# CHAPTER 5: BLOCKCHAINS

## A. Technical Foundations

### NOTE ON BITCOIN

Bitcoin is simpler than it sounds. It is a "cryptocurrency" not because it is mysterious but because it is based on cryptography. To see how, let us consider what jobs a financial record-keeping system needs to do, and then see how Bitcoin does them.

The most intuitive way of talking about money is as a tangible thing: dollars are pieces of paper that you hold in your hand. On this view, the numbers in a bank account balance also represent a thing: the number of dollars "in" the account. So a bank, or an online substitute for one, needs to keep track of who has which things.

But another way of thinking about money is in terms of verbs, rather than nouns. What matters are the transactions in which it passes from hand to hand. When you deposit a $50 birthday check from your aunt in your bank account, that's a transaction in which your aunt gives you $50. You are now capable of engaging in transactions in which you give away up to $50. So you could write a $50 check to your aunt, or a $25 check to your dentist and a $25 check to your cousin. With credit cards and online payment systems like Paypal, the transactions are electronic rather than paper, but the idea is the same: keep track of who pays how much to whom and when.

In this example, the bank maintains a ledger of transactions involving your account. Your aunt's bank maintains a ledger of transactions involving her account. When you deposit her check, the two banks consult with each other, and then very carefully adjust both of their ledgers. Bitcoin is exactly the same, with three differences:

- The Bitcoin ledger, called the *blockchain*, keeps track of transactions involving everyone's Bitcoin accounts.
- Instead of being maintained by a centralized authority, the blockchain is maintained collectively, by everyone who uses Bitcoin.
- The blockchain is secured using public-key cryptography.

First, start with the blockchain. Suppose that Alice sends Bob two Bitcoins. (Perhaps he mowed her lawn, or perhaps he gave her some U.S. dollars in exchange.) Abstracting slightly from the technical details, this transaction could be represented as:

```
From: Alice          To: Bob       Amount:   2.000 BTC
```

Alice makes the transfer to Bob by appending this new transaction to the blockchain. Suppose that just before she does, the blockchain (ordered with the most recent transaction at the top) read:

```
From: Carol          To: Alice     Amount: 200.000 BTC
From: Sujit          To: Rajiv     Amount:    .500 BTC
```

```
From: Dave          To: Alice    Amount:   7.250 BTC
From: Carol         To: Alice    Amount:   5.250 BTC
[millions of previous transactions]
```

After Alice adds her transaction to Bob, the blockchain now reads:

```
From: Alice         To: Bob      Amount:   2.000 BTC
From: Carol         To: Alice    Amount: 200.000 BTC
From: Sujit         To: Rajiv    Amount:    .500 BTC
From: Dave          To: Alice    Amount:   7.250 BTC
From: Carol         To: Alice    Amount:   5.250 BTC
[millions of previous transactions]
```

What keeps Alice honest? It is only possible for Alice to make a transaction giving Bob Bitcoins if there are *previous* transactions giving Alice enough Bitcoins. Just as a bank will bounce a check drawn against an account without sufficient funds, other Bitcoin users will reject the transaction unless there are previous transactions already in the blockchain supplying the necessary Bitcoins.* But if Alice has the Bitcoins to spend, other Bitcoin users will agree to add the transaction to the blockchain. When Bob sees that the blockchain has been extended to include Alice's payment to him, he knows that the payment has succeeded.

Second, the blockchain is publicly maintained. The blockchain is just a large and growing file that lists every Bitcoin transaction ever since the start of time. Instead of a bank storing the file on its servers (with appropriate backups), many different Bitcoin users keep a copy of the blockchain. Every time a new "block" of transactions is added to the chain (hence the name), the user adding the block broadcasts it to other users, who add the new transactions to their own copy of the blockchain. It is this collective process of agreement on which transactions have taken place that most distinguishes Bitcoin from traditional payment systems. Bitcoin relies on a peer-to-peer process of consensus rather than on one authority with the power to say which transactions are valid and which are not. Anyone who wants to take part, or to check up on past Bitcoin transactions, can obtain a copy of the blockchain and examine it. In theory, at least, this makes Bitcoin less vulnerable to arbitrary exercises of power: no single person or government can arbitrarily create new Bitcoins or take them away from their owners.

Third, add security into the mix. Bitcoin uses digital signatures to guard against all of the obvious attacks, and a great many subtle ones as well. Every Bitcoin *address* (the source or destination of a transaction) has its own private-key/public-key pair. The "From: Alice" part of the transaction is a digital signature generated using the private key for Alice's address. If the signature matches, anyone examining the transaction can confirm that Alice authorized it; if the signature doesn't match, the transaction will be rejected. Thus, while it is easy to receive Bitcoins, only someone controlling the appropriate private key can spend them. (This also means that if you lose the private key for a Bitcoin address, the Bitcoins are gone forever; no one can spend them.)

