The Principles of Risk Management for Crypto

Authors: Suzanne Morsfield, Global Head of Accounting Solutions and Brian M. Whitehurst, Head of US Regulatory Affairs of Lukka

Background

Recent developments within the crypto industry have captured the attention of crypto market participants and observers. Due to the plunge of the market earlier this summer, highlighted by the collapse of the TerraUSD (UST) stablecoin, and the insolvency of crypto hedge fund Three Arrows Capital, and CeFi platforms Celsius and Voyager, regulators are paying more attention than ever.[1]

These bankruptcies and significant losses shine a light on a key, even basic financial principle–the risk-return relationship. This relationship implies that to take on higher risk, investors typically require a higher return for their investments. Numerous entities in the crypto environment offered APYs north of 20%, rates unheard of in traditional finance.[2] And while high yields seem great, investors would be wise to ensure they understand that they are most likely also taking on higher risk.[3]

One of the virtues of DeFi (decentralized finance) is that the individual has complete control over their finances (note, not all crypto trading is in DeFi, as much of it has been centralized). But at what point does that control start to become risk-return negative? Too much risk can lead to a collapse of a macro system because the continuous returns associated with the undisclosed risk becomes untenable over time. This leads to the observation that a risk management mindset, coupled with risk management methods, are a necessity in crypto finance.

Realities dictate that regulators worldwide are going to have a say, and while proportional regulation that doesn't stifle innovation is important, it doesn't need to be the only solution. Even with all of its advances over traditional finance, the crypto industry can still learn from traditional finance when it comes to creating and maintaining safer innovation while still enabling responsible profit-taking.

---

[1] "Crypto Winter Watch: All The Big Layoffs, Record Withdrawals And Bankruptcies Sparked By The $2 Trillion Crash", Forbes (August 18, 2022); "Factbox: The crypto crash hit these companies the hardest", Reuters (July 28, 2022).
[2] "Top 25 Projects With the Highest Staking Yields in Crypto", Bitcoinist.com (June 8, 2022).
[3] "What Happens When Cryptocurrencies Earn Interest?", Harvard Business Review (February 23, 2021).

How Can Risk Management Improve Crypto Finance?

Traditional finance, while sometimes viewed as the antithesis of crypto, utilizes core principles and tools which much of the crypto industry has began to institute to a higher degree in order to protect the market as a whole. Moody's Analytics observed:[4]

> "In traditional finance, we rely on the time-tested understanding of micro- and macro-economic structures to evaluate an obligor's risk and creditworthiness. However, DeFi is rapidly evolving with insufficient transparency, a lack of shared awareness about its risks, and methods to measure and mitigate those risks."

Developing the principles below will allow the crypto industry, including those focused on DeFi, to take additional steps towards maturity:

- Focus on substance over form
- Enable and use liquidity analysis and have audited financials
- Conduct ongoing performance monitoring
- Clarify collateral, custody, and segregation of assets
- Enhanced disclosure and Terms and Conditions (T&Cs)
- Don't ignore operational risk domains; such as technology risk, cybersecurity risk, and data quality risk

Focus on substance over form

- The concept of substance over form weighs heavily in securities law, and in tax and financial reporting. At a basic level, it looks beneath the surface of the naming or marketing of the asset or transaction to the underlying economic, tax, accounting, or legal definitions, depending on whether one is looking at a tax return, financial statements or a restructuring, for example. Understanding the substance is necessary to understanding the risk. Experts should weigh in before the product goes to market. The form and substance of a new product should both match, and be made crystal clear when a lawyer or auditor looks in.

  For financial reporting and other regulatory purposes, the substance is especially important. While issuers or holders of particular crypto assets may

[4] See "Block by Block: Assessing Risk in Decentralized Finance," Moody's Analytics (January 2022), for a thorough summary of specific risk-related issues directed primarily at crypto DeFi transactions. Many principles delineated within this report are relevant for other crypto transactions.

have a preferred view, regulators and courts regularly weigh in when that view contradicts substance. Auditors have reminded their clients of their own responsibilities to understand not just the form, but the substance, rights and obligations of their crypto asset holdings.[5]

The SEC has corrected public filings more than once for what they deemed misleading or erroneous interpretations of the substance of reported crypto holdings or transactions. For example:

1. SEC v. REcoin Group Foundation, LLC, DRC World Inc. a/k/a Diamond Reserve Club, and Maksim Zaslavskiy[6]

   "The label Zaslavskiy chooses to attach to the alleged scheme does not control our analysis. See SEC v. Edwards, 540 U.S. 389, 393 (2004) ('Congress' purpose in enacting the securities laws was to regulate investments, in whatever form they are made and by whatever name they are called.') (quoting Reves v. Ernst & Young, 494 U.S. 56, 61 (1990)... simply labeling an investment opportunity as a 'virtual currency' or 'cryptocurrency' does not transform an investment contract – a security – into a currency... in searching for the meaning and scope of the word 'security'...form should be disregarded for substance and the emphasis should be on the economic reality."

