Operational Due Diligence on Cryptocurrency and Digital Asset Funds

Jason Scharfman

Jason Scharfman
is a managing partner at Corgentum Consulting in New York, NY.
scharfman@corgentum.com

KEY FINDINGS

- The rigor of operational due diligence on crypto investments and asset managers has increased as more institutional capital has migrated into the crypto space.
- Crypto asset managers increasingly are focused on developing more institutional operational infrastructures, particularly in areas such as custody for DeFi investments.
- Investors increasingly combine investigative and operational due diligence processes when evaluating crypto asset managers.

ABSTRACT

This article analyzes three key trends that have emerged among institutional investors performing operational due diligence (ODD) on cryptocurrency and digital asset funds. The first trend is enhanced crypto-specific ODD specialization as compared to other alternative asset classes. The second trend is an institutional focus on crypto custody arrangements. The third trend is a rapid movement toward integrating ODD and investigative due diligence processes in the crypto space.

With the continued bull market in the cryptocurrency space, there has been a marked transition from largely retail investors focused on the space toward more institutional interest in cryptocurrencies and digital assets. Much of this interest has come not only in the form of direct investments into cryptocurrencies and related digital assets themselves, but also through allocations to third-party external fund managers that invest in the crypto space. While there are well-established procedures for operational due diligence on alternative investment managers such as hedge funds and private equity funds, as with any emerging asset class, cryptocurrency and digital asset funds present a unique set of asset-specific due diligence challenges. As more capital has flowed into the crypto space, institutional limited partners (LPs) increasingly are struggling to adapt both their investment and operational due diligence (ODD) procedures to the space.

This article will focus on ODD trends that have emerged in the institutional LP ODD space for crypto and digital asset fund managers. These trends are

- Enhanced crypto-specific ODD specialization as compared to other alternative asset classes
- Focus on crypto custody arrangements
- Rapid combination of crypto fund manager investigative due diligence and ODD processes.

It should be noted that these trends cover the entire crypto and digital asset fund manager space and are not necessarily specific to a certain strategy such as decentralized finance (DeFi) or large coin market-capitalization strategies. Prior to continuing with our analysis of these trends in more detail, it will first be useful to provide a historical context on how the current state of institutional LP ODD came about as well as to clarify select relevant terminology.

BACKGROUND

What Is Cryptocurrency Fund Operational Risk?

One of the most established definitions states that operational risk is the risk of loss resulting from inadequate or failed internal processes, people, or systems, or from external events (Basel Committee on Banking Supervision 2011). The term business risk is also sometimes utilized to refer to operational risk. In the world of alternative investments, operational risk has turned into a broad catch-all category for LPs to bucket all other risks that do not directly relate to the investment function of a fund. It should be noted that in practice, there is an overlap between the analysis of operational risk and investment areas of a fund manager. However, this classification of risks into investment and operational buckets is still useful in order to guide an LP's review toward the framework by which certain risks are analyzed. In the crypto space, this same broad operational risk definitional framework is applied much the same way as it is in the alternative investment space.

What Is the Difference between Crypto Operational Due Diligence and Operational Risk?

In the crypto space and the broader alternative investment context, operational due diligence refers to the process by which operational risk is analyzed. Operational due diligence is employed by LPs prior to an investment allocation (i.e., pre-investment ODD) and then on an ongoing basis to monitor operational risks in the crypto funds to which they had previously allocated.

REASONS FOR INCREASED FOCUS BY CRYPTO LIMITED PARTNER OPERATIONAL DUE DILIGENCE

In recent years, LPs have devoted more resources toward the operational due diligence process, and this trend has continued into the crypto space. Unfortunately, very similar to the hedge fund space, a key reason for this has been a series of outright frauds. Although many of the crypto frauds may not have been as large scale or as brazen as the Madoff fraud, the Bayou Hedge Fund Group fraud, or the Galleon insider trading case, the crypto hacks and frauds still have caused significant concerns for investors. Some of the more notable crypto frauds include the more than $460 million stolen from Tokyo-based bitcoin exchange Mt. Gox in 2014 and the $500 million hack of Japanese firm Coincheck in 2018. There also has been a continued series of lower-profile cases that continues to remind investors to focus on operational due diligence.

