Crypto M&A: Current trends and unique legal and regulatory considerations

Dario de Martino & Mara Goodman
Allen & Overy LLP

Abstract

An overview of current trends and unique legal and regulatory considerations in crypto M&A.

Introduction

Despite crypto winter settling in and crypto prices and sentiment being down by more than 75% from their peak in 2021,[1] M&A activity in the crypto space has remained strong.[2]

While most transactions in this space are private, and their terms are confidential or otherwise not material enough to be publicly disclosed, the data available indicates that there have been approximately 764 crypto-related M&A transactions globally since 2013, with about 88 in the first seven months of 2022.[3] It is anticipated that the total estimated value of transactions in 2022 will be roughly $8 billion.[4]

While the crypto winter has brought challenges to the crypto market, unique opportunities and new trends will continue to support crypto M&A, including cross-border M&A, through the foreseeable future.

Trends in crypto M&A

In 2022, a couple of key trends have emerged: first, challenging crypto markets have pushed companies to maximise value in distressed times; and second, increasing interest in the "metaverse"[5] has led established businesses to boost their presence in the digital realm through M&A, particularly involving companies focused on non-fungible tokens ("NFTs").[6]

Transaction strategies in challenging crypto markets

Market players with large cash reserves have indicated interest in using their cash on hand to help troubled crypto firms make it through the current challenging market.

Meanwhile, crypto companies like Voyager Digital and its subsidiaries have sought bankruptcy protection in the hope of finding an acquirer, or alternatively, finding a way to restructure without one.

Other troubled crypto firms may seek different solutions. For example, an acquirer may consider:

- purchasing all of the equity of a distressed target through a stock sale or merger or, alternatively, looking to acquire all or a limited pool of the assets of a troubled or distressed crypto firm;
- conducting an "acqui-hire" wherein the acquirer engages in a purchase transaction principally to acquire the distressed seller's skilled workforce;

- acquiring a distressed seller's technology, in some cases through a licence or an option; or
- engaging in a "loan to own" transaction in which the acquirer advances funds on a secured loan basis to give it the opportunity to take the "pole position" in connection with any future distressed sale.

Despite the stock market volatility and its underlying causes (including rising interest rates, disconnects in supply chain, rising inflation, the ongoing invasion of Ukraine, recession fears, and the upcoming elections), we are still seeing noteworthy transactions in this space; companies are still seeing deal-making benefits, and the strategic trends driving crypto M&A activity are not likely to weaken in the rest of 2022. If the lower valuations reflected by the stock market decline continue, buyers are likely to become more acquisitive to take advantage of multiples that are lower than they have been in recent years. For sellers, turbulent capital markets will encourage companies to continue to re-evaluate their strategic plans and consider whether to sell or spin-off non-core or underperforming assets. Stock price declines may also empower activist investors to demand companies' spin-off businesses to unlock value and improve shareholder returns.

Emerging M&A in the NFT market

Although the NFT market is relatively new, we are now seeing an increasing range of established and emerging businesses across sectors circle this market looking for new opportunities from big corporations seeking to reward loyal customers, obtain access to new cult-like communities, or create a link between real-world assets and the metaverse to emerging artists creating new royalty structures or revenue-sharing models to better monetise their original content.

For example, on December 13, 2021, Nike announced its acquisition of RTFKT, a company that creates virtual sneakers and other collectibles in the form of NFTs.[7] Earlier last year, RTFKT – in a collaboration with the digital artist FEWOCiOUS – sold 600 real sneakers paired with virtual ones (which were released as NFTs) in just seven minutes, generating $3.1 million.[8] John Donahoe, Nike's President and CEO, stated that "this acquisition is another step that accelerates Nike's digital transformation and allows us to serve athletes and creators at the intersection of sport, creativity, gaming and culture".[9]

In the same month, Adidas, one of Nike's biggest competitors, announced partnerships with NFT project Bored Ape Yacht Club, GMoney and PUNKS Comic.[10]

These efforts by Nike and Adidas to establish presence in popular digital ecosystems demonstrate how established companies are refocusing their investment and M&A strategies on NFTs to capture younger consumers and avoid becoming the next Kodak.

Special-purpose acquisition companies ("SPACs") also began getting into the game in 2021.

Getty Images announced on December 10, 2021 that it would merge with CC Neuberger Principal Holdings II, a SPAC formed through a partnership between CC Capital and Neuberger Berman.[11] Getty Images' CEO has discussed publicly that the company's plans for growth include pursuing opportunities in the NFT market.[12]

Also in December 2021, Infinite Assets (also known as "InfiniteWorld"), a metaverse infrastructure platform, announced that it will merge with Aries I Acquisition Corporation, a SPAC.[13] Among other things, InfiniteWorld provides companies with the infrastructure they need to create NFTs.[14]

2022 has also seen significant M&A activity in the NFT market.

Notably, on January 18, 2022, OpenSea acquired Dharma Labs, a company focused on simplifying the process of on-ramping from fiat currency into crypto.[15] Despite more

competitors emerging, OpenSea remains the highest-capitalised NFT marketplace, by transaction volume, and reducing barriers from fiat currency to NFTs will likely help secure additional users.

In addition, on March 11, 2022, Yugo Labs, the creator of Bored Ape Yacht Club, announced its acquisition of the intellectual property ("IP") of the CryptoPunks and Meebits collections from Larva Labs.[16] The acquisition gives Yugo Labs control over three of the most popular NFT collections on the market.[17]

We anticipate increased M&A activity in the NFT market during the rest of 2022 and into 2023, including consolidation among platforms and marketplaces that facilitate the trade of NFTs.

