GLOBAL KNOWLEDGE BRIEF

Fraud

Part 1: Fraud in Digital Assets

The Institute of Internal Auditors

Contents

Introduction **4**

Crypto and fraud in the global conversation 4

Uncertainty in the Cryptosphere **5**

Organizations are now paying attention 5

A Technology Ripe for Fraud **7**

A new tool in the bad actor's toolbox 7

Pig butchering 7

Pump and dump 8

Other fraud examples in a crypto asset context 8

Where Internal Audit Can Start **10**

Issued guidance resources 10

The value of education 11

Conclusion **12**

Internal audit is ready 12

About the Experts

Dana Lawrence, CIA, CRMA, CFSA, CAMS, CRVPM

Dana Lawrence is Fideseo's Chief Compliance Officer. She is a recognized expert and leader in complex compliance, enterprise risk management (ERM), internal audit, and governance program creation, scaling, and remediation. Lawrence's career in technology and financial services spans mortgage, community banking, large U.S. and global banks, open banking partners, fintech, and crypto. She's held senior leadership roles, working directly with banking regulators and internal/external auditors. Lawrence is a popular public speaker and event host, speaking at local, national, and global events with up to 40,000 participants. She is a committed volunteer and thought leader, serving various groups such as The IIA.

Lourdes Miranda, CAMS, CCE, CCFI, CEIC, CFE, CRC, FIS, MS

Lourdes Miranda is the Chief Consultant for Global AML Compliance, Crypto, and Investigations at RaLytics. She is a former CIA Officer and a former FBI Analyst with over 20 years of government and corporate experience specializing in crypto investigations, financial crime investigations, compliance, and intelligence collection and analysis globally. She has extensive field experience targeting money launderers and terrorist financiers. Since 2017, she has been working for Fintechs as a senior crypto investigator, senior compliance officer, and risk manager building compliance, investigations, crypto, and intelligence teams and training programs.

Introduction

Crypto and fraud in the global conversation

Sam Bankman-Fried, the charismatic founder of cryptocurrency exchange FTX, was once worth an estimated $26.5 billion. As the leader of what was at one point the third-largest exchange in the crypto market, Bankman-Fried and FTX were the darlings of a variety of high-profile investors such as BlackRock and NFL player Tom Brady. Yet, Bankman-Fried lost all of his wealth virtually overnight in one of the most dramatic company collapses in modern history.

Bankman-Fried was arrested on December 13, 2022, in the Bahamas. According to published reports, he faces various charges including wire fraud, wire fraud conspiracy, securities fraud, securities fraud conspiracy, and money laundering.

While there is a human interest in the sheer spectacle of such an incredible downfall, the event has also raised greater questions regarding digital assets. With parallels to scandals such as Tornado Cash and Bitzlato, FTX's collapse and the subsequent impact on the industry it represented has led many to question the long-term viability of crypto assets — at least in its current state, which U.S. Securities and Exchange Commission Chairperson Gary Gensler called the "Wild West."

Despite being built on blockchain technology, which is among the most secure ways to maintain crypto assets and information, if the very visible head of one of the world's most prominent cryptocurrency exchanges can allegedly commit acts of large-scale fraud, what other vulnerabilities might exist for companies that operate in the industry in some capacity? How has the risk landscape changed with the meteoric rise of crypto assets, and how are some organizations and their internal audit functions successfully responding to these changes?

Part 1 of this three-part series on fraud will address these questions by examining the common fraud schemes seen in the early stages of a crypto-asset world. For more information on this topic, The IIA will be hosting a replay of its recent webinar "Fraud perspectives: Blockchain, Crypto, and KYC" along with a live Q&A with the subject matter experts cited in this brief.

Uncertainty in the Cryptosphere

An exciting, but risky, future

Organizations are now paying attention

Although its implications are vast and nothing short of revolutionary, blockchain technology is relatively easy to understand conceptually as nothing more than a continuous, ever-growing log of digital asset transactions that can be shared and stored in virtually any network structure. What sets it apart is its use of verification methodologies that continuously encrypt the block with every new transaction, making it more secure.

