Bringing Blockchain Due Diligence into Focus Alongside Uptick in Strategic Dealmaking

SCOTT BENNETT, BENJAMIN GRUENSTEIN, DAVE KAPPOS, EVAN NORRIS, RYAN PATRONE, ELAD ROISMAN AND SASHA ROSENTHAL-LARREA, CRAVATH

JASON TRAGER, FTI TECHNOLOGY

Renewed momentum surrounding blockchain and digital assets indicates that the space is returning to a more stable trajectory. Following a slowdown in industry deal volume in the second half of 2022 and 2023, signals now point toward growth in joint ventures and mergers and acquisitions ("M&A") activity for the year ahead.

This activity is expected to include consolidation in certain digital asset sectors and renewed organic and inorganic investment by traditional financial players in the digital asset space through the remainder of 2024 and into 2025. There will likely also be an uptick in investments and strategic partnerships. Organizations in industries such as entertainment, telecommunications and retail may also increasingly look to develop blockchain and web3 platforms for a range of customer offerings and new business models, spurring further adoption of use cases outside the financial sector.

Still, TradFi institutions and other organizations looking to grow and invest in the digital asset space will do so in the face of lingering worries over the business and legal uncertainty as well as regulatory scrutiny that will likely persist throughout this developing industry, particularly in the United States. Such uncertainty and scrutiny underscore the importance of conducting robust technical, legal and business due diligence to evaluate risk and alleviate concerns in major strategic deals.

With the possibility of enhanced scrutiny, it is imperative that parties looking to enter the digital asset space through acquisitions, joint ventures or other strategic transactions understand the relevant technologies and markets as deeply as possible. This means analyzing the current state of the business and its historical conduct, including its relationship to digital assets and the concentration of its assets, as well as possible regulatory issues.

Given the commercial, regulatory and technical complexities involved in the digital asset space, devising a diligence plan and conducting due diligence require specialized expertise from outside counsel, consultants and accountants who understand the industry's nuances. These advisors will help acquiring companies examine commercial risks that arise in this sector, such as the commingling of customer assets, loss or compromise of digital keys, market volatility and the potential for manipulation or illicit activity. They will also clarify the potential opportunities and benefits of a target's strategy (*e.g.*, faster transactions, increased transparency, efficiency and improved accessibility) so they can be adequately

leveraged. While the involvement of experts is critical for any acquiring company, organizations outside of the digital asset space are likely to have less familiarity with the industry and therefore require more guidance throughout the diligence process.

With the support of the right experts and an understanding of industry nuances that may arise, dealmaking teams should evaluate the following key elements as part of conducting robust due diligence for blockchain and digital asset deals.

A. INTELLECTUAL PROPERTY RIGHTS

Digital asset and blockchain protocols can raise complex copyright, trademark and patent questions. When examining potential target companies that are active in blockchain, digital assets and web3, buying organizations must consider the protections and contracts that targets have implemented around their intellectual property ("IP") to avoid inheriting infringements or investing in IP that may be or may become compromised.

A particular challenge of IP in blockchain projects is separating out IP owned by the target, IP owned by the holders of any digital assets developed by the target and IP owned by any relevant decentralized community (such as a decentralized autonomous organization, or DAO). Careful attention should be paid to the allocation of rights in each piece of IP to understand potential risks posed by various rights holders.

Understanding the technical structure of digital assets and the methods by which they are created and transacted is a business necessity. Buying organizations should examine the architecture of each asset and the relevant blockchain network to determine their suitability for targets' use cases. Proper due diligence should also include research on industry players who pose a potential threat to the IP of a target company.

Copyrights and trademarks

For diligence targets with image- and brand-driven digital assets—such as creators behind non-fungible token ("NFT") collections—acquiring parties should understand the possible copyright and trademark protections for such assets and ensure they are appropriately registered, including with the U.S. Copyright Office and U.S. Patent and Trademark Office ("USPTO"). Copyrights and trademarks serve different but synergistic functions when it comes to digital asset protection. Copyrights may be used to protect original works associated with an NFT, while trademarks offer an additional way to protect against forgeries and unauthorized monetization by third parties. Together, these protections build integrity for the collection and protect the project as a whole.

