2023 BUILDING AND WINNING CRYPTO CASES

Authored by: Nat Abramov (Founder & CEO) - Crystal Vantage

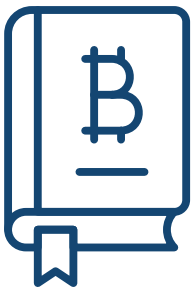
2023 is fast emerging as a formative year for cryptocurrency litigation and crypto fraud recovery. After its spectacular collapse in late 2022, crypto exchange FTX is heading into complex and lengthy bankruptcy with customer losses estimated at $8 billion. At this early stage, it seems FTX may represent simultaneously the most vivid warning light for the egregious excesses and risks of unregulated crypto, but also possibly the most high-profile demonstration of how our existing terrestrial legal systems are called upon to intervene on behalf of injured parties suffering crypto-related losses.

FTX will underscore to the wider world what many practitioners in this field will already know: for better or for worse, cryptocurrency is not a parallel universe, but a digital innovation that exists firmly within the scope and jurisdiction of our laws and institutions. When investors suffer crypto losses, they turn to national courts for disclosure to uncover the beneficiaries of their misappropriated funds, and to petition for bankruptcy when restitution is not forthcoming. How to navigate that reality, and extract the maximum from it, is the business of recovery practitioners operating in the crypto space.

A second instructive case coming to a head in early 2023 is that of crypto lending platform Nexo. As FTX grabbed crypto headlines, in January the Bulgarian National Police Service, in coordination with US authorities, raided the offices of Nexo on suspicion of running similar illicit activities. Nexo may yet emerge as the Inigo Philbrick to FTX's Madoff. It serves as a reminder of the myriad of less high profile, but no less important, crypto fraud cases that continue to proliferate.

As investigators, we see a range of crypto cases with widely varying prospects of success. In this briefing we share our observations on tooling up to succeed in a crypto case, and how to strategise from an early stage. At the outset, we ask ourselves a series of key questions:

1. What type of crypto case is it?
2. What is the evidence of wrongdoing?
3. Who is liable and who is viable as a collection target?
4. Who are the potential co-claimants and allies to the case?
5. What investigative resources are available or needed?
6. What is the best route to recovery?
7. How does the case get funded?



Types of Crypto Cases

By this point in its development cycle, the cryptocurrency sector has spawned a mini-economy comprising exchanges, miners, depositors, investors, insurers, issuers, lenders, intermediaries, programmers, marketers, promotors, IT providers, regulators, advisors, and much else. Cryptocurrency has a press and, like the traditional economy, it has established corporates and smaller challenger outfits or lone investors – a Wall Street and a Main Street.

This means that cryptocurrency cases can now span almost any type of claim. It is becoming outdated to view crypto cases narrowly as instances of disappearing fraudsters – though to be sure those still exist. Rather it is helpful to think about the events and parties to a crypto dispute a little more like an ordinary civil dispute.

By way of example, crypto cases can include:

(a) Claims against insurers, and insurer claims against culprits.

(b) Investor class actions.

(c) Misrepresentation and dishonest solicitation of investment.

(d) Market manipulation, such as rug pulling, or other types of fraud.

(e) Failure to adhere to terms of business or local laws.

(f) Improper liquidation of portfolios.

(g) Theft or non-safeguarding of client assets.

(h) Failure to provide access to funds or accounts.

(i) Bankruptcy and insolvency.

(j) Contractual disputes.

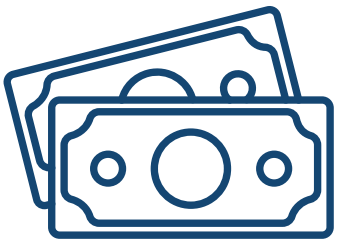
Evidencing Wrongdoing

The 17th century Anglican bishop and philosopher George Berkeley was probably not thinking of cryptocurrency when he asked "if a tree falls in a forest and no one is around to hear it, does it make a sound?"

Today crypto investors are faced with a somewhat updated question – "if my cryptocurrency disappeared when no one was watching, does it exist somewhere, and where can I find it?"

Berkeley concluded the answer to his question was yes because God could hear the tree fall. For slightly different reasons, the answer to the crypto corollary is also likely to be affirmative, because the crypto can be traced, as can the perpetrators; the case will yield to evidence; and recovery can often be achieved through the intelligent pursuit of solvent parties.