Another reason for LPs' increased operational due diligence efforts includes the pervasive skepticism surrounding the security and reputation of crypto-related investments. Many of these concerns are rooted in the traditional black cloud that has hung over the crypto space, where crypto assets such as Bitcoin are perceived

to be primarily utilized by criminals on dark web portals such as Silk Road to conduct criminal activity. Recent studies have shown that these associations continue to overrepresent the illegal ways in which cryptocurrencies are utilized (Lennon 2021). For example, a series of studies conducted by Chainalysis showed that in 2019 criminal activity represented only 2.1% of all cryptocurrency transaction volume or approximately $21.4 billion. In 2021, a revised Chainalysis study (Chainalysis 2021) showed that this number has continued to decrease, with the criminal share of all cryptocurrency activity falling to only 0.34% or approximately $10 billion in transaction volume.

An additional contributing factor toward the continued association between cryptocurrencies and criminal activity involves crypto in ransomware payments. Ransomware attacks are common cybersecurity attacks where criminals install software on a computer or network that locks the legitimate users out of the system until a ransom is paid. Due to their need for speed and anonymity, criminals increasingly require payment in cryptocurrencies such as Bitcoin for their ransom. A May 2021 ransomware attack by the criminal organization the DarkSide group on Colonial Pipeline caused damage to America's supply of gas and resulted in the payment of nearly $5 million in cryptocurrency to the group to unlock the compromised systems (Sigalos 2021). These types of attacks have continued to reinforce concern among regulators and LPs about allocating to crypto hedge funds.

Even before the Colonial Pipeline attack, in 2020, the US Treasury Department, in conjunction with the Financial Crimes Enforcement Network (FinCEN), proposed enhanced rules requiring banks, exchanges, and others dealing in cryptocurrencies to undertake enhanced processes compliance measures. Proposed regulations require these entities to focus on better verifying the identities of individuals attempting to withdraw or resend cryptocurrencies, with a particular focus on unhosted wallets. Unhosted wallets are held by individuals outside of the financial system. As unhosted wallets are unaccountable and unreportable to any exchange or broker with KYC/AML controls, they are more likely to be used to conceal tax liability or illicit activity. This type of evolving regulatory uncertainty, coupled with the increased ransomware attacks to a level quadruple that of 2019, has continued to motivate LPs that seek to allocate to the crypto space to devote more resources toward their crypto ODD procedures (Light 2021).

ENHANCED CRYPTO-SPECIFIC ODD SPECIALIZATION AS COMPARED TO OTHER ALTERNATIVE ASSET CLASSES

The crypto space evolves rapidly. Although the market continues to be dominated by well-established blockchains such as Bitcoin and Ethereum, there is a constant stream of new crypto-related projects and associated new coin offerings. Recently there has also been a large growth in digital art and non-fungible tokens, stablecoins, and DeFi related projects. As a result, institutional LPs have had to markedly increase the specialization of their ODD procedures to more appropriately vet crypto and digital asset–related risks.

A survey of operational due diligence analysts conducted by Corgentum Consulting in May 2021 (Corgentum Consulting 2021) found they are increasingly creating crypto-specific ODD policies and procedures. Specifically, 84% of those surveyed stated they had developed new due diligence questionnaires for crypto fund managers being evaluated, to better address the unique operational challenges presented by crypto investing. Furthermore, 73% of those surveyed said they were struggling to determine what constituted best practices, particularly in the areas of operations and

compliance, in the crypto space. A large contributor to this challenge, noted the ODD analysts surveyed, is the large deviation from traditional institutional level practices that hedge funds employ in key operational areas such as custody and valuation.

FOCUS ON CRYPTO CUSTODY ARRANGEMENTS

One key area to which institutional LPs have devoted enhanced ODD resources is crypto custody. Custody refers to the process by which crypto assets are stored in a secure and documentable manner. In the early days of the crypto space, largely due to the belief that crypto investments should support the decentralization of financial services, many crypto investors held self-custody of assets in cold wallets, such as on their personal computers or portable hard-drive type wallets. This is obviously not the most secure solution because an individual's home computer is subject to failure or hacking. Additionally, cold storage wallets may be lost or stolen. Finally, a user can simply forget the password to the wallet. That issue led to the development of pneumonic seed phrases that can help users remember their passwords, but this is not a foolproof system. For all these reasons, institutional investors are increasingly skeptical of self-custody solutions.