Unique legal and regulatory considerations

Blockchain targets present a host of complex legal and regulatory issues and, accordingly, due diligence has increased in importance. Blockchain companies often operate in international markets. Therefore, due diligence investigations should take into account the target's potential plurality of legal regimes, local norms and applicable practices. Among other things, prospective acquirers may wish to see evidence of compliance, such as copies of licences, as well as policies and procedures to mitigate regulatory risks. Prospective acquirers may also wish to speak with key personnel at the target company regarding compliance. While no publication can provide an in-depth analysis of all the issues that might be relevant to crypto M&A transactions, the following are key legal and regulatory due diligence issues worth considering in the crypto M&A space.

U.S. federal securities laws considerations

As an entirely new type of property, often existing independent of any legal entity issuer, and capable of being deployed to perform a wide range of functions, digital assets defy traditional categories.

While they may feature elements that are seemingly characteristic of securities, commodities and a means of exchange, they are also capable of embodying creative works, performing decentralised functions and executing simple contracts.

One might assume that the word "security" is clearly defined in the law, but unfortunately, it is not.

The definition of what constitutes a "security" found in the Securities Act of 1933 ("Securities Act") and the Securities Exchange Act of 1934 ("Exchange Act") includes traditional instruments issued by legal entities, including as stocks and bonds, as well as the less familiar term "investment contract".

In 1946, the Supreme Court decided *SEC v. Howey*, which provided greater substance to the meaning of this term, but little that anticipated the advent of digital assets. In a case involving the ownership of orange groves combined with service contracts to cultivate and sell the resulting products, the Supreme Court found that the sale of the orange groves together with the means by which to develop the product thereof constituted an "investment contract" and therefore a "security" within the meaning of that term under the Securities Act.

In 2017, the U.S. Securities and Exchange Commission ("SEC") clarified that it would apply the *Howey* test to determine whether digital assets are securities.

In 2019, the SEC published a rather detailed framework[18] for how to determine an investment contract in the context of digital assets. While this framework was helpful guidance, it

created a test under which both the enterprise to cultivate oranges and the resulting oranges would likely be deemed securities.

Typically, a developer issues digital assets or the right to acquire digital assets to fund the further development of the underlying assets. While that schema undoubtedly constitutes an investment contract, many have argued that the SEC's conclusion that the resulting digital assets are securities is rather like concluding that oranges from the Howey groves constituted securities.

In *Howey*, the Supreme Court recognised the need to scrutinise the arrangement, rather than the assets that underlie such arrangement, to determine whether it was an investment contract. The key term is "investment contract", and the inclusion of the word "contract" means that there must be an arrangement, i.e., not every product of an investment contract should be deemed a security.

Often digital assets represent no ownership of a business and no claim on the revenues, income, or assets of the resulting enterprise, although their existence and functionality may have benefitted from the work of the enterprise.

The analytic challenge is aggravated because the Securities Act (and the related Exchange Act) is premised on the assumption that all securities are issued by legal entities.

The result is that if tokens are "securities", there is no path to regularising trading of such interests.

If we continue to apply the *Howey* test, and the related framework, to any asset produced by the subject arrangements or enterprise, then we would need to apply it to other things, such as frequent flyer miles, loyalty points, etc., which would lead to indefensible results.

Interestingly, the SEC staff has determined that only two truly decentralised cryptocurrencies, Bitcoin and (albeit with some less enthusiasm) Ether, are not investment contracts and therefore not securities. In making this determination, the SEC staff emphasised the importance of decentralisation in determining whether a token should be considered a security, stating "[i]f the network on which the token or coin is to function is sufficiently decentralized—where purchasers would no longer reasonably expect a person or group to carry out essential managerial or entrepreneurial efforts—the assets may not represent an investment contract".

However, no helpful guidance has been offered to define or achieve "sufficient decentralisation", leaving market participants in a conundrum.

Fortunately, there is increasing discussion of legislative action in this area, which might distinguish between the promotion of schemes to develop digital assets and the resulting digital assets (provided that they do not independently represent third-party obligations).

To note, on June 7, 2022, Senator Kirsten Gillibrand (D-NY) and Senator Cynthia Lummis (R-WY) introduced the Responsible Financial Innovation Act ("RFIA"), a highly anticipated legislative proposal that, if enacted by Congress and signed into law, would establish a comprehensive regulatory framework for digital assets in the United States. Although it is highly unlikely to become law before this congressional session adjourns on January 3, 2023, the RFIA[19] – if enacted – would, among other things, introduce several digital asset-related definitions and introduce the concept of "ancillary asset", which would be an asset presumed not to be a security if specified periodic disclosure requirements are satisfied.

There is also the possibility that U.S. courts might resolve the quandary, but it is difficult to discern the ultimate path out of the current uncertainty.

The urgency of such measures is amplified by the failure of several intermediaries and the resulting harm to market participants from the lack of regulatory clarity. While the SEC might argue that this results from the refusal to acknowledge the character of many digital assets as securities, its interventions in the markets have neither been constructive nor laid out a clear path that reflects the very different characteristic of many digital assets from securities.

Nevertheless, currently, the lack of clear regulatory standards for determining whether a digital asset is a security limits the ability of crypto companies to ensure that they are not transacting in securities, and exposes them to second-guessing by the SEC and private plaintiffs.

If a blockchain target failed to comply with applicable securities rules and regulations, the SEC may investigate and prosecute alleged fraud in connection with such offerings, which may lead to civil penalties for defendants, including individuals. Unregistered offerings may also be subject to rescission rights and damages claims as well as enforcement actions by U.S. state and/or non-U.S. securities regulators, which may result, and in some cases have resulted, in fines, injunctions and jail time in connection with potential related criminal proceedings.

Ultimately, potential acquirers should review the legal advice a target has received and speak with its outside counsel on these issues. They should also consider whether there are any remedial actions that can be taken before closing and otherwise conduct thorough due diligence investigations to avoid inheriting potential liabilities or having to address potential pitfalls post-closing.