Like most claims, crypto cases turn on good evidence. Many clients approach a professional at the outset with a sense of resignation or helplessness and fail to appreciate how much evidence is actually available to them. In our experience, it can be very useful to guide the client to collect: account information; portal screenshots; wallet addresses; transaction IDs; deposit and transaction logs; consented terms and conditions, privacy notices, and contractual undertakings; email correspondence; and other materials amassed during their commercial interactions. Email correspondence in particular can be helpful as there is often disorganisation and disunity among staff when a crypto outfit is failing, which can result in communication with clients/ investors that inadvertently reveals wrongdoing. The way an investment proposition was sold at the outset is also crucial in substantiating possible misrepresentation claims.



Who is Liable and Who is Viable?

Like any well-run recovery campaign, the imperative is to pursue viable targets for collection, building a strategy around those, rather than an expensive chase after recalcitrant or insolvent parties. Therefore, wherever possible, it is worth considering whether any of these parties may be liable for the loss:

- Traditional financial institutions.
- Large or well-capitalised cryptocurrency exchanges.
- Established business figures or celebrities.
- Significant corporations.
- Third party associates or service providers.

The rationale is that these types of parties will frequently pay out a claim where they are liable, to avoid enforcement and reputational damage. High profile examples include Kim Kardashian who reached a $1.26 million settlement with the SEC in October 2022 for promoting EthereumMax without disclosing that she had been paid for the endorsement. In similar circumstances, boxer Floyd Mayweather and musician DJ Khaled reached settlements over their undeclared paid promotions of various ICOs.

For similar reasons, banks and financial institutions have also been targeted in crypto litigation. JP Morgan and Bank of America have both been sued for the fees they have applied to crypto trading. Italian bank UniCredit has also been sued for closing the accounts of cryptocurrency miner Bitminer Factory, which is said to have prevented an ICO. In March 2022, a court in Bosnia and Herzegovina fined a UniCredit branch €131 million in connection with this episode.

Tracing and Disclosure

In certain cases, tracing of cryptocurrency is necessary. This can typically be (a) to locate the culprits where the fraudster(s)/liable parties are not known at the outset; (b) to locate the missing cryptocurrency for enforcement; or (c) to provide evidence of the loss, even where enforcement might not target the direct proceeds of the fraud.

In these cases, a mixture of court applications and investigative tools are often needed. It is well established that most cryptocurrency can be traced along the public blockchain leger. Depending on the coin, or type of coins being traced, the tools used by crypto tracers include: Chainalysis Reactor; TRM Labs; and Elliptic Navigator, among various other specialist software platforms.

In principle, these platforms allow a client's missing cryptocurrency traced along the blockchain to a specific wallet address, or series of addresses. These may already be known to belong to a certain party or organisation, or may require disclosure to reveal the holder's identity.

There are various impediments to an effective trace. Mixing has been used by some fraudsters as a means of co-mingling assets to mask where a specific set of coins have moved. Some tracing platforms are more effective than others at picking this apart. In some cases, the assets have moved along a non-public blockchain using coins such as Monero (XMR), Dash (DASH) or Zcash (ZEC). In these situations, legal action can be considered to identify the last known user in a public blockchain transaction, before assets moved across to a private coin, or indeed to unmask the private blockchain.

Notwithstanding these issues, in the majority of cases, well established legal routes have emerged to uncover the ultimate owners of wallets which have received client funds. Disclosure orders are now commonplace in many jurisdictions to compel exchanges to reveal their KYC customer data behind a wallet. In Ion Science Ltd v Persons Unknown the English Commercial Court permitted victims of an ICO fraud who did not know the identities of the beneficiaries of the fraud, to serve various orders, including for disclosure, on crypto exchanges overseas. This allows victims to seek assistance from a court to reveal the perpetrators/ beneficiary of a fraud, and to receive information from exchanges in other jurisdictions.

Courts are expanding their support to crypto fraud victims. In Gary Jones v Persons Unknown & Ors the Commercial Court granted freezing injunctions against various unidentified parties who transferred the victim's cryptocurrency across the blockchain. This ensured that their wallets could be frozen to prevent dissipation. This then allowed Jones to include the exchange Huobi in the proceedings. In March 2022, the court held Huobi liable for the loss of £480,206, as a constructive trustee, allowing Jones to recover from the exchange rather than pursuing the end fraudster. In a first, the court also permitted Jones to serve the unknown parties by means of dropping an NFT into their wallets held with Huobi.