"The technology itself can be complicated and it takes lots of training and education to understand and analyze, but I think of the blockchain itself as a financial statement that doesn't contain personally identifiable information, but has a wealth of information that is useful for conducting KYC and investigations," said Lourdes Miranda, chief compliance officer at RaLytics, a Washington, DC and Florida-based consulting firm. "The blockchain contains valuable information such as the transaction hash, both the sender and the receiver, the amount that was transferred, the date and timestamp of transactions, and the remaining change. This information can be used to develop leads, fuse intelligence gaps, and build criminal cases."

Cryptocurrency is arguably the most well-known asset that utilizes this technology, which creates a decentralized, open-source monetary system (or systems) immune from the influence of entities, such as central banks — but other examples of crypto assets based on blockchain include non-fungible tokens (NFTs), distributed ledger technologies (DLTs), and game tokens, among others.

However, as industries are quickly learning, just because crypto assets are built on secure technology virtually impossible to manipulate by traditional methods does not mean that its adopters are immune from risk. The FTX collapse illustrates this in more ways than one. For example, it highlighted just how damaging the lack of proper corporate governance and internal controls can be, not just for the organization, but for investors throughout the entire industry landscape.

This was a point IIA President and CEO Anthony Pugliese made in a recent letter to the U.S. Congress that called for legislators to establish new requirements to bolster corporate governance at cryptocurrency exchanges, blockchain technology companies, NFT marketplaces, and Web3 platforms operating in the United States. "Countless investors are now paying the price for FTX's failures," said Pugliese. "It's clear that we cannot rely on unregulated crypto exchanges to do the right thing on their own — we need to mandate stronger corporate governance standards and ensure accountability when these exchanges aren't protecting their customers. When bad corporate actors fail, it shouldn't be investors who are left holding the bag."

Pugliese emphasized that FTX's collapse and its market consequences could have been mitigated through the actions of a sound internal audit function. "The FTX collapse is the latest reminder that organizations without a robust internal audit function are, at best, playing with fire and, at worst, setting themselves and their stakeholders up for a disastrous – and entirely preventable – fall," he said.

These concerns from Pugliese and others did not fall on deaf ears. On January 3, 2023, the Federal Reserve, Federal Deposit Insurance Corporation (FDIC) and Office of the Comptroller of the Currency (OCC) released their first-ever joint statement on cryptocurrency. In it, they highlighted a variety of risks that could be in play for banking organizations operating in cryptocurrency in some form, including:

- Risk of fraud and scams among crypto-asset sector participants.
- Legal uncertainties related to custody practices, redemptions, and ownership rights.

- Inaccurate or misleading representations and disclosures by crypto-asset companies.
- Significant volatility in crypto-asset markets, the effects of which include potential impacts on deposit flows associated with crypto-asset companies.
- Contagion risk within the crypto-asset sector resulting from interconnections among certain crypto-asset participants, including through opaque lending, investing, funding, service, and operational arrangements.
- Risk management and governance practices in the crypto-asset sector exhibiting a lack of maturity and robustness.
- Heightened risks associated with open, public, and/or decentralized networks, or similar systems.

While these risks are worthy of discussion (and in many cases applicable to organizations beyond banks dabbling in crypto), this brief will limit the focus to acts of fraud committed on crypto participants and the prominent forms they take in the current environment.

A Technology Ripe for Fraud

An ever-expanding risk landscape

A new tool in the bad actor's toolbox

While crypto assets have many advantageous characteristics such as transparency and remarkably advanced encryption against manipulation, these same characteristics have made these assets (and the blockchain technology behind it) a powerful tool for those looking to commit fraud.

Indeed, it is this appeal to bad actors that has drawn the immediate attention of regulators and law enforcement. "Blockchain is very difficult to manipulate, but it can be utilized in ways that promote nefarious activity," said Miranda. "For example, bad actors will use legitimate, stolen identities purchased on the black market in order to be able to pass the KYC [Know Your Customer] onboarding process when they open wallets. These identities do not have criminal backgrounds and are not on any blacklist — they are completely clean. Then, under these clean identities, bad actors can conduct crypto transactions with limited scrutiny."

