THE REVIEW OF
SECURITIES & COMMODITIES REGULATION
AN ANALYSIS OF CURRENT LAWS AND REGULATIONS AFFECTING THE SECURITIES AND FUTURES INDUSTRIES

Vol. 56 No. 19 November 8, 2023

EMERGING ISSUES IN DIGITAL ASSET LITIGATION: DISCOVERY AND BEYOND

With the ongoing growth in the use of digital assets, litigators will increasingly encounter disputes in which digital assets play a meaningful role. In this article, the authors discuss prevalent issues that have emerged during litigation involving digital assets and the approaches that litigators have taken to address them. The authors focus on the service of process and jurisdictional issues, discovery tools, and attachment laws, providing a roadmap for applying existing principles and processes to litigation involving digital assets.

By Mark Cianci, Stefan Schropp, Antonia Miller, and Deborah Pabon Cifuentes *

As the development and use of digital assets – an umbrella term that includes a broad and expanding swath of emerging technologies, such as blockchain-based cryptocurrencies, other more centralized digital currencies, protocol- or application-specific tokens, non-fungible tokens ("NFTs"), and others – has accelerated in recent years, so too have the number and variety of legal disputes involving these technologies. While these disputes often involve litigation *about* digital assets, with increasing frequency, they present well-worn causes of action in which digital assets serve an ancillary role as crucial evidence or as the underlying assets that will or could be used to satisfy an adverse judgment. Accordingly, the novel questions presented by litigation and discovery involving these technologies have taken on salience beyond the nascent "crypto bar," as a broader universe of litigants and courts alike determine how to apply existing principles and processes to litigation around digital assets.

Accordingly, this article explores a select group of the most common and pressing issues that are likely to arise in the course of litigation in which digital assets play a central or supporting role, while providing a helpful road map to navigating those issues for litigators regardless of the frequency with which they encounter crypto-specific disputes. First, it begins by addressing the increasingly prevalent problem of identifying and bringing parties into litigation by describing the processes that litigants in digital asset litigation may use to navigate service-of-process and jurisdictional issues, as a counterparty's physical location is frequently, in this space, difficult to discern. Second, it provides an overview of three tools that can be used to facilitate discovery related to digital asset litigation: early or expedited discovery, third-party discovery, and the use of consultants and experts in the relevant technology. Lastly, the article covers the application of attachment laws to digital asset litigation, a tool that can help prevent dissipation of the assets in question during the course of a pending action.

* *MARK CIANCI is counsel at the Boston office of Ropes & Gray LLP, STEFAN SCHROPP is an associate at their Washington, DC office, and ANTONIA MILLER is an associate at the same firm's New York City office. Their e-mail addresses are Mark.Cianci@ropesgray.com, Stefan.Schropp@ropesgray.com, and Antonia.Miller@ropesgray.com. DEBORAH PABON CIFUENTES is a law clerk in the New York City office.*

RSCR Publications LLC Published 22 times a year by RSCR Publications LLC. Executive and Editorial Offices, 2628 Broadway, Suite 29A, New York, NY 10025-5055. Subscription rates: $1,197 per year in U.S., Canada, and Mexico; $1,262 elsewhere (air mail delivered). A 15% discount is available for qualified academic libraries and full-time teachers. For subscription information and customer service call 609-683-4450; fax 609-683-7291; write Subscriber Services, RSCR Publications, PO Box 585, Kingston NJ 08528; e-mail cri.customer.service@comcast.net; or visit our website at www.rscrpubs.com. General Editor: Michael O. Finkelstein; tel. 212-876-1715; e-mail mofinkelstein@gmail.com. Associate Editor: Sarah Strauss Himmelfarb; tel. 301-294-6233; e-mail sarah.s.himmelfarb@gmail.com. To submit a manuscript for publication contact Ms. Himmelfarb. ISSN: 0884-2426.

BRINGING PARTIES INTO THE ACTION: PROCESS AND JURISDICTION

While the anonymity frequently accorded to digital asset holders through the use of usernames, hashing, crypto wallets, and the like is a – and perhaps *the* – major driver of their ever-increasing ubiquity, that anonymity need not serve as a bar to filing a complaint. To be sure, the anonymous or pseudonymous nature of crypto entities, founders, and users have, unsurprisingly, not caused the U.S. courts to jettison long-standing analytical frameworks for service of process and the establishment of personal jurisdiction over putative defendants. At the same time, both state and federal legislatures have moved cautiously, if at all, with statutory revisions to address the new landscape. But those existing frameworks have – with the benefit of well-reasoned arguments from counsel and a receptive ear from judges – been stretched at the margins to accommodate the realities of digital assets. Accordingly, practitioners should be prepared to aggressively pursue the identities of suspected defendants and to defend the extent to which they are on notice of and subject to the court's jurisdiction in connection with a pending action.