One alternative to self-custody for a crypto fund manager is a hybrid solution sometimes referred to as a wallet plus solution, which uses hardware wallets with additional security measures layered on top. These other security measures might be two-factor authentication protocols or a requirement for multiple signatories, administered by a third party, before transactions occur in the wallet.

The third custody model that crypto fund managers can employ is an entirely third-party custody solution. Third-party custody models are well established for alternative investment vehicles such as non-crypto hedge funds and private equity funds. Hedge funds that are increasingly investing in the crypto space through coins such as Litecoin, Ether, and Bitcoin also have embraced the traditional third-party custody model for crypto assets, with more than 52% of crypto hedge funds employing a third-party custodian as of 2019. Anecdotal evidence suggests this number has steadily increased as more institutional LPs have focused on crypto asset custody during the ODD process (PwC 2019).

Implementing third-party custody solutions has been made easier by the linked custody solutions being offered by crypto exchanges such as CoinBase and Gemini. These exchanges already offer institutional LPs internet-connected hot wallet options that allow crypto funds to store their coins in wallets hosted by the exchange instead of in purely cold wallet storage options. Third-party custodian models meet the more traditional established standards of non-crypto hedge fund and private equity institutional level custody. Due to the enhanced risks of hacks allowing for the virtually anonymous stealing of crypto assets once they are transferred to new wallets, crypto third-party custody solutions increasingly are mirroring the security measures employed by offsite business continuity and disaster recovery sites utilized by hedge funds.

These hardened facilities where physical keys to the assets of crypto fund managers are kept often include military-grade security and biometric scans and highly specialized security devices such as hardware security modules (HSMs), the most secure of which are subject to Federal Information Processing Standard (FIPS) security ratings (Gemini 2019).

Increasingly, institutional LPs are analyzing whether a crypto fund manager is employing purely third-party custody or some other hybrid solution, and they are going a step further to evaluate the quality of the custody solutions and third-party

custodians employed. This type of advanced analysis represents a notable change in the depth of operational analysis being performed by these LPs. As more institutional capital has flowed into the crypto space, many institutional LPs no longer are playing catch up to grasp the basic tenants of crypto custody; many have been able to elevate their analysis to apply more traditional types of deeper analysis. Common questions asked by LPs to evaluate the quality of the third-party custodians being utilized include the following:

- What are the third-party custodian's business continuity and disaster recovery plans?
- Does the third-party custodian maintain any insurance in the event of a hack or other unauthorized transfer of crypto assets?
- How does the third-party custodian approach the staking of crypto assets from a custody perspective?
- How will the third-party custodian approach the custody of newly issued coins for which pre-existing custody solutions may not exist?
- Can the third-party custodian provide auditable paper trails of all transactions into and out of the fund's wallets?

To be clear, some crypto fund managers in spaces such as DeFi may still employ quasi self-custody solutions due to a lack of support for newer or evolving DeFi projects and related coins. In these types of situations, operational due diligence becomes increasingly important. First, the current custody solution employed by the crypto fund manager is analyzed, and the risk level is diagnosed. Then the institutional LP can consult with the crypto GP to determine if any alternative custody arrangements are available, which would facilitate the fund manager's investment process while minimizing the LP's operational risk exposure in the area of custody risk.

TREND OF COMBINING OPERATIONAL AND INVESTIGATIVE DUE DILIGENCE CATEGORIES

Investigative due diligence, also called a background investigation, is the process of verifying and analyzing the background details and reputation related to the individuals involved in managing the crypto fund. The five core areas covered by investigative due diligence, as described by Corgentum (2021), are

- Criminal checks
- Litigation searches
- Regulatory research
- Factual information review and confirmation (i.e., previous employment, educational background)
- News and social media reviews

Historically, many LPs had outsourced the investigative process to a third-party firm that focused only on background investigations, coming from a hedge fund and private equity context. In recent years, a trend that has emerged throughout the alternative investment industry is for LPs to integrate the background investigation process with operational due diligence. A key driver for this trend is that in many cases, increased familiarity with more common reputation and background issues often can help provide a benchmark by which LPs can better compare findings.

This trend also has taken hold in the crypto space, arguably at a faster adoption rate than the speed at which this combined model was adopted in other segments of

the alternative investment space. A key reason for this is because of the aforementioned and often misplaced criminal associations linked to the use of cryptocurrencies and, by association, those that allocate capital in the space. This, combined with increased regulatory uncertainty in the crypto space, has caused more institutional LPs to take rapid measures to adjust their ODD process to integrate investigative due diligence and also to enhance the scope and depth of their investigative efforts. These investigations include reviews of key individuals of the crypto fund general partners, such as the chief investment officer, chief operating officer, key portfolio management personnel, and of fund management entities.