Commodities regulation considerations

As noted, digital assets are not a homogeneous asset class; they may feature characteristics of securities, but also commodities, currency units, or a combination thereof. As a result, the legal analysis relating to a particular digital asset should not be limited to whether securities law is applicable, but instead include multiple regulatory regimes.

Indeed, a potential acquirer should be mindful that cryptocurrencies, whether or not determined to be securities, are treated as commodities (akin to precious metals or physical assets) by the United States. The Commodity Futures Trading Commission ("CFTC") takes the position that all varieties of cryptocurrencies are commodities for purposes of the Commodity Exchange Act.[20]

Acquirers should be aware that the CFTC has issued guidance expansively defining the scope of derivatives it regulates, especially in the case of leveraged or margined transactions involving retail investors, and has pursued cases involving even seemingly minor instances of wash trades and undisclosed proprietary trading in the spot markets.

Perhaps more importantly, however, by virtue of being deemed a commodity, cryptocurrency transactions imbue the CFTC with anti-fraud and anti-manipulation authority. As a result, even when securities law anti-fraud and anti-manipulation authority does not reach a particular transaction, commodities law authority does, and a potential acquirer should make sure to conduct a thorough analysis to avoid inheriting potential liabilities or having to address potential pitfalls post-closing.

Also, to note, the RFIA – if enacted – would designate the CFTC as the primary regulator of the digital asset spot market and create a new registration category for digital asset exchanges.

Federal and state money transmission considerations

In general, unless otherwise exempt, a licence is required to engage in the "business of money transmission" – i.e., to receive and transmit money – under the money transmission laws of each U.S. state in which a person has customers. Separately, a person who is

engaged in money transmission activity will generally also be deemed a money services business ("MSB") under the federal Bank Secrecy Act ("BSA"), and as a result, is subject to a registration requirement and related anti-money laundering ("AML") compliance programme requirements that are further addressed below.

The Financial Crimes Enforcement Network ("FinCEN"), which implements the BSA, has affirmed through guidance that certain activities involving virtual currency – including receiving and transmitting the same – are subject to the BSA requirements (even in cases in which the activity may not be subject to money transmission licensing in a particular state or states). The BSA also operates to reinforce compliance with state money transmission laws by making it a federal felony to engage in money transmission in a state without a required state money transmission licence in that state.[21]

FinCEN has issued extensive guidance on virtual currency activities that constitute MSB activities subjecting a person to the BSA. This guidance establishes that FinCEN interprets its regulations to apply to persons that are administrators or exchangers of virtual currency as "money transmitters". An exchanger is a person engaged as a business in the exchange of virtual currency for real currency, funds, or other virtual currency. An administrator is a person engaged as a business in issuing (putting into circulation) a virtual currency, and who has the authority to redeem (to withdraw from circulation) such virtual currency. An administrator or exchanger that (1) accepts and transmits a convertible virtual currency, or (2) buys or sells convertible virtual currency for any reason would be a money transmitter under FinCEN's regulations, unless a limitation to or exemption from the definition applies to the person.[22] Accordingly, the applicability of the BSA to a person's activities involving virtual currency is a fact-specific inquiry that must be addressed on a case-by-case basis.

A number of state money transmission statutes and regulations have been amended to address the regulation of virtual currency. Furthermore, even a state that has not established a formal, public position could conclude that virtual currency activity is covered by the money transmission law. Market participants should analyse the potential applicability to any particular virtual currency activity of state money transmission licensing laws, as well as any guidance, interpretations, enforcement actions or other rulings pertaining to state regulatory approaches to virtual currency activity, in order to assess whether the current or contemplated activity of the target would constitute regulated money transmission activity, or require licences under such laws.[23]

What constitutes unlicensed state money transmission activity involving Bitcoin was at the heart of a recent federal district court ruling in a criminal AML case suggesting that the transmission of virtual currency on behalf of another person requires a state money transmission licence even if the state's money transmission law does not expressly address the regulation of virtual currency.[24]

Although this case arises out of significant allegations of criminal AML activity, the court's interpretation of relevant laws appears to suggest a default assumption that money transmission licences are required to receive and transmit virtual currency. In addition, the ruling appears to suggest that other activity involving receiving and transmitting money, even if not historically subject to regulation under state money transmitter licensing laws, could be deemed to constitute engaging in unlicensed money transmission activity in the absence of a formal state interpretation to the contrary.

This interpretation has the potential to significantly disrupt current compliance approaches taken by some organisations engaging in virtual currency activity and could make challenging regulatory due diligence even tougher to perform. Acquirers should be mindful

of the fact that, under federal laws, anyone who knowingly conducts, controls, manages, supervises, directs, or owns all or part of an unlicensed money transmitting business could be fined or imprisoned for up to five years.

Finally, it is worth noting that, contrary to the approach suggested by some market participants, it is neither sufficient nor effective to locate a business offshore in order to avoid U.S. federal registration and related requirements or U.S. state licensing requirements. FinCEN regulations related to registration and AML compliance apply to an MSB "wherever located doing business, whether or not on a regular basis or as an organised or licensed business concern, wholly or in substantial part within the United States" and "includes but is not limited to maintenance of any agent, agency, branch, or office within the United States".[25] For example, in August 2021, FinCEN and the CFTC reached a resolution with BitMEX, an offshore cryptocurrency exchange that exists mostly in countries other than the United States, alleging that the company did not comply with AML obligations per the BSA, did not have any AML policies or procedures in place and did not conduct any customer due diligence.[26]

U.S. AML considerations

Under the BSA and its implementing regulations issued by FinCEN, a money transmitter engaging in virtual currency activity (or any other activity) that is deemed to be an MSB is required to: (a) register as an MSB with FinCEN; (b) establish and maintain an effective AML programme that is "reasonably designed to prevent the [MSB] from being used to facilitate money laundering and the financing of terrorist activities"; and (c) comply with certain record-keeping and reporting requirements – including suspicious activity reports ("SARs") and currency transaction reports ("CTRs").