As an initial matter, and while John Doe complaints can be a useful stopgap measure for a time, a natural prerequisite to properly serving and establishing jurisdiction over a defendant is determining the identity of that defendant. On this front, the U.S. government and its various agencies have been at the vanguard of rooting out anonymous crypto users, but the lessons learned from their civil and criminal pursuits are instructive for private litigators as well. As one example, the Internal Revenue Service ("IRS") has consistently and repeatedly used John Doe summonses to extract user information from third-party cryptocurrency exchange platforms and private banks, including, within the last year, convincing both the Los Angeles- and New York City-based federal courts to issue *ex parte* John Doe summonses to cryptocurrency dealers and traditional banks to determine the identities of potential tax evaders.[1] Without alleging any wrongdoing on the part of these third parties, the courts determined that the IRS's requests for identifying information about individuals with more than $20,000 in crypto transactions over a six-year period (2016–2021) were sufficiently directed at an "ascertainable group or class of persons" and concluded that there was a reasonable basis for believing that this group failed or may have failed to meet their tax obligations.[2] Those courts also grounded their conclusions in the fact that the information sought to be obtained (*i.e.*, the identities of the persons with respect to whose liability the summons was issued) was not available from any other source and that the information sought by the IRS was narrowly tailored to the potential infraction, causing IRS Commissioner Chuck Rettig to express his view that "[t]he John Doe summons remains a highly valuable enforcement tool that the U.S. government will use again and again to catch tax cheats."[3]

While the IRS has its purposes for using the "valuable tool" of John Doe or other third-party subpoenas, so too do private litigants. Beginning even with pre-filing discovery mechanisms where they are available, such as New York or California's statutes for the methods of obtaining discovery,[4] would-be or active plaintiffs and their lawyers can and should avail themselves of all avenues available to identify those involved with a particular crypto-based enterprise.[5]

Once the identity of a counterparty or an essential third party has been identified, the critical effort can then turn to getting those parties to court (service of process)

[1] *Matter of Does*, No. 22 MISC. 213 (PGG), 2022 WL 5226993, at *1 (S.D.N.Y. Sept. 21, 2022); Press Release, U.S. Dep't of Just., Court Authorizes Service of John Doe Summons Seeking the Identities of U.S. Taxpayers Who Have Used Cryptocurrency (Aug. 16, 2022), https://www.justice.gov/opa/pr/court-authorizes-service-john-doe-summons-seeking-identities-us-taxpayers-who-have-used-2.

[2] *Id.*

[3] U.S. Dep't of Just., *supra* note 1, at *1.

[4] N.Y. C.P.L.R. 3102 (McKinney); Cal. Civ. Proc. Code § 2035.020 (West).

[5] *Id.*

and keeping them there once they arrive (establishing jurisdiction). Beginning with the former, counsel should be aware that the anonymity of individual digital asset users and the decentralized nature of crypto entities – entities often operating without clear founders, executives or decision-makers, headquarters, or registered agents – has complicated the frequently uneventful service of process. However, litigators who familiarize themselves with the technology underlying these digital assets in combination with leveraging their experience with long-standing procedural rules will find ample opportunities to fulfill the needs of their clients.

Getting Parties to Court: Service of Process

As the first of several examples, the New York courts have determined that serving litigation materials by attaching them to a small amount of cryptocurrency or to an NFT that is then transferred to the target's crypto wallet or account is a reasonable alternative service method, at least in some circumstances. In 2022, LCX AG, a virtual asset service provider, filed a complaint in New York State Supreme Court alleging that anonymous hackers stole $8 million worth of digital assets on the Ethereum platform, a decentralized global software network powered by a blockchain.[6] Although the identities of these hackers were unknown at the time of filing, the court issued an order approving service on the hackers through a cryptocurrency token (Service Token) airdrop to the crypto wallet associated with the $8 million attack.[7] In New York, C.P.L.R. 308(5) permits alternative service of process if the court finds that traditional service is impracticable, with many – if not all – states having similar provisions in their civil practice rules.[8] In allowing service through NFTs, the court eschewed a requirement to prove that there were prior attempts at service and reasoned that it "has broad discretion to fashion the means of the alternative service adapted to the particular facts of the case before it."[9]

With the court's blessing, the plaintiff created a web page on the platform where the incident occurred, visited the service web page to confirm that the service documents had been published, and verified that the service web page directed the viewer to these documents.[10] The plaintiff then created, minted, and served the service token that included the service hyperlink by airdropping it to the address belonging to the blockchain address of the wallet of the perpetrator.[11] The plaintiff also demonstrated that the defendants regularly used this blockchain address and were likely to return to collect the service token.[12] The court found that these steps were reasonably calculated, under all of the circumstances, to apprise the defendant of the lawsuit and noted that similar alternative service methods had been sanctioned by other courts, including a case in which service was accomplished by means of Facebook Messenger.[13]