The crypto asset industry has also introduced a variety of tools that, while designed for consumer convenience, "have a variety of loopholes that can be exploited such as Bitcoin ATMs (BTMs). A bad actor, for example, can use a burner phone at the BTMs to circumvent KYC protocols," said Miranda.

"Let's say I'm in New York, and I have to pay my bad actors in Miami," said Miranda. "They want to be paid and paid fast. I'm not going to write a check, and I don't want to use a computer or laptop, so I use a non-custodial wallet and use a BTM in New York, deposit cash to purchase crypto, and a burner phone. This way, I can send crypto while circumventing anti-money laundering protocols."

Pig butchering

Another common fraud tactic that bad actors can utilize is known by the graphic term "pig butchering." "This is basically the concept of a fraudster metaphorically 'fattening up' their victim by investing a lot of time with them in order to establish trust," said Dana Lawrence, chief compliance officer at business and technology consultant firm Fideseo. The time invested by fraudsters can happen anywhere, according to Lawrence, but most prominently occurs either on social media or through texts over the course of weeks or months. Lawrence cited LinkedIn specifically as a favored platform, as well as social sites such as Twitter.

In these cases, the bad actor typically will present themselves as an influencer or insider who has successfully invested in cryptocurrency. Over time, they will tout the benefits of cryptocurrency in an effort to get the victim to transfer their assets to them. In some cases, fraudsters have even provided the victim with forged financial statements to make it appear substantial returns are being made.

While it is easy to read these signs and find them obvious to spot, fraudsters employing this method have become highly sophisticated. Scamming teams based in countries such as Cambodia and China, for example, have received in-depth training from psychologists in how to make people vulnerable to making unsound decisions.

“They’ve been trained by psychologists to try to figure out the best way to manipulate people,” said Santa Clara County, California, district attorney Jeff Rosen in an interview with CNN. “You’re dealing with people that are going to use different psychological techniques to make you vulnerable and to get you interested in parting with your money.”[1]

Pump and dump

The other major fraud form being seen in the cryptosphere is well-known to long-time observers of the stock market: the so-called “pump and dump” scheme.

“This scheme typically starts with a group coming together to start a new crypto project such as a token, and then uses — commonly with the help of influencers — resources to hype it up on platforms such as Twitter or Discord,” said Lawrence. “There’s currently a lot of fluctuation in the crypto market due to liquidity. So, if a lot of people try to buy something all at once, it kind of shocks the market into raising the price. If this happens, the bad actors in question holding large amounts of the asset suddenly sell it off for a profit, dropping the price suddenly and leaving all other investors with something worth essentially zero.”

The red flag in these situations, said Lawrence, is a distinct lack of disclosures that indicate to potential investors that losing everything is a distinct possibility. The actors will also typically make strong use of copy-and-pasted messages on social media and discussion boards written by posters with similar screen names. And, once the scheme is complete, these screen names will usually disappear, their anonymity completely intact.

Other fraud examples in a crypto asset context

Crypto-based fraud does not always have to be so sophisticated. Within crypto-based organizations, often all that is necessary for a bad actor is the right opportunity. For example, while the blockchain itself will keep digital assets secure, all that is needed to bypass security and empty a crypto wallet is obtaining a private key — a long stream of numbers that could fit on a restaurant napkin and be left anywhere for anyone to find.

"Your private key is your digital identity to the cryptocurrency market, and anyone who gets hold of this can perform fraudulent transactions or steal your crypto coins,” said Lawrence. “If someone somehow gains access to that, and they took all my Bitcoin out, there's nothing I can do about it. I can't get it back, I can't file a complaint, there's no consumer protection agency or regulator to dispute it with — it's literally gone."

As the crypto market matures, crypto security services have emerged that specialize in protecting individual and company keys from misplacement, but in some cases their methodologies are surprisingly primitive. According to Lawrence, the solution some of these services employ is storing the keys in vaults on the side of desolate mountains. Crypto insurance also exists as a safety net for companies that can afford it, but at this stage the entire industry is struggling with profitability, forcing insurers to be incredibly selective while simultaneously offering coverage that has been shrinking by the year.