Now we are ready to answer two questions hanging over the system: *Where do Bitcoins come from?* and *Why do Bitcoin users cooperate in maintaining the blockchain?* The answer is that there are rewards for participating. A new block of transactions is added to the blockchain roughly every ten minutes: the user who first adds it receives a mining reward of a few Bitcoins, plus transaction fees paid

* This checking process is substantially easier because each Bitcoin transaction explicitly identifies the previous transaction or transactions providing the necessary funds.

by the Alices of the world to have their transactions processed.* Which user that is is chosen essentially at random through a digital version of a scratch-off lottery in which there is an immense supply of free tickets and scratching one off takes a little bit of work and time.† Since whoever scratches off a winning number first wins, Bitcoin users have an incentive to devote their computers' time to "mining" Bitcoins, as the process is called. Each time someone proves that they have won the lottery by exhibiting the winning number for a block of transactions, everyone adds that block and immediately starts scratching off tickets in the next lottery for the next block. This scheme cleverly harnesses Bitcoin users' greed to get them to participate in keeping the system working.

Bitcoin raises some interesting questions about anonymity. On the one hand, Bitcoin transactions are not identified with users' names, only with inscrutably opaque Bitcoin addresses like `16UwLL9Risc3QfPqBUvKofHmBQ7wMtjvM`, so it can be hard to tell who is behind Bitcoin transactions. On the other hand, the blockchain is public, so anyone can scrutinize its history. It is easy to follow Bitcoins from one address to another, unlike cash, which can circulate in near-total secrecy.

## B. Possession and Transfer

**HOWELLS V. NEWPORT CITY COUNCIL**
England and Wales High Court (Chancery Division)
[2025] EWHC 22 (Ch)

*Judge Keyser KC:*

1. The claimant, Mr Howells, says that in August 2013 a hard drive containing the private key to his Bitcoin was deposited in error at Docksway Landfill Site, Newport, which is owned and operated by the defendant, Newport City Council. He says that his Bitcoin are now worth in excess of £600 million and that, without the hard drive containing the private key, he is unable to access them. By his claim issued on 17 May 2024 he contends that he is the owner of the hard drive and of everything on it, and he seeks declarations to that effect, an order that the defendant either deliver the hard drive or allow his team of experts to excavate the landfill in order to find it, and (in the alternative) compensation equivalent to the value of the Bitcoin that he can no longer access. ...

---

* As of 2021, the mining reward was 12.5 Bitcoins, worth about $560,000. The mining reward will gradually decrease over time, and be replaced by transaction fees.

† To be a little more precise, Bitcoin miners are computing hash values. The winner is the one who finds a 32-bit number with a hash that is sufficiently close to zero. Since the hash function used by Bitcoin (SHA-256) produces outputs that are all but indistinguishable from random, there is no way to speed up the process other than to try one 32-bit number after another. The Bitcoin protocol automatically calibrates the difficulty of the hashing problem – i.e., the number of winning tickets in the lottery, or how close is "sufficiently close" to zero – so that someone will find a matching hash and add a block roughly every ten minutes. There is no way to save up winning numbers from one block to the next, since the details of the hashing depend on the transactions in the block.

15. For the purposes of the application I assume the following facts, which are averred in the particulars of claim. (Whether or not those facts are correct does not fall for my determination on this application.) On 15 February 2009 the claimant ran Bitcoin software for the first time at his home in Newport, South Wales. In early 2009 he was able to mine 8,000 Bitcoin, which "are currently located in their original wallet addresses". The Bitcoin software created a "wallet.dat" file for the claimant containing a public and private key address, which was saved on an internal laptop hard drive. The private key, stored within the wallet.dat file, is the only information that can enable access to the claimant's Bitcoin. The Hard Drive was 2½ inches in size and black and silver in colour, and it had a white label, on which was black writing. The Hard Drive was owned and in the possession of the claimant. In 2010 the claimant placed the Hard Drive in a drawer located within his home office. (In his evidence he explains why he removed it from the laptop.) Thereafter he accessed the Hard Drive periodically, using a USB connector cable, because it contained not only the wallet.dat file but numerous other files, documents and photographs. The Hard Drive was fully operational and accessible. On 4 August 2013 the claimant had a clear-out from his home office, placing everything that he thought he did not need into two black bin-liner bags. In his drawers he found two hard drives: one was the Hard Drive, and the other was a blank hard drive that contained no data. He meant to throw out the blank hard drive, but instead he mistakenly picked up the Hard Drive and put it into one of the black bin-liners. He then left the two bin bags downstairs in his house and asked his partner at the time to take them to the landfill at the Site the following day after completing the school run. However, she said that she did not want to take the black bin bags to the Site and refused to do so. The claimant was not overly concerned at her refusal, because he decided that on the following morning he would check to make sure that he had put the correct hard drive in the bin bags. However, when he awoke at 9 o'clock the following morning he found that his partner had had a change of heart and had already taken the bin bags to the Site and manually deposited them into the general waste bins at the Site. In October and November 2013 the value of Bitcoin rose sharply and the claimant's holding increased in value to approximately £9 million. (It is implied in the particulars of claim and expressly stated in his evidence that this increase in value of Bitcoin alerted the claimant to the need to check that he had indeed disposed of the correct hard drive.) The claimant first met with a local representative of the defendant (Mr Gwyn Jones, the Operations Manager) on 25 November 2013 to discuss the question of access to the Hard Drive. Thereafter he made repeated requests to the defendant for access to the Site in order to find and retrieve the Hard Drive, but these were largely ignored by the defendant. The claimant then set about securing investment and expertise to enable a team of experts to undertake a landfill excavation and recovery operation and in 2023 he began to advance his case formally to the defendant. ...