Non-crypto Assets

While avenues for recourse in the crypto space are developing, it remains significantly more straightforward to enforce against non-crypto assets. Therefore, where possible, it is worth thinking about avenues for collection against parties who have clearly identifiable and locatable assets. For example:

- **Banking or financial assets.** These could be held by an exchange, businessperson, corporation, or promotor of a coin.
- **Real estate assets.** These could include property owned by a crypto outfit, its principals, or the personal assets of individual(s) liable in a case.
- **Corporate assets.** These may include any relevant subsidiaries of a corporate adversary, or the personal corporate interests of a liable individual.
- **Alternative assets.** In the case of wealthy fraudsters, there may be artwork, valuable jewellery or watches, or other alternative investments against which enforcement can be sought.

In this manner, crypto cases can sometimes resemble regular civil fraud cases in their routes to recovery.

Funding

Crypto cases frequently lend themselves to special funding arrangements. This is because claimants have often not suffered a threshold loss individually, but form part of a collective that is owed a large aggregate sum. As such, class actions are becoming commonplace in the crypto space. Even in cases with large individual losses, clients can be reluctant to singularly fund litigation and recovery, which makes the natural case for finding allies, or similarly aggrieved parties.

In the crypto space, this endeavour can be less difficult than it may first seem. Clients themselves may be acquainted with, or have spoken to, other co-investors who suffered similar losses. Beyond this, the cryptosphere is a brimming network of voices who communicate regularly online through news portals, Telegram channels, forums and blogs, Twitter, and other social media. A modest investment of time in book building, by reaching out to other aggrieved parties, or making it known you represent claimants who suffered a certain loss, can bring forth many parties who may join forces with an existing client's efforts.

Due to the structure of these claims, third party funding would potentially be naturally suited to many crypto cases. While many funders take an interest in the crypto space, the industry remains cautious in deploying funding to these cases, perhaps due to the nascent nature of this space and the many risks that are difficult to assess at this early stage. There are nevertheless organisations that will fund crypto cases, and certain funds set up especially for these types of situations.

In preparing a crypto case for funding, a few key areas are worth addressing:

(a) **Size of claim:** The aggregate quantum of the claim will need to be large enough to allow a funder to invest in the case and achieve a several-fold multiple, and to remain commercially interesting for the claimants. In self-funded cases, those with a small number of co-claimants, or bankruptcy/insolvency cases, the quantum can be smaller while remaining viable.

(b) **Evidence:** The evidence base underpinning the claim should be as developed as possible at the point when funding is being sought. Where additional evidence will be required, it is useful to articulate how/where such evidence will be obtained.

(c) **Legal strategy:** A clear, costed legal strategy should be crafted that allows a funder to envisage the route to success, both legally and commercially. The legal basis for claims against any potential defendants should be firmly established. Given the multi-jurisdictional nature of these cases, it will often be important to address how claims will be legally anchored in the relevant jurisdictions, and how local legal action will lead to eventual recovery of assets. As such, the rationale of pursuing particular parties or legal proceedings should be demonstrable. It helps to have an oven-ready team of legal specialists and necessary consultants/experts in the relevant jurisdictions, who can lend the case their support and credibility.

(d) **Collection and enforcement:** The collectability of the claim is of primary importance for external funding. It can be valuable to draft an enforcement plan setting out what known assets can be pursued from potential defendants; what unlocated assets are expected to be located and how; and what asset tracing work can be carried out to map out the attachable assets of the prospective adversaries. An investigations company can help in putting together a recovery plan and costed asset tracing options. A valuation of any such assets, and explanation of how they can be legally recovered, will be important.

The volume of crypto related cases is naturally expected to grow, but they are also likely to diversify increasingly with the spread of cryptocurrency. The collapse of fraudulent crypto schemes will certainly signal caution, but may not reverse that trend. While the crypto space has been home to many notable frauds, it has also comprised some of the most significant asset freezes of recent times. Therefore, the need has never been higher for expertise to guide victims intelligently and judiciously to recovery in this area, using all the latest tools and strategies available.