But what about situations in which the target of the litigation is not an individual, but rather a collection of individuals operating as a single entity? Service on corporate entities may seem old-hat to most litigators, but what about when that entity has no corporate status, no headquarters, no formal leadership, and no registered agents? Once again, the government has, with the indulgence of the courts, carved out a pathway that private litigants may follow in their own cases. For instance, in 2022, the Commodity Futures Trading Commission (the "CFTC") filed a complaint in San Francisco federal court against "a decentralized autonomous organization," or a "DAO" called Ooki DAO, that the CFTC alleged violated the registration requirements, among other provisions, of the Commodity Exchange Act.[14] A DAO is comprised of often anonymous individuals who hold the DAO's governance tokens, which allow them to vote on DAO propositions in much the same way as voting shares allow investors to participate in corporate governance decisions.[15] Since the litigation was asserted against the Ooki DAO entity and not against its individual token holders, the courts allowed the CFTC to serve process on the DAO through its "Help Chat Box," which is an online discussion forum on its public website. The court reasoned that the chat box was proper under California's alternative service provision and constitutional due

[6] *LCX Ag v. 1.274M U.S. Dollar Coin*, 2022 WL 3585277 (N.Y. Sup. Aug. 21, 2022).

[7] *Id.*

[8] *Id.* at *3.

[9] *Id*.

[10] *Id* at *4.

[11] *Id*.

[12] *Id*.

[13] *Id*.

[14] *Commodity Futures Trading Comm'n v. Ooki DAO*, No. 3:22-CV-05416-WHO, 2022 WL 17822445, at *1 (N.D. Cal. Dec. 20, 2022).

[15] *Id.* at *2. The court noted that the CFTC did not have to serve individual token holders because a simultaneous settlement occurred between the CFTC and bZeroX (later known as Ooki DAO) that served as actual notice and the best notice practicable under the circumstances.

process requirements, finding that Ooki DAO had "structured its business . . . in such a way that it can only be contacted via its online website or perhaps through its social media accounts."[16]

The court listed two reasons why the chat box posting was reasonably calculated to apprise Ooki DAO of this litigation. First, Ooki DAO controls its website via token voting on administrator keys to make changes and would therefore notice the service of process post, which gained considerable traction with its users and the national media.[17] Secondly, the court reasoned that snapshot votes of governance proposals, which are usually taken before taking binding votes, are based on topics discussed on the discussion post, so "[p]osting notice of this litigation in that same Forum, then, is reasonably calculated to notify *at least some* Token Holders of the ongoing litigation."[18]

Keeping Parties in Court: Establishing Jurisdiction

Turning then to the final topic – keeping counterparties in the litigation once they have been identified and received notice – as *Ooki DAO* exemplifies, the blockchain networks behind many digital assets are entirely decentralized, and it therefore follows that personal jurisdiction issues are likely to arise in crypto litigation. Against this backdrop, courts have split on whether these entities have purposefully availed themselves of the jurisdiction in question, which has fostered unpredictability in pursuing litigation against decentralized digital asset exchanges, particularly when compared to the more lenient approach courts have taken towards service of process. As a result, unique elements like the geographic location from which digital asset users register for a particular platform and the specific site of the network nodes – physical connection points in a digital communication network – although not dispositive, are becoming increasingly central to the establishment of personal jurisdiction over digital asset entities.

Exemplifying this split, in 2017, Tezos, a self-amending decentralized platform for building decentralized applications ("dApps"), conducted an online fundraising effort that ultimately prompted a group of contributors to sue various project participants for the sale of unregistered securities. Although Bitcoin Suisse AG, a Swiss organization that assisted customers in purchasing coins, was also named, the court only found personal jurisdiction over Tezos because its website was hosted on an Arizona server that was freely accessible by U.S. citizens and was highly interactive, thereby encouraging U.S.-based participation.[19] Additionally, the court found that the "network of global 'nodes' [were] clustered more densely in the United States than in any other country,"[20] that Tezos seemed to market only to U.S. customers, and that significant portions of the token sale contributors were U.S. citizens. Conversely, the court found that Bitcoin Suisse did not provide services for the token sale directly to any U.S. investors and specifically noted that a different conclusion as to its jurisdiction over Tezos would be warranted if the contributors were a "small number of well-informed Americans who managed to learn about and participate in the coin offerings that were marketed in some foreign country."[21] Instead, the court reasoned that Tezos, unlike Bitcoin Suisse, (1) encouraged U.S. citizens to participate in the ICO, (2) made it easy for them to participate, and (3) generated results that reflected these efforts.[22]

Similarly, in the Southern District of New York, the Chinese e-commerce company Alibaba was eventually able to establish personal jurisdiction in order to pursue a preliminary injunction seeking to bar the unrelated Alibabacoin Foundation from using its protected marks to promote the Alibabacoin.[23] Under New York's long-arm statute, personal jurisdiction could be exercised over Alibabacoin if (1) Alibabacoin transacted any business within the state and (2) the cause of action – in this case, a trademark preliminary injunction and restraining order – arose from that business transaction.[24] In the first instance, although the court found that Alibaba's websites were highly interactive because customers could register accounts, download content, and interact with the Alibabacoin sales team, this alone was insufficient to establish personal jurisdiction because Alibaba did not establish a reasonable probability that these websites had "been actually used to effect the commercial transactions with consumers in New

[16] *Commodity Futures Trading Comm'n v. Ooki DAO*, No. 3:22-CV-05416-WHO, 2022 WL 17822445, at *11 (N.D. Cal. Dec. 20, 2022).