Beyond NFTs, blockchain technology consists of software and other content that may be copyrightable. Many blockchain projects rely on open-source software, so acquiring parties should carefully diligence the proprietary or open-source licensing schemes under which the target's software is developed. The presence of copyleft licenses, for example, may compromise the commercial potential of the technology.

Additional license schemes, including the Business Source License, which permits copying for only non-production purposes for a certain period and later converts to an open-source license within four years, have also gained popularity. Diligence teams should ensure that the target company's software development and usage comply with such licensing requirements and that the target's software products are adequately protected.

Patents

Certain blockchain technologies and web3 applications are also patent-protectable. Unlike traditional business methods, which are difficult to patent due to eligibility hurdles, blockchain technologies may be technical systems directed to more than an abstract concept and thus may be more likely to be viewed as patent-eligible subject matter when compared to TradFi business methods. The USPTO has granted more than 10,000 patents for blockchain-based inventions to date, and the number of patent infringement suits related to blockchain-related patents has also increased. Diligence teams should investigate and understand in depth the technical mechanisms, as well as the target company's patent portfolio, and, if any, anticipate any associated patent litigation risk.

B. DIGITAL ASSET GOVERNANCE & OWNERSHIP STRUCTURE

Custody and ownership of assets

Verifying assets under custody (or the claims that a target has made about the volume or value of assets it has under custody) is particularly challenging, as the process for doing so is different from standard approaches for validating individual ownership of currency and traditional assets. The diligence process must include validation of how custody has been defined, who has control of the assets on chain and off chain, the accounting processes involved and the governance controls around custodied assets. Doing so is typically a highly technical assessment of underlying infrastructure. Verifying the ownership of such assets may also prove to be particularly challenging for digital asset targets with products that focus on privacy or with complex organizational structures.

Technical considerations

The technical considerations that may be relevant to a due diligence team are fact specific and dependent on the company and the product or service at hand. Generally speaking, however, diligence teams should ensure that they have a clear understanding of the type of digital asset being offered, use cases for such digital asset, the methods by which outside users may interact with the asset, the asset's distribution system, the target's smart contract infrastructure, the programmability of such digital asset and any policies, protocols or internal controls limiting programmability and how the asset functions on the blockchain at a technical level, including its path from the target to the investor or end user.

C. REGULATORY COMPLIANCE

Diligence teams should assess whether a target's compliance teams, policies, procedures and tools are adequately robust to ensure compliance with applicable regulatory requirements. Depending on an organization's industry, operations and location, it may be subject to an array of federal, state and foreign regulatory requirements. These requirements could include, among other things, obligations arising under securities and commodities laws, sanctions restrictions, transaction monitoring requirements, anti-money laundering ("AML") and know-your-customer ("KYC") controls, anti-fraud and corruption measures and data security requirements. Of course, each target organization is different, and it is important that diligence teams consult with counsel to determine which of these requirements may apply in a specific instance.

U.S. securities laws

A common issue facing target companies in this space is whether the digital assets related to their business are securities, and, if so, whether those digital assets have been offered or sold in violation of securities laws and whether the target companies have violated securities laws. Without adequate compliance with the applicable securities laws, web3 target companies may be subject to a number of legal issues and potential liability, including from regulators.

The U.S. federal securities laws apply to the initial offering and sale, as well as subsequent offers and sales, of digital assets if such digital assets are securities. Whether a digital asset is a security under the Securities Act of 1933 generally depends on whether the digital asset is an investment contract. A digital asset is generally considered a security by virtue of being an investment contract if it satisfies the four-prong test that the U.S. Supreme Court articulated in its landmark 1946 decision, *SEC v. W.J. Howey Co.*[1] The *Howey* test applies to any contract, scheme or transaction, regardless of whether it resembles a traditional security.

The Securities Act establishes a transaction-based, mandatory disclosure regime designed to provide investors material information relating to securities offerings that do not fit within specified exemptions. The Securities Act makes it unlawful for issuers to offer or sell securities, including digital assets that qualify as securities, unless the offer and sale: (i) is pursuant to a registration statement filed with the U.S. Securities and Exchange Commission ("SEC") or (ii) qualifies for an exemption from registration. Additionally, under the Securities Exchange Act of 1934, certain issuers of securities must file periodic disclosures with the SEC. These disclosures are designed to provide investors material information about the issuer, including its financial condition, operations and governance.