This enhanced investigative and operational work takes place in other crypto-related investments as well. When a private equity firm makes a direct ownership investment in a decentralized crypto exchange (DEX), for example, the private equity GP likely would perform deal-level operational due diligence and investigative due diligence on the DEX and associated key personnel. From an LP's perspective, when seeking to allocate capital to the private equity firm that made the DEX investment, many LPs increasingly have modified their due diligence efforts under this new combined model to look through the private equity GP to the underlying DEX investment. This enhanced level of due diligence may result in the LP performing its own background checks on key DEX personnel and entities, as well as evaluating the rigor of the DEX's operations and compliance infrastructure, particularly in the area of anti-money laundering (AML) compliance. By combining the ODD and investigative due diligence procedures, LPs in the crypto space are finding they are better suited to evaluate the often enhanced operational complexities and reputational risks associated with investing in the crypto space.

CONCLUSION

As institutional capital has continued to flow into the crypto space, traditional approaches toward due diligence increasingly have had to adapt to meet the new operational, compliance, and regulatory challenges. Three key trends have emerged in the operational due diligence procedures employed by investors allocating to crypto and digital asset hedge funds in the space. The first trend is the enhanced crypto asset-specific specialization that institutional LPs have undertaken. This trend has taken hold because of the quickly evolving nature of the crypto space and the unique operational and compliance challenges presented by crypto assets.

The second trend has involved a specific focus by institutional LPs during ODD on crypto custody arrangements. As the focus on this area has increased, crypto custody due diligence has continued to evolve beyond allowing LPs to develop a basic understanding of the crypto custody space toward conducting more-sophisticated analyses of the counterparty risk and quality of third-party crypto custody providers.

The third trend that has developed, largely due to the continued associations of the crypto space with criminal activity and regulatory uncertainty, is the rapid acceptance of due diligence models that combine investigative due diligence and ODD processes for crypto-related investments.

As institutional investors continue to embrace crypto-related investments, institutional LPs likely will continue to evolve and refine their operational due diligence procedures to adapt to the evolving series of cryptocurrency operational risks. These evolving ODD practices will also benefit from enhanced regulatory clarity toward the oversight of crypto assets, such as the forthcoming pan-European regulation called the Markets in Crypto-Assets Regulation (MiCAR). These regulations will provide a clearer roadmap that gives institutional investors more confidence in the regulatory oversight of the crypto space—and likely will serve to support the existing institutional ODD frameworks that have evolved in the area.

REFERENCES

Basel Committee on Banking Supervision. 2011. "Principles for the Sound Management of Operational Risk." June. Available at: Principles for the Sound Management of Operational Risk (bis.org).

Chainalysis. 2021. "Crypto Crime Summarized: Scams and Darknet Markets Dominated 2020 by Revenue, but Ransomware Is the Bigger Story." January 19. Available at: Chainalysis Blog | Crypto Crime Summarized: Scams and Darknet Markets Dominated 2020 by Revenue, But Ransomware Is the Bigger Story.

Corgentum Consulting. 2021. "Investigative Due Diligence/Background Checks." Available at: Cloud Level (com.services).

Gemini. 2019. "A Guide to Crypto Custody." Available at: guide-to-crypto-custody.pdf (gemini.com).

Lennon, H. 2021. "The False Narrative of Bitcoin's Role In Illicit Activity." Forbes, January 19. Available at: The False Narrative Of Bitcoin's Role In Illicit Activity (forbes.com).

Light, J. 2021. "Crypto's Anonymity Has Regulators Circling after the Colonial Pipeline Hack." *Bloomberg Businessweek*, May 12. Available at Crypto's Anonymity Has Regulators Circling After the Colonial Pipeline Hack – MCC.EXCHANGE.

PwC. 2019. "Crypto Hedge Fund Report." Available at: pwc-elwood-2019-annual-crypto-hedge-fund-report.pdf.

Sigalos, M. 2021. "Colonial Pipeline Cyberattack Is No Cause For Panic – Here's Why." CNBC, May 14. Available at: Colonial Pipeline cyberattack is no cause for panic – here's why (msn.com).