Generally, an MSB's BSA/AML programme must be in writing and commensurate with the company's specific risk profile, i.e., the programme must be risk based and cannot be an off-the-shelf solution. At a minimum, an MSB's BSA/AML programme must: (a) include policies, procedures, and internal controls that are reasonably designed to ensure ongoing compliance with the BSA; (b) designate an individual responsible for the MSB's BSA/AML programme (a "BSA Officer"); (c) provide adequate BSA/AML-related training to all appropriate personnel; and (d) conduct independent (internal or external) testing.

Many MSBs also establish and implement policies and procedures specifically addressing the identification and verification of beneficial owners of legal entity customers.

An MSB that violates the registration requirement and BSA/AML programme requirements can face enforcement actions from regulators or law enforcement agencies, which may include severe monetary penalties. In addition, engaging in or aiding and abetting money laundering is a criminal offence under the U.S. Money Laundering Control Act ("MLCA") that is punishable by a maximum of 20 years in prison and fines of up to $500,000 or twice the amount of the transaction involved, whichever is greater. The MLCA applies to all persons and businesses in the United States as well as to persons and businesses in other countries if at least one part of a transaction is executed in the United States.

It is therefore of utmost importance for an acquirer of a business with virtual currency activities to conduct a thorough AML due diligence in order to determine: (a) whether the target is an MSB that is required to register with FinCEN and have a BSA/AML programme; and, if yes, (b) whether such programme is effective, adequate, and appropriate. We note that there may be additional state legal requirements with regard to an MSB's BSA/AML compliance programme. For example, there are the New York State Department of Financial Services' ("NYDFS") so-called "Part 504" requirements, which provide for minimum standards for transaction monitoring and filtering programmes and an annual compliance certification requirement for money transmitters that are licensed by the NYDFS.

In addition to the above U.S. legal requirements, many jurisdictions have similar statutory and regulatory frameworks in place. The following principles generally apply and should be considered for transactions involving foreign virtual money transmitters, as well.

The scope and thoroughness of an AML due diligence should be risk based, taking into account the target's risk assessment, all AML-related policies and procedures (including "know-your-customer" ("KYC") requirements, customer due diligence/enhanced due diligence, transaction monitoring and SAR filings, and other reporting and record-keeping requirements), independent testing reports and management responses, training materials, and the structure of the target's BSA/AML compliance department and the BSA Officer's roles and responsibilities.

Further, an acquirer should be mindful to include strong AML-related representations and warranties in any agreement. For effectiveness and efficiency's sake, an acquirer may want to consider combining the AML and sanctions due diligences and closely coordinating these activities.

Considering the legal and reputational risks for being associated with, or being involved in, (alleged) money laundering and terrorist financing activities, an acquirer should also strongly consider conducting at least a limited AML due diligence for any blockchain M&A transaction, even if the target is not directly involved in virtual currency and/or money transmitter activities.

Sanctions considerations

Sanctions refer to legal restrictions that governments impose on transactions with specific persons or entire jurisdictions (i.e., embargoes). U.S. sanctions are generally strict liability and carry steep fines (for most violations, the greater of approximately $300,000 or twice the value of the transaction). This creates significant risk for companies that operate in the blockchain space since digital assets may facilitate anonymous or pseudonymous transactions, such that blockchain participants could unwittingly engage in transactions prohibited by sanctions.

Many U.S. sanctions targets have attempted to use blockchain technology to either circumvent U.S. sanctions or engage in malign activity that U.S. sanctions target, and the Office of Foreign Assets Control ("OFAC"), the U.S. agency primarily responsible for implementing and enforcing U.S. sanctions, has taken an interest in cryptocurrency transactions. In September 2021, OFAC designated a Russian virtual currency exchange for facilitating financial transactions for ransomware actors.[27]

Targets that develop or use blockchain technology should be reviewed for sanctions controls and compliance, such as a process to collect identifying information on blockchain participants, and screen information against the Specially Designated Nationals and Blocked Persons ("SDN") List, as well as IP blocking. Additional controls to look for include permissioned blockchains that condition participation on users providing information about their off-chain identities (that can then be screened against the SDN List), or smart contracts that halt transactions when users add keywords to transaction data such as "Iran" or "Cuba".

When targets lack appropriate controls to mitigate sanctions risk, acquirers should add indemnifications to purchase agreements that last at least five years to mitigate the risk of undiscovered sanctions violations cropping up after purchase.

1940 Act considerations

The Investment Company Act of 1940, as amended ("1940 Act"), imposes a strict regulatory regime on investment companies that are required to register under such Act. An investment

company is defined in Section 3 of the 1940 Act, in relevant part, as an issuer primarily engaged in investing in securities or as an issuer that invests or holds 40% or more of its total assets (excluding cash and U.S. government securities) in "investment securities".

Since many blockchain companies hold digital assets that likely would be deemed securities, it is critical to conduct an investment company analysis to determine whether the proposed target is subject to regulation under the 1940 Act.

To operate in the United States, an investment company must either register as such with the SEC, or fall within an exception or exemption from registration. A non-U.S. investment company cannot register with the SEC without obtaining exemptive relief, which the SEC infrequently provides. Nevertheless, a non-U.S. investment company could issue securities tokens pursuant to investment company exceptions for issuers that engage in private offerings in the United States either (1) to fewer than 100 U.S. "accredited investors", or (2) solely to U.S. investors that are "qualified purchasers".

