topic of market integrity and investor protection.

About Deloitte's Blockchain and Digital Assets Practice

At Deloitte, our people work globally with clients, regulators, and policy makers to understand how blockchain and digital assets are changing the face of business and government today. New ecosystems are developing blockchain-based infrastructure and solutions to create innovative business models and disrupt traditional ones. This is occurring in every industry and in most jurisdictions globally. Our deep business acumen and global industry-leading audit, consulting, tax, risk and financial advisory services help organizations across industries achieve their blockchain and digital asset aspirations. Reach out to our leaders to discuss harnessing the momentum of blockchain and digital assets, prioritizing initiatives, and managing the opportunities and challenges associated with blockchain adoption effort.



Endnotes

1. https://www.marketwatch.com/story/sec-chair-gensler-says-crypto-rife-with-fraud-scams-and-abuses-threatens-national-security-11628010216
2. https://coinmarketcap.com/alexandria/article/i-lost-everything-how-squid-game-token-collapsed
3. https://www.vice.com/en/article/z3new3/squid-game-memecoin-collapse
4. https://www.sec.gov/news/speech/gensler-securities-enforcement-forum-20211104
5. https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Financial-Services/gx-design-market-manipulation-in-digital-assets-whitepaper-v2-1.pdf
6. https://www2.deloitte.com/content/dam/Deloitte/us/Documents/finance/us-october-2021-digital-assets-regulatory-update.pdf
7. https://www.sec.gov/enforce/33-10920-order-s
8. https://www.cftc.gov/PressRoom/PressReleases/8366-21
9. https://www.bloomberg.com/news/articles/2021-09-17/u-s-s-binance-probe-expands-to-examine-possible-insider-trading
10. https://ciphertrace.com/cryptocurrency-crime-and-anti-money-laundering-report-august-2021/
11. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0593
12. https://beyer.house.gov/uploadedfiles/beyer_028_xml.pdf
13. https://www.nasdaq.com/articles/the-sec-still-doesnt-like-spot-bitcoin-etfs
14. https://www.nfa.futures.org/rulebook/rules.aspx?Section=9&RuleID=9073
15. https://www.cftc.gov/PressRoom/PressReleases/8162-20
16. https://www.sec.gov/files/digital-assets-risk-alert.pdf
17. https://www.cftc.gov/PressRoom/PressReleases/8336-20
18. https://www.finra.org/rules-guidance/guidance/reports/2017-report-exam-findings/product-suitability
19. https://www.federalreserve.gov/newsevents/pressreleases/files/bcreg20211123a1.pdf
20. https://occ.gov/news-issuances/news-releases/2021/nr-occ-2021-121.html

Contact us

Tim Davis
Principal
Deloitte Risk & Financial Advisory
Deloitte & Touche LLP
timdavis@deloitte.com

Richard Rosenthal
Principal, Business Entity Transformation
Deloitte & Touche LLP
rirosenthal@deloitte.com

Niv Bodor
Senior Manager
Deloitte Risk & Financial Advisory
Deloitte & Touche LLP
nbodor@deloitte.com

Will Killeen
Senior Consultant
Deloitte Risk & Financial Advisory
Deloitte & Touche LLP
wkilleen@deloitte.com

Subramanian Krishnan
Consultant
Deloitte Risk & Financial Advisory
Deloitte & Touche LLP
subrak@deloitte.com

Elia Alonso
Principal and Conduct Risk Practice Leader
Deloitte Risk & Financial Advisory
Deloitte & Touche LLP
elaonso@deloitte.com

Irena-Gecas-McCarthy
FSI Director, Deloitte Center for Regulatory Strategy, Americas
Deloitte & Touche LLP
igecasmccarthy@deloitte.com

Khyati Kabra
Senior Manager
Deloitte Risk & Financial Advisory
Deloitte & Touche LLP
kkabra@deloitte.com

Vaishali Singh
Senior Consultant
Deloitte Risk & Financial Advisory
Deloitte & Touche LLP
vaishasingh@deloitte.com

Pragya Chaturvedi
Consultant
Deloitte Risk & Financial Advisory
Deloitte & Touche LLP
pragchaturvedi@deloitte.com

Roy Ben-Hur
Managing Director
Deloitte Risk & Financial Advisory
Deloitte & Touche LLP
rbenhur@deloitte.com

Petal Walker
Managing Director
Deloitte Risk & Financial Advisory
Deloitte & Touche LLP
pewalker@deloitte.com

CJ Burke
Senior Consultant
Deloitte Risk & Financial Advisory
Deloitte & Touche LLP
cjburke@deloitte.com

Hilak Asheshkumar Patel
Senior Consultant
Deloitte Risk & Financial Advisory
Deloitte & Touche LLP
hilakpatel@deloitte.com

Deloitte.