In an article published in the U.K.’s Insurance Times, RPC Insurance group partner James Wickes discussed the challenges of the crypto insurance market. “The relatively small number of insurers currently active in the crypto asset insurance space are likely to be keen to review the fine print on policy wordings to limit potential exposure from the volatility of the crypto markets, as demonstrated by the recent crash,” he said. “The insurance market for these assets is in its infancy and it remains to be seen whether a sufficient body of insurance carriers will be prepared to provide enough capacity to meet the demand and how brave the market will be to extend coverage beyond the traditional theft risk.”[2]

Despite these precautions, however, there remain certain tools bad actors can apply to utilize crypto assets and blockchain without directly bypassing an established account — namely mixers, also known as tumblers. One of the core features of a blockchain is its transparency; within any blockchain explorer, anyone can view the record of all blockchain transactions

1. Josh Campbell, “Beware the ‘Pig Butchering’ Crypto Scam Sweeping Across America,” December 26, 2022, https://www.cnn.com/2022/12/26/investing/crypto-scams-fbi-tips/index.html.
2. Isobel Rafferty, “Cryptocurrency Crisis Leading to Insurance Policy Wording Amendments,” Insurance Times, July 18, 2022, https://www.insurancetimes.co.uk/news/cryptocurrency-crisis-leading-to-insurance-policy-wording-amendments/1441786.article.

since the launch of cryptocurrency in 2009. Mixers allow the user to essentially jumble the amount of crypto assets in question before delivering them to intended recipients, giving them a degree of anonymity since it is so difficult to decipher exactly who sent how many assets to whom. Using a mixer, all an explorer will show is that one person, as well as dozens of other people, sent assets to a mixer, who then sent the assets in varied amounts to a variety of other people. The result, in essence, resembles a perfected form of money laundering.

Facing these realities, organizations that choose to exist in the cryptosphere must accept that they are largely on their own when it comes to risk mitigation at this stage. This does not mean that crypto should be avoided, but it does mean that compliance, sound internal control, fraud detection and deterrence efforts, and internal audit must play an outsized part in crypto conversations from the board level down.

Where Internal Audit Can Start

Regulation is here with more to come

Issued guidance resources

As previously mentioned, the regulatory frameworks companies can look to for handling security and governance regarding crypto assets and associated fraud-based risks is scant. However, certain industries such as financial services are not entirely bereft of resources that address proper governance principles regarding digital asset protection — many of which are applicable to cryptocurrency.

In October 2022, the European Union introduced the agreed-on text of the Markets in Crypto-Assets (MiCA) Regulation, which is one of the first attempts globally at comprehensive regulation of cryptocurrency markets, although the legislation has been tabled until April 2023 to translate it into 24 different languages. Should it be formally adopted, the regulation will:

- Officially define a crypto asset as "a digital representation of value or rights which may be transferred and stored electronically, using distributed ledger technology or similar technology." Additionally, it offers four different categories of crypto-assets: asset-referenced tokens, e-money tokens, utility tokens, and a fourth category for crypto-assets that do not fall in the other three categories.
- Officially make crypto providers liable if they lose investors' crypto assets.
- Requires actors in crypto-asset markets to declare information on their environmental and climate footprint.
- Overlap with updated legislation on anti-money laundering, and task the European Banking Authority (EBA) with maintaining a public register of non-compliant crypto-asset service providers.
- Require crypto-asset providers to have authorization to operate in the EU.
- Provide a strong framework applicable to "stablecoins" (cryptocurrency that is pegged to an external reference asset), which will require every stablecoin holder to be offered a claim at any time by the issuer, free of charge.[3]

In the U.S., the joint statement from the Federal Reserve, Federal Deposit Insurance Corporation (FDIC), and Office of the Comptroller of the Currency (OCC) offers a few resources for U.S. firms that provide guidance designed to help "banking organizations engage in robust supervisory discussions regarding proposed and existing crypto-asset-related activities."[4] These include:

- OCC Interpretive Letter 1179: "Chief Counsel's Interpretation Clarifying: (1) Authority of a Bank to Engage in Certain Cryptocurrency Activities; and (2) Authority of the OCC to Charter a National Trust Bank."
- Federal Reserve SR 22-6/ CA 22-6: "Engagement in Crypto-Asset-Related Activities by Federal Reserve-Supervised Banking Organizations."
- FDIC FIL-16-2022: "Notification and Supervisory Feedback Procedures for FDIC-Supervised Institutions Engaging in Crypto-Related Activities."