It is important to remember that an entity that illegally operates as an investment company in the United States is subject to draconian penalties, including the voidability of all contracts.

IP rights considerations

While blockchain-related M&A transactions are relatively new in the M&A landscape, IP rights considerations are simply variations on standard themes. An acquirer of a blockchain target may, however, find additional potential risks, including those related to a more pronounced reliance on open-source software, and a greater likelihood of a target being subject to patent litigation claims. The following are a sampling of IP rights considerations that should be kept in mind when performing IP due diligence of a blockchain target.

A threshold concern when acquiring any IP right is ownership. An acquirer should consider conducting searches of registered IP to establish ownership, applicable jurisdictions in which registrations have been secured, and the periods during which such registrations will remain in effect.

As blockchain technology often includes open-source software, the licence terms of such software may impact an acquirer's assessed value of, and ability to exploit, the technology. An acquirer may wish to assess whether open-source software is included in the target's software. A careful review of applicable licence terms may be warranted, since open-source licences vary, from permitting licensees a broad right to use, modify, and distribute software that is based on open-source software, to a more restrictive "copyleft" licence that requires the source code of any software based on open-source software to be redistributed at no cost.

Acquirers should also confirm chain of title with respect to IP rights, whether registered or not, by confirming that the target has put in place a practice of having all employees, independent contractors, and consultants enter into robust proprietary information and inventions assignment agreements whereby the employees, independent contractors, and consultants are not only obligated to keep all company proprietary information confidential, but also agree that whatever they develop, invent, discover, or create during the course of their employment or engagement is owned by the target. Acquirers should also consider whether the target has followed best practices such as fairly compensating patent owners for their innovations or entering into such arrangements as a patent pool.

Lastly, blockchain-related patents are on the rise not only due to companies investing in their own blockchain-related solutions, but also due to non-practising entities acquiring blockchain-related patents; as a result, companies developing blockchain technology may

face a greater number of patent infringement claims than other targets engaged in more conventional businesses. Accordingly, extensive patent due diligence and freedom-to-operate analyses may be advisable.

Privacy and cybersecurity considerations

The use of blockchain in a business model presents unique privacy issues. This includes scenarios where personal information about natural persons is processed on the blockchain, as well as those in which personal information is stored off-chain but associated with, or linked to or from, the chain (and even when the information on the chain is about both consumers and individual business users using the blockchain application for business use). Even a user's public-private encryption key associated with its identity is covered by many data protection laws.

Crypto companies should be aware that privacy laws may impose broad requirements, and may apply outside the borders of the country that promulgated the law (e.g., the European Union's General Data Protection Regulation 2016/679 applies to non-European Union establishments if they are doing business with people located in the European Union).

Data protection laws globally impose requirements and restrictions on processing personal information about individuals, whether they are acting as retail consumers or representatives of businesses. For example, under some laws, called data export restrictions, personal information may only be exported from one country to another if certain conditions are met. This is a challenge for a global blockchain application in which the data is housed and duplicated around the world. If the blockchain application is private, the data export requirement can be met by including certain terms in the contract between the participants. Similar laws, called data location laws, require that the "master" copy of data be housed in a particular country, even if it may also be stored elsewhere. This poses another challenge for a blockchain application where there is no one true "master" copy.

Data protection laws often also give individuals various rights with regard to companies' use of their data. Sometimes, laws require that individual consent be obtained in order for their data to be used. In a blockchain model, this would require the individual to agree, electronically, to a data agreement before their personal information can be processed on the chain. In some cases, there is no opportunity to obtain this consent directly from the individual, so the participants in the blockchain have to rely on a contractual representation from other participants that they obtained the required consents.

These laws also give individuals the right to request that businesses delete or correct their personal information. Due to the immutable nature of blockchain data, deleting and making changes to data that is stored on the chain is impossible or practically impossible. Therefore, business models that use blockchain must find other ways to honour these requests, such as possibly by all participants disposing of a decryption key or by adding a corrective annotation to the data that the individual requested to correct.

Many of these challenges can be avoided by storing personal information off-chain instead of on-chain, and some can be managed by using a private blockchain instead of a public blockchain, so that all participants can agree contractually to the rules of the road for the use of personal information in blockchain businesses.

Last, but not least, crypto companies are also at risk of cybersecurity hacks, breaches or other incidents. Cybersecurity is a key area of disclosure focus not only for investors, but also for the SEC. Targets should ensure that cybersecurity risks, including any past incidents, are properly disclosed and presented in the offering document in order to protect against disclosure liability.

CFIUS considerations

An increasingly powerful force that non-U.S. acquirers and U.S. targets (including U.S. subsidiaries and branches of non-U.S. companies) ignore at their peril is the U.S. Committee on Foreign Investment in the United States ("CFIUS").

CFIUS is an interagency committee of the U.S. government that reviews certain prospective transactions involving foreign investment into the United States to determine, and potentially mitigate, the effect of such transactions on the national security of the United States, or otherwise prevent the transfer of technology, sensitive personal data, and other resources outside of the United States.

Under the recent regulations implementing the Foreign Investment Risk Review Modernization Act of 2018, CFIUS has the authority to review not only transactions through which a non-U.S. person could gain "control" of a U.S. business, but also certain non-controlling investments in U.S. businesses involving critical **t**echnologies, critical **i**nfrastructure, or sensitive personal **d**ata (so-called "TID" businesses).

The definition of "critical technologies" includes, among other things, the currently undefined category of "emerging technologies", which likely will comprise certain blockchain technologies, among others (other examples include artificial intelligence, quantum computing, robotics, and data analytics).

In addition, a U.S. blockchain target that performs critical infrastructure functions, including by providing internet protocol networks and exchange points, data centres, and core processing services for financial institutions, telecom, energy, or utility companies, may also fall within CFIUS's heightened scrutiny on non-controlling investments.