Moreover, in the United States, a digital asset platform that offers trading in digital asset securities and meets the definition of an exchange must either register with the SEC as a national securities exchange or operate pursuant to an exemption from registration, including as an alternative trading system.

---

1 328 U.S. 293 (1946). Under *Howey*, a non-traditional asset (such as a digital asset) is a security if: (i) there is an investment of money, (ii) in a common enterprise, (iii) with the expectation of profits, (iv) to be derived from the efforts of others. All four factors must generally be met to be classified as a security. *See also Reves v. Ernst & Young*, 494 U.S. 56 (1990) (resulting in the so-called "Reves test", infrequently applied to digital assets in comparison with *Howey* but relevant to certain digital assets that resemble "notes").

The current chair of the SEC has stated (but not speaking on behalf of the SEC) his belief that "of the nearly 10,000 tokens in the crypto market . . . the vast majority are securities."[2] Recent enforcement actions and guidance by the SEC highlight the agency's focus on tokens and digital assets, although there have been entities that have challenged its authority and jurisdiction in court.[3] A comprehensive regulatory framework specific to digital assets offered, sold or resold in the United States, or to persons in the United States, does not exist. Instead, U.S. regulators apply traditional regulatory and legal frameworks to digital assets. Such frameworks require fact-specific analysis, which generally leaves market participants to gauge adequate compliance based on prior regulatory or judicial determinations and regulators' public statements.[4]

Given the status of the digital asset markets, issuers of digital assets may be subject to a number of legal issues and potential liability, including from SEC enforcement. These issues could include individual liability and monetary damages, as well as operational impediments caused by orders to cease and desist from further violations of U.S. securities laws and regulations. It is crucial for diligence teams to validate a digital asset issuer's compliance with the U.S. securities laws and regulations as well as assess compliance for those that provide services to the issuer if, for example, they are distributing tokens on behalf of the issuer.

In addition, targets may have financial commitments or other obligations to early investors, such as obligations pursuant to simple agreements for future tokens or equity. Prior transactions, previous or planned initial coin offering activity and prior associations are likely to impact deal terms and deal value, and sometimes even viability. Understanding these early in the process is critical to supporting risk mitigation, accurate valuation and negotiations.

Commodities laws

Diligence teams should similarly take care to ensure that companies trading in digital asset commodities or derivatives are in compliance with the rules and regulations governing such instruments. The Commodity Futures Trading Commission ("CFTC") regulates U.S. derivatives markets, including the trading of certain commodity derivatives products such as futures, options or swaps. Certain digital assets, including some virtual currencies, may qualify as commodities under the Commodity Exchange Act of 1936, which is enforced and administered by the CFTC.[5] Individuals, firms and exchanges engaged in commodities derivatives trading must adhere to Commodity Exchange Act requirements, including registration as a regulated exchange or intermediary.

---

2 *See https://www.sec.gov/news/speech/gensler-sec-speaks-090822.*

3 *See, e.g., SEC v. Ripple Labs, Inc.*, Case No. 1:20-cv-10832-AT-SN (S.D.N.Y. July 13, 2023) (holding that the *Howey* test was not met where a digital token was sold programmatically, *i.e.*, via a trading algorithm, on a blind bid/ask basis—where the purchaser did not know the seller and the seller did not know the purchaser—or where the token was distributed as compensation in exchange for services).

4 For example, some market participants have sought No-Action Letters from the SEC's Division of Corporation Finance requesting confirmation that the offer or sale of a given digital asset will not violate U.S. securities laws (or have structured their digital assets conservatively to ensure they fit within the parameters of existing SEC No-Action Letters).

5 The Commodity Exchange Act defines "commodity" broadly to include all "goods and articles, … and all services, rights, and interests … in which contracts for future delivery are presently or in the future dealt in." 7 U.S.C. § 1a(9). Generally, the CFTC's regulatory jurisdiction is limited to derivatives—the agency's authority over the underlying commodity (spot) is limited to anti-fraud/manipulation.