3. General Secretariat of the Council, "Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937 (MiCA)," Council of the European Union, October 5, 2022, https://data.consilium.europa.eu/doc/document/ST-13198-2022-INIT/en/pdf.
4. "Joint Statement on Crypto-Asset Risks to Banking Organizations, Board of Governors of the Federal Reserve System Federal Deposit Insurance Corporation Office of the Comptroller of the Currency, January 3, 2023, https://www.fdic.gov/news/press-releases/2023/pr23002a.pdf.

These are hardly the only resources available. In the wake of the FTX collapse, the SEC also released guidance advising companies to disclose their involvement with digital commodities firms.

The value of education

Assuming it is adopted, the proposed EU legislation would take effect in 2024, but it almost certainly will not be the last. As the patchwork regulatory landscape fills in month to month, the most valuable action an internal auditor can take is to make every effort to stay abreast of the changes and clearly articulate those changes to the board and applicable stakeholders.

In the current environment, internal auditors should also inform stakeholders of other regulations applicable to crypto. For example, said Lawrence, a company offering its own cryptocurrency may require registration with the U.S. Financial Crimes Enforcement Network — a critical detail that could be easily overlooked because crypto is not specifically cited in the legislation. "There is a lot of uncertainty now," she said. "It is up to internal auditors to inform leaders about what is applicable and what is not."

Focus on new technologies should also not distract companies from basic best practices regarding digital asset protection, including the use of a virtual private network (VPN) and proper security, collection, and, when needed, disposal of user profile information — especially consumers. "User profiles are a critical organizational control," said Miranda. "If I was conducting transaction monitoring, I would verify that user profiles match their transactional activity. For example, where a user physically resides is incredibly important in compliance and investigations. The users' profile reflects that they listed their home and/or business address from a non-sanctioned country to ensure they pass KYC protocols, but their transaction activity reflects that they are sending and receiving transactions to and from a sanctioned country."

For more information, The IIA's Supplemental Guidance "Internal Audit and Fraud: Assessing Fraud Risk Governance and Management at the Organizational Level, 2nd Edition" offers clear direction regarding organizational roles and responsibilities for sound fraud risk governance and management, as well as recommendations for additional guidance such as COSO's Fraud Risk Management Guide.

Conclusion

Internal audit is ready

Cryptocurrency and the technology that it is based on are too revolutionary for internal audit to ignore, with stakes that more than deserve the attention of the board. Risk assessments that ignore it have a critical blind spot. Cryptocurrency may be a relatively new concept for many, but it does not diminish the value of a sound fraud risk management framework that can be measured and tested by internal audit.

While it is easy to bemoan yet another risk area to add to internal audit's ever-growing radar, the good news is that no other organizational department is positioned better to address it. Much like the Sarbanes-Oxley Act (SOX) did in 2002, the evolution of cryptocurrency regulation virtually assures internal audit a valued position at the table for years to come. Even if the function does not yet know crypto, it does know fraud, and it does know risk; that alone is enough to prime internal audit to take a position of leadership tackling the challenges ahead.

About The IIA

The Institute of Internal Auditors (IIA) is a nonprofit international professional association that serves more than 230,000 global members and has awarded more than 185,000 Certified Internal Auditor (CIA) certifications worldwide. Established in 1941, The IIA is recognized throughout the world as the internal audit profession's leader in standards, certifications, education, research, and technical guidance. For more information, visit theiia.org.

Disclaimer

Copyright

January 2023

The Institute of Internal Auditors

Global Headquarters
The Institute of Internal Auditors
1035 Greenwood Blvd., Suite 401
Lake Mary, FL 32746, USA
Phone: +1-407-937-1111
Fax: +1-407-937-1101