Finally, CFIUS may also review certain transactions involving a U.S. blockchain target to the extent it maintains or collects sensitive personal data of U.S. citizens, including financial, geolocation, and health data.

Under relevant statutes and regulations,[28] the President of the United States is authorised to block or unwind acquisitions of, or investments in, U.S. companies by non-U.S. persons when, in the President's view, such transactions threaten the national security of the United States, and the threat cannot otherwise be mitigated. In addition, contrary to CFIUS's long-standing history as a purely voluntary process, certain transactions by non-U.S. persons involving a U.S. TID business are now subject to a mandatory review by CFIUS. Failure to notify CFIUS of a transaction subject to mandatory filing can result in civil penalties up to the value of the transaction.

As a result, it is more critical than ever for dealmakers to closely assess the CFIUS risk profile of a blockchain target and consider whether to voluntarily notify CFIUS, or if not, whether they should voluntarily notify CFIUS to seek pre-closing "clearance", i.e., formal confirmation that there are no unresolved national security concerns.

CFIUS-related risk is generally addressed by requiring representations, covenants and a closing condition tied to a successful outcome of the CFIUS review process, and sometimes by including a reverse break fee in the event that the outcome of the CFIUS review process prevents completion of the transaction. Moreover, where the CFIUS risk is high, U.S. targets may consider requesting that the non-U.S. acquirer deposit the amount of the reverse break fee into a U.S. escrow account in U.S. dollars. Non-U.S. acquirers may also consider purchasing CFIUS-risk insurance to cover payment of the reverse break fee, plus other broken deal costs, such as attorneys' fees, investment banking fees, financing costs, and other due diligence expenses, at a cost of approximately 10–15% of the reverse break fee.

Tax considerations

Tax due diligence is an important aspect of every M&A deal. All M&A deals should include an analysis of the tax implications at the U.S. federal, U.S. state, and local and international levels. M&A deals involving targets with digital assets require the same due diligence considerations as deals involving targets with assets that are more traditional. However, M&A deals involving targets with digital assets may have another level of complexity and require additional scrutiny due to the fast-moving pace of the industry. As new and innovative digital assets continue to emerge, tax authorities have struggled to keep up, which has resulted in a lack of uniformity in reporting and record keeping.

For example, for U.S. tax purposes, the Internal Revenue Service has taken the general position that digital assets are treated as property (and specifically not as currency, regardless of how the assets may be treated by other governmental authorities). Therefore, tax due diligence applicable to property may broadly be applied, and should include an analysis to confirm that the target has been properly reporting and sourcing receipts arising from the digital assets in all jurisdictions (U.S. and international) that may assert taxing nexus.

However, there are often gaps in record keeping of digital assets that may result in difficulties for determining even threshold considerations, such as the property's basis. Digital assets are also notoriously difficult to value. Further, it is often difficult to classify the receipts generated from the holding and selling of digital assets. Typically, attempts to classify such receipts require an analogy to more traditional intangible property. However, digital assets do not always have straightforward analogous traditional counterparts. Digital assets may have characteristics of several categories of traditional intangible property, or may have no analogous counterpart at all.

Depending on how a particular digital asset is classified, consideration should also be given to potential depreciation and whether the target has been properly depreciating the asset and in the appropriate jurisdiction. For example, under the 2017 Tax Cuts and Jobs Act, tech companies have generally not been able to obtain the benefits of the 100% expensing in connection with asset acquisitions, given that qualifying assets generally include only tangible asset classes and do not include intangible assets. Also, if one or more of the target's digital assets may be considered a capital asset, attention should be given to the holding period of that asset(s), which, along with other considerations, may inform whether the transaction should be structured as an asset purchase (which generally would start new holding periods) or a stock purchase (which generally would preserve the holding periods).

Finally, depending on the structure of the transaction and the classification of the digital assets, acquirers should be aware of potential transfer tax liabilities that may arise as a result of the deal.

Other special considerations

Recent trends in challenging crypto markets and in the emerging NFT space raise special considerations, as well.

Distressed assets

Transactions involving distressed assets present their own considerations. With any distressed seller for which valuations have tumbled dramatically, the spectre of fraudulent transfer claims arises if a sale takes place outside of a formal sale process like a bankruptcy or foreclosure, and it becomes difficult to determine whether an opportunistic acquirer has paid fair or reasonably equivalent value for a distressed target or its assets and creditors are paid less than what they are owed.

Distressed sales can take place quickly in different ways that maximise value and efficiency for sellers and provide protection for acquirers.

As an example, a distressed seller like Voyager could sell its assets free and clear of claims and interests in the assets under Section 363 of the U.S. Bankruptcy Code. A relatively straightforward auction and sale process on a relatively quick timeline gives the debtor-seller a chance to maximise value, and provides the successful acquirer with the protection of a court order authorising the sale of the assets free and clear of any claims or liens and granting protection from future fraudulent transfer attack. Importantly, bankruptcy court sale orders can override most contractual limitations on transfers of such contracts and secured creditors can credit bid all or part of their secured claims.

As another example, to the extent a distressed seller has loans outstanding secured by the assets of its business, it could look to facilitate a "friendly" foreclosure sale by its secured lender(s), either to its existing secured lender(s) who may credit bid all or part of such secured claim, or to a third-party bidder. Notice requirements in foreclosure sales tend to be shorter and the opportunity to conduct diligence is more limited. As a result, the process is faster and less expensive than a bankruptcy sale that benefits the existing secured lender(s) and any potential acquirer that has familiarity with the seller and its business. Courts generally recognise the validity of properly conducted Uniform Commercial Code ("UCC") sales, but such sales do not have the same level of protection in respect of future fraudulent transfer or successor liability claims as bankruptcy sales (i.e., a court order) as most UCC sales are carried out without judicial intervention or supervision. For this reason, it is important to ensure that any UCC sale complies with well-recognised procedures and practices to protect the sale from any future legal attack. Moreover, the lack of judicial intervention means that acquirers may have to comply with consent requirements for the transfers of contracts that may not be necessary in a bankruptcy sale.