17. On this application the claimant has produced evidence that he has assembled an expert team of recovery specialists, who consider that there is a good chance of locating and recovering the Hard Drive and of successfully using recovery technology to recover the private key even if the Hard Drive is damaged. The defendant does not accept that this is so, and I make no find-

ings as to whether it is so, but for the purposes of this application I shall assume the evidence to be correct. ...

## Discussion

### This Case is not about Ownership of the Bitcoin

19. In my judgment, the only relevant issues in this case concern ownership of, and rights of access to, the Hard Drive. It is necessary to make this clear at the outset, because at the hearing of the defendant's application there was reference to rights regarding Bitcoin and intangible property. I shall explain briefly why I consider those matters to be irrelevant to the real issues in the case.

20. The law of England and Wales has historically recognised two different kinds of personal property: things in possession (tangible property), and things in action (intangible property). In broad terms, things in possession are physical things, and things in action are rights that have existence only as being enforceable within a legal system (such as debts that one is owed, or intellectual property rights). It is now generally recognised that cryptocurrency, such as Bitcoin, is also property, although it does not fit within what the law recognises as tangible or intangible property; as such, it is commonly said to constitute, or to be within, a "third category" of personal property. On this, see: *Tulip Trading Limited v Van Der Laan* [2023] EWCA Civ 83 at [24]; Law Commission, Digital Assets: Final report (Law Com No. 412, 2023), chapter 3; and the recent decision of Mr Richard Farnhill, sitting as a deputy High Court judge, in *D'Aloia v Persons Unknown and others* [2024] EWHC 2342 (Ch), especially at [104] and [173].

21. The only thing that went into the landfill was the Hard Drive. The defendant has made remarks to the effect that this included all the intangible property on the Hard Drive. That does not make good sense, in my view, because intangible property has no location and cannot be "on" anything tangible. However, the remarks led Mr Armstrong KC for the claimant to mock the inference that, if the defendant is the owner of physical items in the landfill and of intangible property on those physical things, it is the owner of (for example) Microsoft's intellectual property of programmes on any hard drive in the landfill. The conclusion would, of course, be absurd; but the absurdity results from the notion that the intellectual property could be located on the hard drive. (If a copy of the novel that won the Booker Prize in 2024 were thrown into the landfill, the author's copyright would not go with it.) In order to avoid going down blind alleys, one needs to focus on what property one is talking about.

22. The particulars of claim seek a declaration that the claimant is the legal owner of both the tangible and the intangible property of and in the Hard Drive. The tangible property is simply the Hard Drive, which is what went into the landfill. Paragraph 58 of the particulars of claim identifies the intangible property on the Hard Drive as the Bitcoin, and in his oral submissions Mr Armstrong KC ended up contending that the Bitcoin were "on" the Hard Drive. That is plainly wrong. Bitcoin are not tangible property and cannot be on the Hard Drive or in the Landfill. Bitcoin are also not intangible property (on this, see the helpful discussion in the Law Commission's Digital Assets: Final report, at paragraphs 3.52 to 3.54), and neither intangible property nor property within the third category has physical location.

Mr Armstrong's late contention is, in fact, contrary to the case advanced in the witness statement of the claimant's solicitor, Mr Manley, which says in paragraph 33 that the Bitcoin "exist independently on the Blockchain, away from the hard drive".

23. Anyway, the defendant has not asserted and does not assert that it is the owner of the Bitcoin. It accepts that it does not own the Bitcoin and that (if it is true, as the claimant says, that he mined them and has not thereafter divested himself of them) the claimant is the owner of the Bitcoin. Mr Goudie KC accepted unequivocally that this was so. The defendant's case is not that it owns the Bitcoin. Its case is that it owns the Hard Drive and that the claimant has no right to have it or to gain access to it. There simply is no issue between the parties about ownership of the Bitcoin.