2. SEC comment letter to Microstrategy Incorporated[7]

   "We note your response to prior comment 5 and we object to your adjustment for bitcoin impairment charges in your non-GAAP measures. Please revise to remove this adjustment in future filings. Refer to Rule 100 of Regulation G."

- Crypto asset classifications that look beyond marketing to the underlying characteristics and components of the products are important.

  Specific countries are specifically regulating the marketing of crypto assets.[8] The SEC has pursued the classification issue with filers across a variety of

[5] "Cryptoassets - Accounting and tax, What's the impact on your financial statements?," KPMG (April 2019).
[6] United States District Court for the Eastern District of New York, Case No. 1:17-cr-00647-RJD-RER.
[7] SEC letter, dated December 3, 2021, to Microstrategy Incorporated, Re: Microstrategy Incorporated Form 10-K for Fiscal Year Ended December 31, 2020, Filed Filed February 12, 2021, Form 10-Q for the Quarter Ended September 30, 2021, Filed October 22, 2021, File No. 000-24435.
[8] For example, see: "Dubai issues crypto marketing rules to better protect investors" (Cointelegraph, August 29, 2022) and UK Advertising Standards Authority, "Cryptoassets" (August 17, 2022).

transactions or holdings. Initially, much of the attention was directed at Initial Coin Offerings (ICOs) offerings that were marketed as utility tokens, and the SEC believed them to be, in fact, securities. This regulatory oversight has also included asset classifications that directly affect the financial reporting within registrants' 10-K or 10-Q filings.

1. Former SEC Chairman, Jay Clayton, statement[9]
   "Merely calling a token a 'utility' token or structuring it to provide some utility does not prevent the token from being a security. Tokens and offerings that incorporate features and marketing efforts that emphasize the potential for profits based on the entrepreneurial or managerial efforts of others continue to contain the hallmarks of a security under U.S. law."

2. SEC comment letter to BTCS Inc[10]

   "We do not believe that the digital assets you hold meet the requirements in ASC 825 to permit application of fair value option. Based on your responses, we also understand that the digital assets you hold are not rights to cash or ownership interests in an entity. Therefore, it appears that the subsequent measurement of your digital assets is subject to the requirements for indefinite-lived intangible assets in ASC 350-30. We also note that your digital assets are not productive assets and therefore cash flows from their purchase or sale do not appear to meet the definition of investing activities. If our understanding is correct, please revise your financial statements accordingly."

Enable and use liquidity analysis and audited financials

- If institutional investors involved with crypto conducted thorough pre-investment analysis, and required audited financials, this would require their crypto counterparties to comply with normalized best practices without waiting for regulators to step in.

As the crypto market has both matured and experienced significant disruptions, some have questioned how and if valuation and risk assessment can be conducted for crypto transactions and assets. EY notably stated:[11]

[9] "Statement on Cryptocurrencies and Initial Coin Offerings", SEC Chairman, Jay Clayton, December 11, 2017.
[10] SEC letter, dated August 21, 2018, to BVTCS, Re: BTCS Inc., Amendment No. 6 to Registration Statement on Form S-1, Filed July 25, 2018, File No. 333-219893.
[11] "The valuation of crypto-assets," EY (2019).

> "In our view, a focus on determining fundamental value, based on traditional valuation techniques and principles, remains appropriate and applicable to these assets. Such techniques should consider the inherent volatility or riskiness of these assets, and are never more important than in times when market exuberance (and the base emotions of greed and fear) drive pricing."

Further, there has been a growing call for audits of crypto transactions and entities, beyond the traditional audits of publicly-traded entities that may hold or deal in crypto. While this raises the issue of how and what exactly to audit, the conversation is being had, and not solely by regulators.[12]

Conduct ongoing performance monitoring

- The entity who made the investment should be responsible for conducting its own ongoing financial performance monitoring of the crypto product/transaction and counterparty.
- The contracts should provide for regular financial statements that mirror those of similar traditional transactions, and for a legally enshrined right to inspect the books.
- Reliable fair value assessments of the crypto held, pledged as collateral, or otherwise used will be a key part of this analysis.