Potential acquirers may also seek to gain an inside track by strategically purchasing an existing secured loan note from the lenders to a troubled company in light of the legal right of a secured lender in both a bankruptcy sale and a UCC sale to credit bid the outstanding loan as all or part of the purchase price at either type of sale. It will be critical for any such party to confirm perfection of the liens in the assets before negotiating the final purchase of the secured loan that will constitute the consideration or purchase price in either form of sale.

If an acquirer looks to negotiate and close a sale outside of the bankruptcy or foreclosure processes, that buyer may want to obtain a "fairness opinion" from a well-regarded valuation firm to reduce the risk of fraudulent transfer claims from a distressed seller's creditors.

Finally, it is important to understand exactly what is being purchased, especially on an expedited basis: crypto firms may be brokerages or custodians for clients or both. Parties must determine "who has what rights" to the assets managed by the distressed seller.

NFT marketplaces

We believe that a key and unique area for M&A in the NFT market will be consolidation among platforms and marketplaces that facilitate the trade of NFTs. In addition to the considerations above, this will involve significant complexity from both a legal and regulatory perspective. There are already many competing marketplaces, but they come in different shapes and sizes and with a variety of approaches in hosting content creators and trading in their work.

Currently, there are three typical business models:

- Open marketplaces, which allow any content creator to mint and trade NFTs on their platforms (e.g., OpenSea and Rarible).

- Proprietary marketplaces, which offer NFTs created by the marketplace operators and do not facilitate the display or trade of any other digital collectibles (e.g., Bored Ape Yacht Club and Top Shot).
- Curated marketplaces, where the marketplace operators select which NFTs may be minted, displayed and traded (e.g., mintNFT, Nifty Gateway and SuperRare).

As the NFT market expands, it is likely that we will see some of the biggest marketplaces look to acquire smaller rivals. As a result, it is important to understand the above three typical business models, as the legal issues raised by each may vary. Consideration of the legal issues raised by the varying business models will likely affect which marketplaces rivals target (i.e., should a marketplace looking to acquire target a rival that operates according to the same business model to avoid potential integration complications?). Different approaches to IP rights make this particularly true. For example, marketplaces may have different terms with respect to who owns content created on the marketplace platform and what rights the users of the marketplace platform have (i.e., display rights, right to copy, right to sell, right to store, etc.).

Conclusion

2022 has been the year of unique opportunities in the crypto M&A space. Challenging markets and increasing interest in the metaverse have led companies to embrace new transaction strategies, which, in turn, have given rise to novel legal and regulatory considerations.

If there is any lesson to learn from the global financial crisis of 2007–2009, it is that companies that made significant acquisitions outperformed those that did not. There is truly no rest for strategic crypto buyers, as premiums are likely to come down and assets that companies had been reluctant to sell may become available or become available at a more attractive price. Several companies are likely examining their existing lines and getting ready to act fast. However, if history is any indication, the window for maximising value could be relatively narrow.

Crypto M&A remains the answer for dealmakers seeking to create synergies, drive growth, or enter new, exciting markets in uncertain times, but it requires additional expert deal analysis and planning given the many variables of our times.

* * *

Endnotes

1. *See*, TokenData, https://research.tokendata.io (last updated August 2022).
2. We generally refer to "M&A" to include partnerships, joint ventures, mergers and acquisitions, and other strategic and private equity transactions.
3. *Supra* note 1.
4. *Ibid*.
5. The term "metaverse" refers to something akin to cyberspace where people can interact through avatars (i.e., virtual representations of their digital personae – think The Matrix but with a broader physical and commercial potential). Although what it will be is still evolving (*see*, *e.g.*, https://www.wired.com/story/what-is-the-metaverse), companies are already lining up to join it.
6. Non-fungible tokens are blockchain-enabled unique digital files that typically contain data that point to an online version of digital art, collectibles (such as digital trading cards) or other digital content (which visually appear in gif, jpeg, or other common

media formats) or a physical asset, and usually record ownership, evidence authenticity or provide certain rights of use.