24. What is on the Hard Drive is at most a digital record of the private key, which is a code provided to the claimant to enable him to operate his cryptocurrency account. Mr Armstrong KC began by accepting in terms that the private key was information, not property. In my judgment that is clearly correct. (See the brief discussion in Bridge et al. eds., The Law of Personal Property, 3rd edition, at paras 10.44 to 10.46.) But any question on the point would be immaterial. The Hard Drive contains not the private key but a record of the private key. The position is no different in principle from what it would be if the record of the private key had been written on a piece of paper that had been put into the landfill. If the claimant had a separate record of the private key, he could use the private key to access the Bitcoin. If the record that in fact exists is a digital file on the Hard Drive, it can indeed be said to be "on" the Hard Drive: a digital record, being mere information, must be embedded in a physical medium. (That, I think, is what the defendant has meant in saying that it owns the Hard Drive and any intangible property on it.) No doubt, the private key is confidential information and its use by others to gain access to the claimant's cryptocurrency account would be unlawful. (See, for example, the remarks of HHJ Pelling QC, sitting as a Judge of the High Court, in *Fetch.AI Ltd v Persons Unknown* [2021] EWHC 2254 (Comm), at [10].) Mr Goudie KC again accepted that, if somehow the defendant were to gain knowledge of the private key, it could not use it to access the claimant's Bitcoin account. There is, again, no issue between the parties on this point. Thus, even if it be arguable that the right to use the private key is capable of constituting property, the claimant's case is not advanced, because the defendant does not claim such a right and the record of the private key on the Hard Drive in the landfill is different from a right to use the private key. Mr Armstrong's submission that, even if the defendant owns the Hard Drive, its refusal to deliver it to the claimant is a wrongful interference with his property rights is a non sequitur and without any proper basis in law.

**The Hard Drive**

25. The primary contention of the defendant is that, even if all the facts asserted by the claimant are true and correct, his claim cannot succeed, because the Hard Drive is the property of the defendant. ...

26. Section 12 of CPA 1974 imposes on each collection authority a duty to arrange for the collection of household waste in its area. Section 14 imposes on each disposal authority a duty to arrange for the disposal of the waste

collected by it in pursuance of section 12; and, for the purpose of the performance of that duty, it empowers each disposal authority to provide places at which to dispose of the waste, plant and equipment for processing or disposing of waste, and places at which to deposit waste before it is transferred to a place or plant and equipment for the sorting and processing of waste: section 14 (1), (3), (4). Section 14 (6) provides:

> ... anything delivered to the authority by another person in the course of using the facilities shall belong to the authority and may be dealt with accordingly.

27. What was delivered to the landfill was the Hard Drive. The defendant's simple contention is this: it is the claimant's case that the Hard Drive was delivered to the Site by "another person", namely his partner at the time; she delivered it "in the course of using the facilities"; and, in those circumstances, the Hard Drive belongs to the defendant and the claimant is not entitled to it.

28. In my judgment, the defendant's argument is correct and provides a complete answer to the claim. ...

**The Equitable Proprietary Claim**

42. In the particulars of claim (paragraphs 51 to 54) the claimant advances what he calls an "equitable proprietary claim". The formulation of the claim is not entirely clear: in paragraph 51 it is put on the basis that, if the defendant is indeed the legal owner of the Hard Drive, it is the constructive trustee for the claimant of "the intangible property contained on the hard drive including the wallet.dat file providing the key to the Bitcoin"; however, paragraphs 52 to 54 aver that the defendant holds the Hard Drive itself on constructive trust for the claimant. Anyway, the gist of the argument is that, if indeed the legal ownership in the property (namely, as explained above, the Hard Drive) has passed to the defendant, the claimant nevertheless has an equitable interest in the property under a constructive trust. ...

45. The claimant's case on constructive trust was not developed before me in any detail. ... The case, as I understand it, is that, if indeed the defendant is the legal owner of the Hard Drive, it held the Hard Drive on trust for the claimant since it learned, in November 2013, that it had received the Hard Drive without the knowledge or consent of the claimant, because he did not know of its disposal, and so holds it on trust for him. This form of trust was considered by Lord Browne-Wilkinson in *Westdeutsche Landesbank Girozentrale*, in the context of a discussion of *Chase Manhattan Bank N.A v Israel-British Bank (London) Ltd* [1981] Ch 105, a case concerning the receipt of money paid under a mistake. He said at [1996] AC 669, 715:

> The defendant bank knew of the mistake made by the paying bank within two days of the receipt of the moneys ... [This fact] may well provide a proper foundation for the decision. Although the mere receipt of moneys, in ignorance of the mistake, gives rise to no trust, the retention of the moneys after the recipient bank learned of the mistake may well have given rise to a constructive trust

46. A claim based on such a trust would, in my judgment, have no realistic prospect of success in the present case. First, the existence of the necessary

equitable interest on the part of the claimant is precluded by section 14(6)(c) of CPA 1974, as already explained. This is the critical point, because it rules out any trusts claim, however formulated.