[17] *Id.* at *11.

[18] *Id.*

[19] *In re Tezos Sec. Litig.*, No. 17-CV-06779-RS, 2018 WL 4293341, at *6 (N.D. Cal. Aug. 7, 2018).

[20] *Id.* at *6.

[21] *Id.*

[22] *Id.*

[23] *Alibaba Grp. Holding Ltd. v. Alibabacoin Found.*, No. 18-CV-2897 (JPO), 2018 WL 2022626 (S.D.N.Y. Apr. 30, 2018).

[24] *Id.* at *3.

York."[25] It was not until Alibaba produced a list of e-mail addresses associated with Alibabacoin investors, including the e-mail address of a New York resident who had allegedly transacted within the state, that the court was able to find that there was "reasonable probability" that the New York defendant had transacted business in the state for purposes of establishing personal jurisdiction.[26]

Conversely, in 2019, the Colorado federal district court dismissed a complaint against Vircurex, the operators of an online digital currency exchange, after it froze customer funds while descending into insolvency, thereby preventing users from withdrawing their deposited Bitcoin. The court reasoned that in order to exercise personal jurisdiction over Vircurex, plaintiffs needed to establish either (1) the existence of continuing relationships between Vircurex and Colorado residents, (2) deliberate exploitation of the Colorado market by Vircurex, or (3) Vircurex's business having harmful effects in Colorado.[27] In rejecting the existence of a continuing relationship, the court explained that the plaintiff did not offer evidence that there were any negotiations or future consequences to creating an account, any terms of service between himself and Vircurex, or anything that would be considered direct communication between the parties.[28] Similarly, when deciding whether there was deliberate exploitation of the Colorado state market, the court found that the plaintiff had failed to allege that Vircurex advertised in Colorado or even in the United States more generally or to allege what amount of frozen funds originated in Colorado in order to analyze whether regular sales were made in the state.[29] Finally, in deciding whether there were harmful effects, the court reasoned that Vircurex did not purposefully direct their activities at Colorado because the plaintiff did not identify what creating his account entailed, what information Vircurex collected about its account holders, whether Vircurex knew that he was located in Colorado, or whether Vircurex even knew that an injury would be felt there.[30]

Although the Colorado court did not find personal jurisdiction over Vircurex, it bears similarities to – and should cause litigants to draw the same conclusions as – the New York court in *Tezos* in finding that courts are willing to look at advertising in the United States as a country and not necessarily in the specific forum state. However, the New York court in *Alibaba* specifically noted that nationwide advertisement is insufficient and that Alibaba would have to show a specific connection to New York. Therefore, to take the safest approach to establishing jurisdiction, litigants should consider whether an entity has specifically availed itself of the specific forum state rather than rely on rulings that availing itself in the United States is sufficient. Litigants seeking these state-specific local connections should examine (and plead, where appropriate) whether the digital asset site requires a user to input an address at registration, if a state-specific bank interacts with the digital asset site by investing or otherwise passing currency with the digital asset platform, or if any advertising efforts are made directly to the forum site. Additionally, litigants should consider whether the platform or any of its affiliates specifically target users from a particular state, whether the user is a digital asset novice or tech-savvy, and whether they actively sought out platforms in other jurisdictions.

As courts apply traditional standards like C.P.L.R. 308 in New York to evaluate digital asset litigation, it is important for parties to have counsel that is well-versed in how clients interact with digital assets. Counsel should study the website to determine the different avenues of communication between the entity and its users, for example, whether it features a Help Chat, like in *Ooki DAO*, or a similar communication forum, and whether the entity maintains social media accounts or discussion boards, as these could be potential vehicles for service of process. Although this could change in the future, as *Tezos* and *Shaw* seem to demonstrate, parties interested in pursuing litigation must also exhibit well-rounded evidence that discretions were aimed at their specific jurisdiction rather than just targeted nationally at the United States. Parties should consider researching where these transactions occurred and whether the decentralized entity has a way of knowing that their actions are specifically reaching the jurisdiction at hand.

IDENTIFYING SPECIFIC ASSETS: FACT DISCOVERY

As disputes relating to digital assets increase in number, trends are emerging with respect to the kinds of issues that may arise in the fact investigation stage of digital asset litigation. In this area of litigation, discovery is primarily focused on the nature and extent of digital assets, ownership, custody, or control of those

[25] *Id.* at *4.