7. *See*, NIKE, Inc. Acquires RTFKT, available at: https://news.nike.com/news/nike-acquires-rtfkt (December 13, 2021).
8. *See*, NFTs Are the Biggest Internet Craze. Do They Work for Sneakers?, available at: https://www.wsj.com/articles/nfts-and-fashion-collectors-pay-big-money-for-virtual-sneakers-11615829266.
9. *See*, NIKE, Inc. Acquires RTFKT, available at: https://news.nike.com/news/nike-acquires-rtfkt (December 13, 2021).
10. *See*, Today we leap Into The Metaverse with @BoredApeYC, @gmoneyNFT & @punkscomic, available at: https://twitter.com/adidasoriginals/status/1466443459951271939?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E1466443459951271939%7Ctwgr%5E%7Ctwcon%5Es1_&ref_url=https%3A%2F%2Fcointelegraph.com%2Fnews%2Fadidas-enters-the-metaverse-with-nft-partnerships (December 2, 2021).
11. *See*, Getty Images to Become Publicly Traded Company Through Combination with CC Neuberger Principal Holdings II, available at: https://www.globenewswire.com/news-release/2021/12/10/2349924/0/en/Getty-Images-to-Become-Publicly-Traded-Company-Through-Combination-with-CC-Neuberger-Principal-Holdings-II.html (December 10, 2021).
12. *See*, Getty Images CEO Talks NFT Aspirations After $4.8 Billion Deal With Blank Check Company, available at: https://www.bloomberg.com/news/newsletters/2021-12-10/getty-images-ceo-talks-nft-aspirations-after-4-8-billion-deal-with-blank-check-company (December 10, 2021).
13. *See*, InfiniteWorld, a Leading Metaverse Infrastructure Platform for Brands, Announces Plans to Become a Publicly Traded Company via a Merger with Aries I Acquisition Corporation, available at: https://www.businesswire.com/news/home/20211213005343/en/InfiniteWorld-a-Leading-Metaverse-Infrastructure-Platform-for-Brands-Announces-Plans-to-Become-a-Publicly-Traded-Company-via-a-Merger-with-Aries-I-Acquisition-Corporation (December 13, 2021).
14. *Ibid*.
15. *See*, OpenSea buys DeFi wallet startup Dharma Labs, appoints new CTO, available at: https://techcrunch.com/2022/01/18/opensea-buys-defi-wallet-startup-dharma-labs-appoints-new-cto/ (January 18, 2022).
16. *See*, Yuga Labs Acquires CryptoPunks and Meebits from Larva Labs; Grants IP and Commercial Rights to Individual Owners, available at: https://www.businesswire.com/news/home/20220311005470/en/Yuga-Labs-Acquires-CryptoPunks-and-Meebits-from-Larva-Labs-Grants-IP-and-Commercial-Rights-to-Individual-Owners (March 11, 2022).
17. *See*, Bored Ape creator's purchase of CryptoPunks means it now owns two of the top-selling NFT projects, available at: https://markets.businessinsider.com/news/currencies/bored-ape-yacht-club-nft-cryptopunks-meebits-opensea-larvalabs-yugolabs-2022-3 (March 14, 2022).
18. *See*, Framework for "Investment Contract" Analysis of Digital Assets (2019), available at: https://www.sec.gov/corpfin/framework-investment-contract-analysis-digital-assets.
19. *See*, The Responsible Financial Innovation Act, Section 4356, 117th Congress (2022), available at: https://www.congress.gov/bill/117th-congress/senate-bill/4356/text.
20. The term "commodity", defined in Section 1a(9) of the Commodity Exchange Act, is extremely broad, covering everything from physical commodities to "services, rights,

and interests", which the CFTC believes includes cryptocurrencies, and are therefore subject to the CFTC's jurisdiction.

21. *See*, 18 U.S.C. § 1960(b)(1)(B).
22. *See*, FIN-2013-G001, Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies (March 18, 2013).
23. State money transmission licensing laws generally define regulated activity broadly to include "receiving money for transmission", and many state statutes define "money" to include "monetary value". Any state that has, to date, not established a formal position with respect to the regulation of virtual currency activity could: (1) deem the receipt, holding, or transfer of fiat currency in connection with virtual currency activity (such as facilitating a virtual currency exchange platform) to constitute money transmission subject to regulation in its own right; and (2) deem virtual currency activity itself to be subject to regulation in a manner similar to activity involving fiat currency, such as receiving and transmitting virtual currency.
24. *See*, *U.S. v. Harmon*, Case 1:19-cr-00395-BAH (D.D.C. July 24, 2020).
25. *See*, 31 CFR § 1010.100(ff)(5).
26. *See*, *CFTC v. HDR Global Trading Ltd. et al.*, Case 1:20-cv-08132 (S.D.N.Y. August 10, 2021).
27. *See*, United States Office of Foreign Assets Control, Sanctions Compliance Guidance for the Virtual Currency, available at: https://home.treasury.gov/policy-issues/financial-sanctions/recent-actions/20211015.
28. *See*, 31 CFR Part 800.

Dario de Martino
Tel: +1 212 610 6329 / Email: dario.demartino@allenovery.com

Dario de Martino is an M&A partner in the New York office of Allen & Overy LLP, and serves as co-chair of its Blockchain, Web3, and Fintech Group.

He has a wide range of experience representing U.S.-based and global technology, financial services, healthcare, and industrial companies with respect to their complex strategic transactions, including advising on transformative domestic and cross-border public and private mergers, tender offers, acquisitions, divestitures, global carve-outs, joint ventures, and other strategic investments.

He regularly counsels some of the most influential crypto market participants with respect to a variety of matters relating to blockchain, tokenisation, cryptocurrencies, and smart contracts. His experience in the digital asset space includes advising public and private companies with respect to M&A, strategic investments, reorganisations, joint-ventures, digital asset offerings, blockchain licensing and service agreements, and structuring of new blockchain-enabled products in compliance with the U.S. regulatory framework.

Dario is a frequent speaker and writer on various topics relating to tech M&A, and is also an active leader in the firm's diversity, equity, and inclusion initiatives.

Mara Goodman
Tel: +1 646 946 6533 / Email: mara.goodman@allenovery.com

Mara Goodman is an associate in the New York office of Allen & Overy LLP and a member of the firm's Corporate Department.

Her practice focuses on complex M&A, joint ventures and broader corporate matters. She has advised clients on matters across a range of industries, including consumer goods, life sciences and technology.

Allen & Overy LLP

221 Avenue of the Americas, New York, NY 10020, USA
Tel: +1 212 610 6300 / URL: www.allenovery.com

www.globallegalinsights.com

Other titles in the **Global Legal Insights** series include:

AI, Machine Learning & Big Data
Banking Regulation
Bribery & Corruption
Cartels
Corporate Tax
Employment & Labour Law
Energy
Fintech
Fund Finance
Initial Public Offerings
International Arbitration
Litigation & Dispute Resolution
Merger Control
Mergers & Acquisitions
Pricing & Reimbursement

GLI GLOBAL LEGAL INSIGHTS