47. Second, the trust is based on unconscionable retention of property. In my view there would be no realistic prospect of a finding that the defendant's retention of the Hard Drive was unconscionable. The defendant was not retaining it for gain or because it wanted it. It was retaining it because it was buried in landfill. Even by 25 November 2013, when the claimant explained the position to the defendant's officer, Mr Gwyn Jones, at the Site, the Hard Drive was buried and the claimant was able only to identify "which area approximately within the Newport Landfill site the hard drive had been buried in": see paragraphs 56 and 57 of the claimant's witness statement dated 31 March 2024. The claimant has adduced a report prepared for him in March 2021 by Mr Gwyn Jones, according to which in November 2013 the Hard Drive was "probably" located "within an area of approximately 2,000 square metres of the site" and "within an approximate volume of 10,000–15,000 tonnes of waste." It would be a criminal offence for the claimant or anyone acting for him to sort over or disturb any refuse deposited at the Site, unless he were authorised to do so by the defendant: see section 27 of CPA 1974 and section 60 of the Environmental Protection Act 1990. The defendant could only give such authorisation, or excavate the Site itself, if it were first to apply for and obtain a new environmental permit from NRW, as the Schedule of permitted activities in its existing permit does not allow excavation of the Site. The defendant has refused to give authorisation or to apply for a new environmental permit so as to give itself power lawfully to give such authorisation or excavate the Site itself. No challenge to that refusal by way of a claim for judicial review has ever been brought, and such a claim would now be well out of time. In any event, it is fanciful to suppose that the refusal of the defendant to permit disturbance and excavation of the landfill would be held to be unconscionable. For one thing, as already mentioned, there are obvious practical reasons for declining to permit such activities—even if, as the claimant asserts, they could be successfully carried out. But the matter goes further. The case is nothing like the typical case where the property in question is, for example, money sitting in a bank account or a car sitting in a garage, either of which might be readily restored. Here the asset (the Hard Drive) is both within land of which the defendant is in possession and buried under an amount of material of which the defendant is the owner. It did not get into that position by reason of any wrongdoing on the part of the defendant. I see no reasonable basis on which the claimant could assert an entitlement either (i) to require the defendant to excavate its own land to recover his Hard Drive—which, for obvious reasons, is not actually what he is seeking—or (ii) to enter himself onto the defendant's land and interfere with the defendant's property. In the course of oral argument, Mr Armstrong KC suggested that the matter would turn on a balance of competing interests. While that has obvious attraction for the claimant, when the balance is said to be on the one hand a Hard Drive giving access to hugely valuable Bitcoin and on the other hand a pile of rubbish, such a balance has no basis in property law. This seems to me to undermine any claim for delivery of the Hard Drive; more particularly, it undermines the con-

tention that the retention of the Hard Drive in the landfill could be unconscionable.

48. Third, the claimant knew the facts material to his claim by November 2013 but did not commence proceedings until May 2024. In those circumstances, in my judgment, his claim is barred by lapse of time. ...

**YUGA LABS V. RIPPS**
, No. 2:22-CV-04335-JFW-JEM (C.D. Cal.)

MOTION FOR TURNOVER ORDER
Dkt. 514 (filed Apr. 21, 2025)

Plaintiff Yuga Labs, Inc. ("Yuga Labs" or "Judgment Creditor") moves this Court, pursuant to Federal Rules of Civil Procedure, Rule 69(a) and California Code of Civil Procedure ("CCP") § 669.040, for an order compelling defendant and judgment debtor Jeremy Cahen ("Cahen") to turnover possession of crypto assets located within four crypto wallets owned and controlled by Cahen. ...

MEMORANDUM OF POINTS AND AUTHORITIES

Notwithstanding Cahan's professed inability and outright refusal to satisfy any portion of this Court's nearly $9 million judgment (the "Final Judgment"), Cahen holds substantial crypto assets in four crypto wallets that he has placed beyond Yuga Labs' reach. Based on information that Yuga Labs has obtained through post-judgment discovery, Yuga Labs requests that the Court enter an order pursuant to CCP § 699.040 requiring Cahen turnover possession of all crypto assets contained in the following four crypto wallets to the United States Marshals Service ("US Marshals")

1. `bc1q5n2n00w8njg02tkv5mzmp3a25lhe7jm933akay`
2. `bc1qvpzczaswt3qd0n4ttk5mj2za6c5057ym7rfnnz`
3. `bc1q3cy7ehjunq6a4pl9ercderc3ml0ch2lqawvs7f`
4. `0x4424DEb10592aB4aCcE038000e2544aBaC520563`

CCP § 699.040 provides that following the issuance of a writ of execution, a judgment creditor may request an order requiring a judgment debtor "to transfer to the levying officer" either "[p]ossession of the property sought to be levied upon if the property is sought to be levied upon by taking it into custody" or "possession of documentary evidence of title to property of or a debt owed to the judgment debtor that is sought to be levied upon."