[26] *Alibaba Grp. Holding Ltd. v. Alibabacoin Found*., No. 18-CV-2897 (JPO), 2018 WL 5118638, at *3 (S.D.N.Y. Oct. 22, 2018). *Shaw v. Vircurex*, No. 18-CV-00067-PAB-SKC, 2019 WL 2636271, at *3–4 (D. Colo. Feb. 21, 2019).

[27] *Shaw v. Vircurex*, No. 18-CV-00067-PAB-SKC, 2019 WL 2636271, at *3–4 (D. Colo. Feb. 21, 2019).

[28] *Id*.

[29] *Id.*

[30] *Id.* at *4.

assets, and transactions involving those assets. While not all digital assets are anonymous or pseudonymous, those that are will pose greater challenges in identifying the existence and ownership or control of digital assets and requesting information pertaining to the same via discovery requests. Critical to this effort is a thorough understanding of where this information may reside, and familiarity with discovery processes that can facilitate their disclosure.

To obtain relevant information in discovery in the course of digital asset litigation, litigants should understand what sources of information may be most relevant to their claims. For example, a litigant will want to discover a cryptocurrency user's wallet, since it will contain the majority of a user's cryptocurrency activity and house the user's wallet address and private key.[31] Accordingly, a litigant should craft discovery requests to seek to determine whether or not the wallet is a software wallet, a web-based wallet, or a "hard"/"cold" wallet located on a local drive, and request to search computers, servers, and local drives. Moreover, because cryptocurrency transactions occur via a network connection, litigators should seek all devices that can connect to the internet, or data that could contain relevant digital evidence, which could include social media communications or forum chats, web browsing activities, e-mails, information stored in cloud services, and computer system evidence of bitcoin malware, decryption keys, and so on. Discovery requests should also go beyond bank and credit card records. Since users typically need to convert some form of fiat currency at an online exchange to obtain cryptocurrency, records from these exchanges may be an important source of information in the discovery process.[32]

Although transaction records and other data on the blockchain can be transparent, where information is stored "off-chain," or parties to blockchain transactions are anonymous or pseudonymous, litigants may encounter obstacles in identifying relevant parties and transactions for formulating these discovery requests. Moreover, if a private key has been disclosed to third parties, this presents even further challenges identifying the relevant user to a litigation. Designing discovery to correlate digital assets, wallet addresses, or transactions with the identity of the corresponding user is critical. To try to obtain the necessary information to formulate effective discovery requests, litigants can make use of a few discovery processes that have now featured frequently in digital asset litigation: early/expedited discovery, third-party discovery, and use of consultants/experts.

Early or Expedited Discovery

As noted briefly above, litigants have made use of early or expedited discovery procedures in actions where a defendant cannot be identified. In federal court, a party cannot seek discovery prior to the initial discovery conference that will govern how the parties engage in discovery, absent a stipulation or a court order permitting expedited discovery.[33] Courts generally grant motions for expedited discovery where "the request for expedited discovery is reasonable under the circumstances and good cause exists for granting the motion."[34]

In the last few years, courts have permitted this discovery process in digital asset litigation to identify unknown defendants, particularly in actions involving digital asset theft.[35] In *ZG Top Technology Co. Ltd. v. John Doe*,[36] plaintiff ZG Top, a global cryptocurrency trading platform and digital wallet host lost hundreds of thousands of cryptocurrency tokens as a result of a hack.[37] ZG Top was not able to identify the hacker but was able to determine and present evidence to the court that the stolen tokens were transferred to an account at Bittrex, Inc., a crypto asset trading platform.[38] Although Bittrex identified the account holder, it refused to disclose the user's identity absent consent or a court

[31] Michael Doran, *A Forensic Look at Bitcoin Cryptocurrency*, SANS Institute (2021), https://www.sans.org/white-papers/36437.

[32] *See, generally, id*.

[33] Fed. R. Civ. P. 26(d)(1).

[34] *JTH Tax, Inc. v. M&M Income Tax Serv.*, 2013 U.S. Dist. LEXIS 15843, at *5 (D.S.C. Feb. 6, 2013) (granting motion for expedited discovery to aid the court in making a determination at the preliminary injunction hearing); *see also adMarketplace, Inc. v. Tee Support, Inc.*, 2013 WL 4838854, at *2 (S.D.N.Y. Sept. 11, 2013) (granting motion to expedited discovery where plaintiff stated a prima facie case for defamation and was unable to identify defendants without a court-ordered subpoena).

[35] *See, e.g., ZG Top Tech. Co. v. Doe*, No. 19-92, 2019 WL 917418, at *2 (W.D. Wash. Feb. 25, 2019); *SingularDTV GmbH v. Doe*, No. 21-6000, 2021 WL 3668161, at *1 (S.D.N.Y. Aug. 16, 2021).

[36] *ZG Top Tech*, 2019 WL 917418, at *2.

[37] *Id.* at *2.