Ongoing performance monitoring, regardless of the underlying type of transaction, and regardless of whether it is conducted using crypto or fiat, is a given for most entities. However, in the case of crypto transactions, additional safeguards and expertise may be required. In fact, the Bank of England's Prudential Regulation Authority (PRA) directly acknowledges this for those companies that fall under its prudential framework, including:[13]

> "In 2018 I wrote to the CEOs of banks, insurance companies, and designated investment firms to remind them of relevant obligations under PRA Rules, and to communicate the PRA's expectations regarding firms' exposures to cryptoassets.
>
> As I noted in 2018, for firms operating in these areas, crypto risks should be considered fully by the board and the highest levels of executive management. In particular, an individual approved by the PRA to perform an appropriate Senior Management Function (SMF) should be actively involved in

[12] "The Need for Crypto Audit Standards," Forbes (May 29, 2022).
[13] "Dear CEO, Existing or planned exposure to cryptoassets," Bank of England, Prudential Regulation Authority (March 24, 2022).

> reviewing and signing off on the risk assessment framework for any planned business direct exposure to cryptoassets and/or entities heavily exposed to cryptoassets. Given the expansion in crypto activities being contemplated by firms, we are also undertaking a survey of firms' current and planned exposures over 2022.
>
> Firms will likely need to adapt existing risk management strategies and risk management systems to suit the different risk profile of many crypto activities. In particular, financial, prudential, operational, and reputational frameworks may need adjustment to reflect crypto activity risks. For instance, some activities may require more frequent monitoring, greater uncertainty factored into modeling or valuation, or lower risk tolerance levels than might typically be applied. Firms may also need to rely to a greater extent on proxies, and make more material assumptions about relationships between differing exposures. Given these uncertainties, firms should also consider the use of stress tests to provide greater confidence that risks are being captured."

In addition to the regular monitoring of performance and risk, crypto assets present an additional area for assessment and reassessment–i.e., that of the fair value of crypto held, used in transactions, or pledged (accepted) as collateral. The challenges of estimating a reliable and timely fair value, including any related impairment, are readily acknowledged by the crypto industry, and its auditors, regulators and standard setters:

> "The more time that passes between the initial transaction date and the measurement date, the less relevant the initial transaction price might become."[14]
>
> "Credit risk: There would be potential challenges in credit risk management associated with the use of crypto-assets as collateral for lending, due to potential price volatility and illiquidity. These challenges would need to be well managed, with a focus on the accuracy and reliability of valuations, the calculation of provisioning levels, and the ability to claim on the security if needed."[15]

Clarify collateral, custody, and segregation of assets

- Applying traditional financial collateral and its processes could be transformative for the maturation of the crypto finance ecosystem i.e., custody

[14] "Cryptographic assets and related transactions: accounting considerations under IFRS," PwC (December 2019).
[15] "Crypto-assets: Risk Management Expectations and Policy Roadmap," Australian Prudential Regulation Authority (April 21, 2022).

should be clear, the pledged assets should not be commingled with corporate assets, and the security interest should be carefully documented so that the lenders are adequately protected.

The concepts of collateral, custody, and segregation of assets are regular features in traditional financial arrangements. They all also are present in similar crypto transactions. However, additional clarity is needed in a crypto setting because some key aspects may be different due to the decentralized nature of the financial arrangements or the fact that the custody of the collateral is less clear. As a result, participants in these transactions will benefit from more structure and stronger due diligence:[16]

> "Lenders must clearly delineate the rights held by the borrowers in their cryptocurrency serving as collateral throughout the crypto-loan term. Many options are available to the parties depending on whether a borrower is comfortable putting its cryptocurrency under the care of a trustee or a custodian, with limited to no access, or if it wants to continue to use it in some way or another. There are also advantages for the lenders should they set up a trustee or custodian structure, since in doing so they obtain control over the collateral and gain the possibility of earning yield revenues on the cryptocurrency deposits under their management, on top of earning the usual interest payments and credit fees.
>
> Thorough due diligence is also very important. Before granting credit facilities to a borrower, lenders must take steps to ensure all cryptocurrency wallets related to the collateral under the loan agreement are disclosed in sufficient detail. Due diligence also ensures the intended use of the collateral by the borrower is clearly set out and compliant with the terms of the loan agreement. Questions of due diligence should cover the ownership of cryptocurrency portfolios as well as all their business activities involving cryptocurrency, among other things."

Enhanced disclosure and Terms and Conditions (T&Cs)

- How crypto businesses handle customer assets should not be trade secret. By sufficiently disclosing risks and basic practices, providers will not only protect their customers, but also themselves.
- Promoting mature and easy to understand terms and conditions with fulsome disclosures provides customers a better understanding of the risk they are taking on.

[16] "Crypto lending: Legal implications for taking security interests in cryptocurrency", Norton Rose Fulbright (April 20, 2022).