Cahen's crypto assets in these four wallets include Bitcoin, Ethereum, and PEPE coin and are specifically identified on the public blockchain ledger. To effectuate the transfer of these assets, the US Marshals require access to the cryptographic keys associated with the wallets. Accordingly, an order from this Court directing the turnover of those keys to the US Marshals is necessary to facilitate enforcement of the Final Judgment.

I. BACKGROUND ON POST-JUDGMENT ENFORCEMENT

On February 2, 2024, this Court entered its Final Judgment against Defendants Ryder Ripps and Cahen (collectively, "Judgment Debtors") for $8,895,346.50, plus attorneys' fees, costs, and post-judgment interest. Cahen did not post a bond to stay execution on the Final Judgment or otherwise obtain a stay of enforcement. *See* Fed. R. Civ. P. 62(b) (providing for the procedures a judgment debtor must fol-

low to stay enforcement of the judgment). The Final Judgment has been enforceable since March 3, 2024.

Shortly after entry of judgment, this Court issued a writ of execution and Yuga Labs commenced post-judgment enforcement efforts to identify and seize Cahen's property subject to the Final Judgment. ...

Yuga Labs has taken affirmative steps under California law essentially every month since the Court issued its Final Judgment to locate and execute upon Cahen's assets. Still, Cahen has made a mockery of this Court's Final Judgement by refusing to pay any portion of the judgment or comply with any post-judgment discovery. Indeed, a cursory review of Cahen's numerous (and frequently banned) X.com accounts show that he regularly flouts his supposed wealth by sitting courtside at Los Angeles Clippers games. Cahen continues to assert—despite not having posted a bond or obtained a stay—that he is not obligated to comply with post-judgment discovery while the appeal is pending. See ECF No. 488 at 5:26–6:1–2 ("Mr. Cahen respectfully submits that post-judgment discovery should be delayed pending the imminent decision from the Court of Appeals..."). As a result, Yuga Labs has been forced to proceed with third-party post-judgment discovery directly from banks and crypto exchanges via subpoena and levy. Cahen has not objected to nor sought a protective order in connection with any of the subpoenas nor levies that Yuga Labs issued to banks and crypto exchanges. Through these discovery efforts, Yuga Labs has identified assets subject to execution.

### II. Gemini Subpoena and Records Subject to This Motion ...

Yuga Labs served a Subpoena on Gemini Trust Company, LLC ("Gemini"), which offers a cryptocurrency exchange and related custodial services, to identify any cryptoassets owned by Cahen (the "Subpoena"). The Subpoena requested records necessary to identify Cahen's assets so that Yuga Labs can satisfy the Final Judgment.

In response to the Subpoena, on January 15, 2025, Gemini produced a spreadsheet of all transactions associated with Cahen's accounts with Gemini, including his account ending in 7560. ...

The spreadsheet indicates that Cahen, while Yuga Labs was attempting to enforce the Final Judgment through a levy directed at Gemini, transferred his cryptoassets to two distinct cryptowallets.

First, on October 21 and 22, 2024, Cahen transferred a total of 2.000 Bitcoin ("BTC") to a cryptowallet with the blockchain address:

- `bc1q5n2n00w8njg02tkv5mzmp3a25lhe7jm933akay` (the "First Wallet").

BTC, the native cryptocurrency of the Bitcoin blockchain, had a market value of approximately $67,367 per coin at that time. Accordingly, the total value of Cahen's transfer to the First Wallet was approximately $134,734.

Then, on October 28, 2024, Cahen split the remaining 2.000 BTC stored in the First Wallet into two equal parts. He transferred 1.000 BTC to each of two additional cryptowallets with the following blockchain addresses:

- `bc1qvpzczaswt3qd0n4ttk5mj2za6c5057ym7rfnnz` (the "Second Wallet"),

and

- `bc1q3cy7ehjunq6a4pl9ercderc3ml0ch2lqawvs7f` (the "Third Wallet").

As of the date of this filing, the BTC remains in those wallets.

Second, the Gemini transaction records reflect that on October 25, 2024—just one day after the levy was served on Gemini—Cahen transferred 107.640597982645 ETH to a cryptowallet with the blockchain address:

- `0x4424DEb10592aB4aCcE038000e2544aBaC520563` (the "Fourth Wallet").

ETH, the native cryptocurrency of the Ethereum blockchain, had a market value of approximately $2,436 at that time. This transfer amounted to a value of approximately $262,212.[2]

In total, Cahen moved $396,946 worth of cryptoassets to avoid the duly served levy. These non-exempt assets are still in Cahen's possession. ...