The CFTC has exercised its enforcement authority after determining that trading in certain digital assets is subject to its authority. Additionally, federal district courts have held that some digital assets, including certain cryptocurrencies, are commodities subject to CFTC jurisdiction. Acquiring parties should investigate whether target companies that trade digital assets are subject to the Commodity Exchange Act and CFTC rules and regulations.

The Bank Secrecy Act and AML obligations

Under the Bank Secrecy Act, web3 companies may be required to implement controls to ensure that their digital asset platforms are not exploited for money laundering or terrorist financing. Diligence teams should determine whether a target is required to comply with the Bank Secrecy Act and, if so, ensure that adequate AML protections are in place.

The Bank Secrecy Act requires financial institutions to implement an AML program that includes KYC procedures and various reporting and record-keeping requirements. Financial institutions subject to the Bank Secrecy Act are required to implement adequate measures to verify customer identities, monitor transactions and report suspicious transactions. A compliant AML program must be in writing and include, at minimum, (i) the development of internal AML policies, procedures and controls; (ii) a designated compliance officer; (iii) an ongoing employee training program; and (iv) independent audits to ensure the program functions adequately.

In addition to traditional banks, broker-dealers and futures commissions merchants, the Bank Secrecy Act's definition of financial institutions applies to "money services businesses", a type of non-bank financial institution that includes money transmitters ranging from remittance providers to centralized digital asset exchanges.[6] In 2019, the U.S. Treasury Department's Financial Crimes Enforcement Network ("FinCEN"), the agency with primary enforcement responsibility for the Bank Secrecy Act, published a detailed guidance titled, "Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies." Under that guidance, money transmitters include exchangers, which exchange virtual currency for real currency or other virtual currency, and administrators, which have authority to put into or withdraw virtual currency from circulation.[7] With limited exceptions, money transmitters are required to register as money services businesses with FinCEN and have the same reporting, record-keeping and AML obligations as other financial institutions.[8]

Over the last few years, FinCEN and the CFTC have brought multiple enforcement actions against web3 companies for alleged violations of the Bank Secrecy Act, including for failure to implement an adequate AML program and failure to register as a money services business, regulated exchange

6 The Bank Secrecy Act obligations of money transmitters under FinCEN rules arise independently of Bank Secrecy Act obligations of certain businesses subject to SEC and/or CFTC jurisdiction (*e.g.*, broker-dealers and futures commissions merchants). Diligence teams should consider whether a target is required to have implemented an adequate AML program under any of these bases.

7 FinCEN Guidance, "Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies," at 13 (May 9, 2019).

8 FinCEN, "Interagency Interpretive Guidance on Providing Banking Services to Money Services Businesses Operating in the United States," at 2 (Apr. 26, 2005).

or intermediary. The U.S. Department of Justice has also brought criminal charges against officers of companies that willfully failed to register as a money services business and implement adequate AML programs.

Given regulatory scrutiny of AML programs in this industry, diligence teams should assess whether a target is or may be subject to regulation by federal or state agencies. Where such obligations exist, due diligence teams should ensure that such targets have met any registration, record-keeping and AML obligations. Where appropriate, diligence teams may need to conduct an AML risk assessment, investigate customer due diligence procedures and review the use of proprietary or in-house blockchain analytics tools.

That said, significant uncertainty remains as to how AML principles apply to digital assets services. Due diligence teams should take particular care to validate the claims of a target that holds itself out as exempt from Bank Secrecy Act obligations. Some targets may rely on geo-blocking to exclude U.S. customers and thus avoid U.S. jurisdiction. In such instances, diligence teams should ensure that the geo-blocking measures are effective at restricting access by U.S. customers, including those using virtual private networks or anonymizing browsers. Given this regulatory uncertainty, acquirors should be especially diligent to understand the technical underpinnings of target companies and assess whether they may give rise to regulatory obligations. If so, diligence teams should ensure that targets have implemented adequate AML and customer due diligence procedures.