[38] *Id.* at *2.

order. ZG Top then filed a "John Doe" lawsuit against the unknown hacker and moved for expedited discovery on Bittrex to identify the hacker.[39] The court found there was "good cause" to support ZG Top's request for information from Bittrex identifying John Doe's identity because the request was "reasonably likely to lead to the production of information" that would permit ZG Top to serve process on the defendant. The court noted that the evidence ZG Top had provided in support of its motion appeared to trace the allegedly stolen funds to an account on Bittrex, including communications between ZG Top and Bittrex that suggested the account holder's identity was "already known or ascertainable."[40]

Although the anonymity or pseudonymity of cryptocurrency users presents challenges, recent actions involving digital assets reveal that litigants and courts have mitigated this issue by employing this discovery mechanism already employed in other kinds of actions involving unknown defendants. It is worth noting, however, that the courts permitting early or expedited discovery in this area have generally declined to allow discovery requests that go beyond identifying an unknown defendant. In *ZG Top*, the plaintiff had argued that expedited discovery on Bittrex "and possibly others" was necessary to identify the unknown defendant, trace and freeze the allegedly stolen assets, and preserve evidence.[41] Nonetheless, the court declined to authorize "open-ended discovery," and did not allow ZG Top to serve discovery requests on other persons besides Bittrex prior to any discovery conference, and did not permit its requests to Bittrex to facilitate the tracking, freezing, and recovery of the allegedly stolen cryptocurrency or preservation of evidence.[42] The court reasoned that these requests sought ultimate, affirmative relief that was not appropriate for expedited discovery.[43] Accordingly, practitioners should be cognizant of the application of this mechanism when facing an unknown defendant in digital asset litigation, including the parties to whom movants have directed expedited discovery and the support relied on to buttress their motions.

[39] *Id.* at *2.

[40] *Id.* at *2.

[41] *Id.* at *2.

[42] *Id.* at *3.

[43] *Id.* at *3. *See also Jacobo v. Doe*, 2022 WL 2079766, at *4 (E.D. Cal. June 9, 2022) (declining to allow discovery requests for documents and information regarding transactions involving the wallet addresses and communication with the defendant and any non-party accountholder of the wallet addresses).

Third-Party Discovery

As previewed in *ZG Top*, correlating digital asset transactions to real identities requires additional discovery steps. Discovery requests to third parties, such as cryptocurrency exchanges in particular, can help litigants identify the owners of digital wallets and identify transactions that are a critical source of information. If the identified exchanges are located in the United States, they are increasingly adopting "know-your-customer" procedures at onboarding, as a result of regulatory and prosecutorial pressure, such that the exchanges possess records that match the user's identity with the transactions on those exchanges.[44] If the digital assets at issue are held on an exchange (or held by a similar custodial service provider), the exchange operator may comply with court orders to provide information revealing a user's identity and associated transaction records. Discovery should seek records from these platforms demonstrating the discovery target's identity, use of the exchange, and trading history. However, it is worth noting that if the exchange is "decentralized" or located offshore, or simply does not comply with various applicable regulations, there is a risk the exchange may not respond to discovery requests or comply with court orders. While litigants can seek to compel compliance with a court's discovery order, non-U.S. exchanges are generally beyond the enforcement reach of American courts.

Consultants, Experts, and Technology

Prior to crafting discovery requests, litigants may need to plan for utilizing consultants, subject-matter experts, and outside technology to identify custodians and decode and trace blockchain transactions, as their sophisticated technical knowledge may enable practitioners to analyze and utilize all relevant public data available on the blockchain and information that can be obtained from cryptocurrency wallets. A subject-matter expert can study records from third parties, such as bank statements, trace activity on the blockchain ledger, reverse-engineer identities, and aid litigants in searches of a party's devices (*e.g.*, cellphones, computers, hard drives) to extract information leading to the ownership of digital assets.[45] For example, forensics experts have tested the anonymity of cryptocurrency

[44] Benedict George, *What is KYC and Why Does it Matter For Crypto?* Coindesk (May 11, 2023), https://www.coindesk.com/learn/what-is-kyc-and-why-does-it-matter-for-crypto.

[45] *See, generally*, Michael Doran, *A Forensic Look at Bitcoin Cryptocurrency*, SANS Institute (2021), https://www.sans.org/white-papers/36437.

transactions, including by refining techniques to "de-anonymize" bitcoin users and entities by clustering different Bitcoin addresses to assign common ownership to a user's pseudonym.[46]

Two cases illustrate the use of third-party discovery and of consultants/experts and technology in furtherance of discovery in digital asset litigation. In *United States v. Gratkowski*,[47] the government made use of both sophisticated software and third-party intermediaries to discover relevant information. Over the course of an investigation into an illicit website that accepted payment in cryptocurrency, federal agents used forensic software to analyze the blockchain by means of the clustering technique referenced above.[48] Federal agents contracted an outside service to analyze the publicly viewable blockchain and identify a cluster of Bitcoin addresses controlled by the website.[49] The government used the addresses in the cluster to subpoena Coinbase for all information on its customers whose accounts had transacted with any of the addresses in the website's cluster.[50] The agents used the records to establish probable cause to obtain a warrant to search the defendant's home, where they uncovered incriminating evidence.