## IV. ARGUMENT

### A. Yuga Labs Has Shown the Need for a Court Order Granting the Levying Officer Access to Cahen's Cryptowallets Due to His Dilatory Tactics in Hiding Cryptoassets

Upon receipt of a judgment and corresponding writ of execution, a judgment-debtor may levy upon property owned by a judgment creditor. See CCP 695.010(a) (". . . all property of the judgment debtor is subject to enforcement of a money judgment). Accordingly, because digital assets, such as cryptoassets located within cryptowallets, are property, they are appropriately subject to a levy from a judgment creditor.

Here, as reflected in the Gemini records, Cahen possesses cryptoassets held within the cryptowallets, which are subject to enforcement and may be used to satisfy Yuga Labs' Final Judgment. However, to effectuate the transfer of these assets, the US Marshals require access to the cryptographic keys associated with the wallets to which Cahen transferred the assets. Accordingly, an order from this Court directing the turnover of those keys is necessary to facilitate enforcement of the judgment, as these assets are subject to the levy previously served upon Gemini.

Thus, pursuant to CCP § 669.040, this Court may order the transfer of Cahen's cryptoassets, or access to the cryptoassets in his cryptowallets via private key, to the US Marshals. In fact, a court in this District has previously ordered a defendant to provide cryptowallet identification numbers and corresponding electronic access keys to the US Marshals as necessary to satisfy an attachment order, and held the defendant in contempt for failing to do so. *See Handley v. La Melza*, Case No. 2:22-cv-00797-MCS-MARx, 2022 WL 3137718 (C.D. Cal. July 13, 2022) ("... this Court's [Orders] required Defendant to: (3) Provide the electronic access key for each cryptocurrency wallet in Defendant's Possession.").

All that is required for this Court to order the turnover of Cahen's cryptoassets is a showing of "need" pursuant to CCP § 669.040. Courts in this District have previously found this "need" requirement is met when a judgment debtor commits dilatory tactics to avoid payment of the judgment. *See UMG Recordings, Inc. v. BCD Music Group, Inc.*, No. CV 07-05808 SJO (FFMx), 2009 WL 2213678, at *4 (C.D. Cal. July 9, 2009) (judgment debtor refused to pay the judgment; the court held that judgment debtor's "behavior in refusing to pay any portion of the settlement amount or judgment suffices to demonstrate the need for such an order.").

Here, Cahen's dilatory tactics are apparent. On October 24, 2024, the US Marshals served Gemini with a writ of execution, notice of levy, and memorandum of

---

2 A review of the Fourth Wallet on the public blockchain reveals that Cahen also holds PEPE assets in the same location.

garnishee, targeting all funds and accounts held in Cahen's name or for his benefit. Following this action, the US Marshals provided notice to Cahen himself, ensuring he was aware of the levy. However, in a clear attempt to sidestep his financial responsibilities, Cahen transferred his ETH from Gemini to the Fourth Wallet on October 25, 2024, just one day after the levy was served. This transfer occurred before Gemini froze his accounts, showing a deliberate and calculated move to shield his assets from the Final Judgment. Cahen's actions here are not those of an individual passively awaiting the collection process but rather an intentional effort to evade payment at all costs. This pattern of behavior is a transparent attempt to frustrate the enforcement of the Final Judgment.

This intentional attempt to evade lawful enforcement highlights the urgent need for judicial intervention.... In light of Cahen's deliberate transfer of assets following the levy, it is essential that the Court order him to turn over the cryptoassets contained in his digital wallets to prevent the Final Judgment from being effectively nullified....

As evidenced by Cahen's transfer of BTC and ETH to the cryptowallets, Cahen owns the cryptowallets, which, at the end of October, contained Cahen's transferred cryptoassets with a value of nearly $396,946 USD. Cahen's ownership of the cryptowallets is further bolstered by the fact that Gemini's records indicate that these were the sole accounts Cahen transferred his assets, which were previously located within his personal Gemini account. Therefore, a turnover order directing Cahen to either surrender or provide access to these cryptowallets for the levying officer is necessary and appropriate to satisfy the Final Judgment.[4]

## OPPOSITION TO MOTION

Dkt. 517 (filed May 5, 2025)

Defendant Jeremy Cahen respectfully opposes Plaintiff Yuga Labs, Inc.'s misplaced request for a turnover order ... .

### III. Arguments

Yuga has failed to satisfy two of the requirements for a turnover motion: Mr. Cahen does not possess the property Yuga seeks and Yuga seeks intangible property that cannot be subjected to a turnover order. Accordingly, this court should overrule their motion.