U.S. sanctions

Blockchain technology can help accelerate the distribution of digital assets across global markets. With such a potential for global reach, compliance with U.S. sanctions laws should be a key focus for acquiring parties. The U.S. currently maintains comprehensive sanctions against Iran, North Korea, Syria, Cuba and the Crimean, Donetsk and Luhansk regions of Ukraine, as well as extensive, though not comprehensive, sanctions on individuals and entities in Venezuela and Russia. These sanctions are administered and enforced primarily by the U.S. Treasury's Office of Foreign Assets Control ("OFAC"). OFAC also has authority to designate individuals and entities as Specially Designated Nationals pursuant to U.S. sanctions, antiterrorism and anti-drug-trafficking laws. Although each sanctions program differs, U.S. law generally prohibits U.S. persons from engaging in transactions, directly or indirectly, that involve a person or entity in a sanctioned country or on the Specially Designated Nationals list. U.S. law also generally prohibits individuals and entities (including non-U.S. persons) from facilitating, or causing a U.S. person to engage in, a prohibited transaction.

OFAC has made clear that the agency views its sanctions authorities as applying with full force to web3 systems and transactions. OFAC has thus put even highly decentralized platforms on notice that, in the agency's view, the services offered by such platforms must comply with U.S. sanctions, antiterrorism and anti-drug-trafficking laws.

Due diligence teams should ensure that targets are also in compliance with such laws. For instance, where appropriate, diligence teams will want to review the robustness of a target's transaction monitoring program and how rapidly it responds to alerts, as well as evaluate its methods to blacklist addresses and procedures for mandatory reporting.

D. POTENTIAL CONTINGENT LIABILITIES

Without adequate attention to identifying and evaluating contingent liabilities, acquirors may inadvertently buy into hidden risks. Such risks can arise from a target's failure to comply with the regulatory requirements described above, which can lead to investigations of or proceedings against the target. Similarly, the target's contracts can be another source of potential contingent liabilities and, in extreme cases, can even have material impacts on the acquiror's existing businesses.

Regulatory issues

Diligence teams should determine whether a potential target is subject to regulatory oversight or is likely to invite regulatory scrutiny, including investigation. Acquisition targets may be subject to ongoing investigations by regulators, among them the SEC, CFTC, OFAC, FinCEN and state regulators like the New York Department of Financial Services, for potential legal and regulatory violations. A target may also become involved as a third party in investigations and proceedings between a regulator and another company. In the course of these investigations, regulators may request company documents, witness interviews and written responses to questions. The subjects of these investigations may need to dedicate substantial resources to comply with the requests, cooperate with regulators and minimize legal and financial risks.

Regulatory investigations may result in decisions by regulators to commence enforcement actions in administrative proceedings or in federal or state court. These actions implicate the risk of sizeable judgments and, where willful misconduct is involved, criminal liability. As with regulatory investigations that publicly settle, public court filings and orders may also carry reputational risks.

If diligence teams determine that a potential target is or is likely to be subject to regulatory scrutiny, diligence teams should request to meet with counsel for information about any investigation or inquiries from regulators as well as facts learned by the company from internal reviews. Additionally, diligence teams should also determine whether any agreements to toll applicable statutes of limitations are in place. Based on the information they receive, diligence teams should assess the potential financial, legal and reputational risks associated with any ongoing investigations.

Litigation

Litigation risks that apply to traditional targets also apply to targets in the digital asset space. This is true for web3 companies, including highly decentralized companies, even when they do not fit the traditional corporate mold. Additionally, judicial orders that result from litigation initiated by regulators can have serious collateral consequences for a business's ability to operate. Depending on the business, potential targets may also face class action litigation.

Diligence teams should thus inquire about any potential or ongoing litigation involving the target and assess the potential outcomes, risks, consequences and likelihood of a material impact on such target's financial performance, reputation, legal status or operations.

E. CONTRACTS

Acquirors should take care to review material contracts and agreements of a target company, regardless of its industry, to identify any risks or potential liabilities arising from such contracts and agreements. In addition, a target's contracts may contain provisions that are implicated by the contemplated transaction or, in extreme cases, may have material impacts on the acquiror's existing business.

Legal contracts

In order to assess if any potential liability exists related to a potential or ongoing breach of contract or counterparty dispute, an acquiror's diligence team should inquire as to whether there are any existing, expected or alleged contractual breaches by the target company or any disputes between the target company and any of its counterparties. Due diligence teams should also request and review a target company's material contracts and agreements.