In *Strivelli v. Doe*,[51] the plaintiff owned smart contracts that generated cryptocurrency revenue that was stolen by an unknown wrongdoer with access to the plaintiff's private keys. The plaintiff enlisted the services of a cryptocurrency consulting firm, Coinfirm, to trace the stolen assets. Coinfirm determined that the wrongdoer had transferred the assets between several digital wallets, some of which were hosted on several cryptocurrency exchanges (including Coinbase, KuCoin, FTX, and Opensea).[52] The plaintiff sought expedited discovery from the exchanges to uncover the wrongdoer's identity and a temporary restraining order to enjoin the wrongdoer as well as the exchanges from conducting further transactions with his stolen assets.[53] In granting the motion for expedited discovery, the court noted that the plaintiff had provided "compelling evidence" – *i.e.*, Coinfirm's report tracing the stolen assets to wallets and transactions on the exchanges and indicating that at least some of the exchanges perform "know-your-client" checks at the time of onboarding – that would help plaintiff uncover the wrongdoer's identity.[54] Finally, the court noted that the plaintiff had "properly tailored his discovery" to finding information about the wallets and the wrongdoer's transactions identified in the report.[55]

Both *Gratkowski* and *Strivelli* illustrate the discovery value of third-party discovery and of consultants, experts, and software in advancing fact discovery in litigation involving digital assets. Regardless of existing knowledge of digital asset technologies, or litigation background in this area, practitioners can avail themselves of these resources in their fact investigations to gather and analyze relevant data and information to wield in litigation. Moreover, as *Strivelli* demonstrates, the work product of consultants, experts, and software can also be used to bolster a litigant's discovery motions before the court. In particular, as the technology in this area continues to evolve, and with it, the legal landscape, litigants may lean on these resources to facilitate effective discovery.

These examples shed light on the discovery tools and strategies that can aid litigants in identifying, requesting, and obtaining highly relevant information in digital asset litigation. Litigants should keep in mind and plan for additional cost and effort to conduct this supplementary early discovery. The manner in which these disputes have played out in existing actions reveals that courts are amenable to advancing these critical information-gathering steps.

PROTECTING DIGITAL ASSETS: ATTACHMENT

If a party is able to successfully bring its adversary to court and identify information to seek in discovery, there

[46] *Id*. When an organization creates multiple Bitcoin addresses, it can combine its Bitcoin addresses into a separate, central Bitcoin address, called a "cluster." A "cluster" of Bitcoin addresses held by one organization may be identified and linked back to the organization by analyzing the Bitcoin blockchain's transaction history. *United States v. Gratkowski*, 964 F.3d 307, 309 (5th Cir. 2020).

[47] 964 F.3d 307 (5th Cir. 2020).

[48] *Id.* at 309-10.

[49] *Id.* at 309-10.

[50] *Id.* at 309-10.

[51] 2022 WL 1082638 (D.N.J. April 11, 2022).

[52] *Id.* at *2.

[53] *Id.* at *2.

[54] *Id.* at *2.

[55] *Id.*; *see also Wuluvarana v. Does*, 2023 WL 183874 (E.D. Wis. Jan. 13, 2023). Plaintiff used Coinstructive, a cryptocurrency analysis and investigative firm, to identify wallet addresses and determine that they were tied to specific accounts at Coinbase, Binance, and Gemini.

still remains a major risk that the assets dissipate before judgment is rendered. As the *Shaw* case discussed above exemplifies, companies can – and in the crypto space, frequently do – go insolvent while holding assets belonging to users. And even if a prejudgment attachment of digital assets is secured, there are additional risks associated with the dissipation of these funds during and after litigation due, in large part, to the volatility of the prices of such assets. Therefore, parties should consider how assets can be frozen to mitigate the risk of asset dissipation as well as how to safekeep digital assets during the litigation, including considering the risk that these digital assets could be stolen. Accordingly, litigators must examine whether a trust can be created to keep these digital assets, how these digital assets could be turned over to it (and what personal information would need to accompany such a transfer), or whether it would be safer to liquidate the assets.