The need to improve the quality of disclosure and information is regularly discussed within the crypto industry. Researchers from Duke University surveyed 76 industry experts in 2020 and found that 83% of them did not believe utility token issuers disclosed enough information to their stakeholders at that time.[17] Although focused solely on the Initial Coin Offering market, it is a telling metric. They further proposed seven recommendations for additional disclosure that ranged from key financial information to project progress indicators.

A fully mature market should not hide behind minimal disclosures that leave consumers "holding the bag" in the event of a negative downturn. As the crypto market continues to evolve, so too must the disclosures associated with projects, investments, and trading.[18] Regulatory framework developments across the globe will mostly likely include enhanced disclosure requirements. In the US, SEC Chair Gary Gensler has noted crypto's lack of disclosures and its effect on consumer's understanding of risk:

> "The investment public is not getting disclosures...When you make other asset purchases, we have this basic bargain, you the investing public can make your choices about what risks you take...There's supposed to be full and fair disclosure, and people aren't supposed to lie to you."

Terms and conditions often vary considerably across platforms, exchanges, and protocols, often for the same underlying type of crypto transaction. This lack of standardization can be confusing for consumers. Separately, it can lead to very different financial reporting outcomes for the same type of transaction, which only leads to further complications around financial analysis and performance monitoring. The variability and lack of clarity can also lead to confusion for investors, as to who truly owns the crypto asset, and where the risk lies in the event of theft, loss or bankruptcy. .

The SEC signaled the importance of these issues when it issued Staff Accounting Bulletin (SAB) 121, March 31, 2022. Although SAB 121 is only applicable to specific entities and their related transactions, the additional disclosures required could be indicative of the future direction of travel:[19]

> "For example, to the extent it is material, Entity A may need to provide disclosure describing the types of loss or additional obligations that could occur, including customer or user discontinuation or reduction of use of

[17] "Seven Disclosure Recommendations for Cryptocurrency and Utility Token Issuers," The FinReg Blog, Duke Financial Economics Center (June 25, 2020).
[18] "SEC Chain Gensler warns on investing in crypto after meltdown," https://news.yahoo.com/sec-gensler-warns-on-investing-in-crypto-185859765.html (May 16, 2022).
[19] SEC Staff Accounting Bulletin No. 121, 17 CFR Part 211 (March 31, 2022).

services, litigation, reputational harm, and regulatory enforcement actions and additional restrictions. A discussion of the analysis of the legal ownership of the crypto-assets held for platform users, including whether they would be available to satisfy general creditor claims in the event of a bankruptcy should be considered. Further, Entity A may need to provide disclosure of the potential impact that the destruction, loss, theft, or compromise or unavailability of the cryptographic key information would have to the [*sic*] ongoing business, financial condition, operating results, and cash flows of the entity. As part of this disclosure, Entity A should also consider including, to the extent material, information about risk-mitigation steps the entity has put in place (e.g., insurance coverage directly related to the crypto-assets held for platform users)."

Don't ignore operational risk

- Ultimately, you can't manage financial risk with technology that doesn't function as it was designed and as you need it to.
    - Frameworks such as the AICPA SOC (Systems and Organization Controls) 1 and SOC 2 help Service Organizations give assurance and add transparency for their customers when managing vendor risk.
    - SOC 1 reports evaluate a service organization's internal control over financial reporting.
    - SOC 2 reports evaluate additional risks such as those related to Availability, Security, Processing Integrity, Confidentiality, and Privacy.
    - Note, not all SOC audits are the same, so it's important to look not only at the reports but the reputation of the auditor performing a SOC audit and the comprehensiveness - a Type 1 is much less thorough than a Type 2 for example (each a SOC 1 and SOC 2 can be either Type 1 or Type 2).
- If the data that you use to calculate financial information is incomplete or inaccurate, then the results will not be accurate.
    - Data governance is a key indicator that the underlying data quality will meet the standards you expect it to.
    - Do not assume that the data you buy is accurate - make sure to do your diligence.

Conclusion

As crypto matures the ecosystem may need to start incorporating some of the principles found in traditional finance in order for the ecosystem to continue

growing. Having institutional quality solutions that allow for crypto businesses to incorporate these principles allows for greater confidence in crypto assets.

Lukka has built best-in-class data and software offerings to aid businesses in managing their risk when they interact with crypto finance. The firm offers fair value and impairment services through Lukka Prime and Lukka Enterprise Software making it possible to meet current accounting standards and better prepare financial statements for entities holding crypto. Lukka also offers data solutions like LDACS, that demystify an asset's primary purpose and use case, as well as Lukka Reference Data, which offers a comprehensive set of security masters from exchanges and other sources across the crypto ecosystem that standardizes crypto-asset names, tickers, trading pairs, and more.