As part of this review, an acquiror's diligence team should focus on (i) any contractual provisions that may be implicated as a result of the acquiror's contemplated transaction, including change-of-control or anti-assignment provisions; and (ii) any contractual restrictions that could undercut the strategic rationale for the contemplated transaction and/or are drafted so broadly that, by their terms, they could apply to the acquiror's existing business. At the outset, it is crucial that diligence teams understand the nuances of the proposed transaction structure, the scope of the acquiror's existing business and the acquiror's plans for the target's business after the proposed transaction is completed, as each of these will influence the type of contractual provisions that may be implicated by, or have a material impact on, the proposed transaction.

Smart contracts

Target companies in the digital asset space often use smart contracts in their business operations. A smart contract is a set of functions in code built on top of and secured by blockchain technology that can execute "agreements" without human intervention. These "agreements" are effectively self-executing if-then programs—if a predetermined thing occurs, the smart contract will automatically execute a predetermined action. Acquirors should assess the validity and feasibility of smart contracts, as well as the underlying risks and vulnerabilities in the participants and infrastructure of the target's smart contracts.

F. TOP EXECUTIVES AND KEY PERSONNEL

Headline cases in the digital assets industry over the past two years have underscored just how much the missteps and misconduct of high-ranking individuals can expose a company and its investors. Evaluation of the culture, behaviors and governance decisions of the people in power within a target is a critical step in the diligence process.

G. CORPORATE STRUCTURE

Companies in blockchain and digital assets industries will often build and fund or otherwise have associations with entities that exist solely to support a specific blockchain ecosystem. Without proper diligence, this can bring exposure to unforeseen legal risks. Consideration should be given to any foundations, DAOs and other third-party partnerships a target is involved in to ensure those activities are managed with appropriate attention to governance, compliance and contractual obligations.

Organizational documents

In this space, a target's organizational structure may be more complicated than a traditional organizational structure, as potentially complex digital asset distribution structures may create the need for sub-governance entities (*e.g.*, DAOs) and more complicated legal structures (*e.g.*, offshore entities, legal wrappers). Particular attention should therefore be paid to the form of corporate entity (*e.g.*, C-Corporation, Limited Liability Company); the jurisdiction in which a parent company and any subsidiaries, if applicable, have been formed; and the existence of any sub-governance entities.

Compliance paradox

Centralized governance assists with compliance, yet it raises concerns under securities laws. As discussed, digital assets that are determined to be investment contract securities under *Howey* are required to be registered with the SEC or otherwise qualify for an applicable exemption. Digital asset creators may be incentivized to decentralize their corporate structures in order to seek to avoid the need for SEC registration (or exemption), among other reasons. However, per The Bank Secrecy Act and AML obligations, certain compliance regulations may require digital asset protocols to conduct KYC checks and screenings, which could require some degree of centralization. Moreover, decentralization may in some circumstances make a target less attractive to a strategic acquiror from a business perspective. It is important for diligence teams to be aware of these potential issues and understand both legal and business risks.

CONCLUSION

Depending on the outcomes of a diligence exercise, acquiring institutions and investors may need to make adjustments to their plans. The implications of due diligence findings may include adjustments or potential adjustments to purchase price, changes to the acquisition contract (*e.g.*, reps, disclosure, covenants, conditions, termination provisions, indemnities), modifications of transaction structure and/or adjustments to the roadmap for integration and post-closing operations.

Any legal team familiar with the M&A process understands the importance of due diligence. In deals within the digital asset space, additional complex and technical considerations, each requiring close attention, are introduced. Conducting a detailed, expert-led technical and legal examination of potential risks and the nuances unique to digital assets companies and models will position acquiring companies and investors to avoid surprises and enhance the ultimate value of the deal.

Cravath, Swaine & Moore LLP

NEW YORK

Two Manhattan West
375 Ninth Avenue
New York, NY 10001
T+1-212-474-1000
F+1-212-474-3700

LONDON

CityPoint
One Ropemaker Street
London EC2Y 9HR
T+44-20-7453-1000
F+44-20-7860-1150

WASHINGTON, D.C.

1601 K Street NW
Washington, D.C. 20006-1682
T+1-202-869-7700
F+1-202-869-7600