On this front, courts have recognized the issue of cryptocurrency dissipation for companies that only transact in cryptocurrency and have made arrangements to mitigate the risk of a judgment not being satisfied. The Southern District of New York, for instance, found that there was a risk that ICOBOX Hub, a U.S.-based initial coin offering ("ICO") incubator, and its creator would not satisfy a judgment and therefore should be enjoined and restrained from making sales, assignments, or transfers of any property until a final judgment in a worker's compensation case was rendered. The plaintiff made a showing of the danger of the dissipation of assets by adducing evidence that (1) the creator failed to respond and appear in a civil enforcement action brought by the U.S. Securities and Exchange Commission ("SEC") (who secured a default judgment against him), (2) that the creator is a Russian citizen and that there are "significant doubts about his current whereabouts," (3) that ICOBOX operates offshore and has no U.S. operations, and (4) that ICOBOX transacted only in Bitcoin, a "completely decentralized currency, operating free of nation states or central banks."[56]

The Southern District of New York granted another prejudgment attachment that ordered crypto-exchanges Xapo, Coinbase, Poloniew, and Bittrex to freeze a defendant's cryptocurrency. Winklevoss Capital Fund ("WCF"), an investment company, filed an *ex parte* application for prejudgment attachment of up to 5,000 bitcoin or its equivalent against Charles Shrem, who was supposed to purchase virtual currency for WCF through his online platform.[57] The court concluded that WCF met the criteria for prejudgment attachment because it showed that (1) there was a valid cause of action for a money judgment totaling no less than 5,000 bitcoin, (2) there was a probability that it would succeed on the merits to recover at least the sum of 5,000 bitcoin, (3) Shrem is a citizen of Florida and has evidenced an intent to frustrate the collection efforts of his creditors, and (4) Shrem has no apparent counterclaims against WCF for money damages.[58]

These cases demonstrate the different ways that U.S. courts have attempted to prevent the risk of defendants' defaulting on judgment payments in digital asset litigation cases. Although not dispositive, the court in *ICOBOX* recognized the decentralized nature of a digital asset as a potential risk in the dissipation of a future judgment. This is an important point for litigants to highlight, especially in cases when dealing with entities that transact solely in digital assets. The *WCF* case showed that the courts can freeze funds in the digital asset state by ordering third parties to comply with freezing orders; however, this order did not prevent the frozen assets from dissipating while in the possession of the third party, which can be a huge risk for litigants hoping to collect judgment. Accordingly, litigants would be wise to consider more extreme actions where there is a risk that defendants will flee a jurisdiction or claim insufficient funds in their cryptocurrency wallets.

For example, the U.S. District Court for the Central District of California ordered a defendant to transfer all assets, which included cryptocurrency, to the U.S. Marshall to secure the amount of attachment after a defendant fled his jurisdiction abroad.[59] While residing in the Netherlands, the defendant had represented to a Dutch plaintiff that the defendant was seeking investors for an internet start-up, and the plaintiff transferred funds to defendant via various cryptocurrencies.[60] After being unable to retrieve the assets, the plaintiff successfully filed for attachment of the defendant's assets in Amsterdam, but the defendant then fled the Netherlands and moved to Los Angeles.[61] The U.S. court then issued a writ of attachment that required the

[56] *Morozov v. ICOBOX Hub Inc.*, 2020 WL 5665639, at *11 (S.D.N.Y. May 5, 2020), *report and recommendation adopted*, 2020 WL 5665563 (S.D.N.Y. Aug. 18, 2020).

[57] *Winklevoss Cap. Fund, LLC v. Shrem*, 351 F. Supp. 3d 710, 714 (S.D.N.Y. 2019) (ECF No. 30).

[58] *Id*.

[59] *Handley v. La Melza*, 2022 WL 3137718 (C.D. Cal. July 13, 2022).

[60] *Id.* at *2.

[61] *Id.*

defendant to (1) attach all assets, including cryptocurrency sufficient for the amount of attachment; (2) provide the wallet identification number for each cryptocurrency wallet in the defendant's possession; (3) provide the electronic access key for each cryptocurrency wallet in the defendant's possession; and (4) deposit the attachment account into a court-operated account.[62] When U.S. Marshalls went to collect the attachment, however, the defendant refused to comply with the order and denied possessing sufficient cryptocurrency despite evidence to the contrary from the plaintiff.[63]

In addition to demonstrating that court attachments do not equate to securing judgments in digital asset litigation, the California case demonstrates the importance of understanding how digital assets are held and transferred to secure a court order that can hold a defendant accountable. Although it is unknown how the investors were identified in this case, learning to understand how a blockchain function may help litigators identify other users that have contributed to a specific wallet, which may potentially reveal witnesses and evidence to be used in litigation and help to identify the amount of digital assets in the defendant's possession. These sources of information were both vital in the California court's decision to find that a defendant had violated a court attachment order.

CONCLUSION

The rapid growth of digital assets, and the legal disputes they have prompted, have resulted in an evolving litigation landscape. The unique features of digital assets have led to discernible patterns at all stages of the discovery process of litigations involving digital assets with which litigants should familiarize themselves and use to plan in the course of their own actions. This landscape, however, is rapidly changing as new technologies emerge and are featured in legal disputes. Attention to the decisions of courts, creative and resourceful strategies of litigants and changing laws will be critical for practitioners navigating litigation involving digital assets going forward. ■

[62] *Id.* at *3.

[63] *Id.* at *2.