#### a. Yuga seeks property outside Mr. Cahen's possession

Yuga demands the impossible: that Mr. Cahen turnover property that he does not possess. A turnover order is only "appropriate where.... the judgment debtor is in possession of that property." *Ally Fin., Inc. v. Claremont Hyundai, LLC*, No. CV 19-7858 PSG (KSX), 2022 WL 1839075, at *1 (C.D. Cal. Feb. 8, 2022). Courts deny turnover orders when the judgment debtor does not possess the property in question. *See Palacio Del Mar Homeowners Assn., Inc. v. McMahon*, 95 Cal. Rptr. 3d 445, 449 (2009) (holding that "the turnover order is wrongly directed at [the debtor] because [the creditor] has not shown the domain name is in his possession."); *Ally Fin., Inc.*, 2022 WL 1839075, at *2 (holding that a turnover order was not appropriate as the creditor's "own evidence suggests that [the debtor] does not have possession of the funds [the creditor] seeks."). The statute itself provides "for

4 While Cahen may argue that the current evidence does not establish his ownership of the cryptowallets, his continued refusal to comply with post-judgment discovery is precisely what has prevented Yuga Labs from obtaining additional evidence.

an order directing *the judgment debtor* to transfer" property to the levying officer. CCP § 699.040 (a) (emphasis added). A judgement debtor cannot transfer what they do not possess.

Yuga has pointed only to evidence that some crypto assets were transferred into the wallets it seeks access to in a weak attempt to establish ownership. As his declaration makes clear, however, Mr. Cahen does not own any of the four crypto wallets Yuga seeks in its turnover request. [Cahen declared, "1. I do not own, possess, or control the following four crypto wallets … 2. I do not own season tickets to the Los Angeles Clippers."] Mr. Cahen cannot turnover crypto wallet keys that he does not own. Accordingly, the court must deny Yuga's turnover request.

**b. Yuga impermissibly seeks the turnover of intangible assets**

Not only does Yuga demand Mr. Cahen turnover property that he does not possess, the crypto wallets Yuga seeks are intangible assets that cannot be subjected to a turnover order. It is well established that section 699.040 has a limited scope and applies only "to tangible property that can be 'levied upon by taking it into custody' (or tangible, 'documentary evidence of title' to property or a debt)." *Palacio Del Mar Homeowners Assn., Inc.*, 95 Cal. Rptr. 3d at 448–49. As the statute itself makes clear, it applies to property that can be "levied upon by *taking it into custody*." CCP § 699.040 (a)(1) (emphasis added). Courts interpreting this statute have denied turnover requests where the property sought is an intangible asset. *See Ally Fin., Inc.*, 2022 WL 1839075, at *2 (denying a turnover request where the property sought was a right to payment); *Palacio Del Mar Homeowners Assn., Inc*, 95 Cal. Rptr. 3d at 448–49 (2009) (denying a turnover request where the property sought was a domain name registration); *Pac. Decision Scis. Corp. v. Superior Ct.*, 18 Cal. Rptr. 3d 104, 109-110 (2004) (interpreting the analogous Cal. Civ. Proc. Code § 482.080 and holding that a turnover was not authorized for an account receivable and a deposit account).

Here, Yuga seeks access to several crypto wallets and the multitude of crypto assets contained within them. Crypto wallets, unlike a traditional bank account, exist on the blockchain and can contain not only (intangible) cryptocurrency but an assortment of intangible digital assets and art, such as non-fungible tokens. Cyrpto wallets are intangible property that cannot be subjected to a turnover order. Accordingly, Yuga's motion is improper and should be denied.

REPLY IN SUPPORT OF MOTION
Dkt. 524 (filed May 12, 2025)

Plaintiff Yuga Labs, Inc. hereby replies to judgment debtor Jeremy Cahen's opposition to Yuga Labs' Motion For Turnover Order. …

**I. The Court Should End Cahen's Obvious Obstruction …**

**a. Crypto Is Tangible Property As Provided by this District's Precedent.**

Cahen's argument that California Code of Civil Procedure section 699.040 precludes a levying officer from taking possession of cryptographic keys or Wallet access is a misapplication of case law. The authority Cahen cites addresses the turnover of legal rights—not digital assets like cryptocurrency, which the IRS has expressly classified as property. *See Ally Fin.* (requesting that rights to payment be turned over); *Palacio Del Mar* (requesting that the rights to a domain name be turned over); *Pac. Decision Scis.* (requesting the right to access an account receivable).

Accordingly, Cahen's argument fails to account for the fundamental distinction between intangible legal rights and tangible digital property, rendering his interpretation of section 699.040 inapplicable to cryptocurrency.

Crypto assets qualify as property and are therefore the proper subject of a turnover order. Critically, Cahen's opposition fails to even address the case cited by Yuga Labs wherein a court in this District ordered that a judgment debtor turn over electronic access keys to cryptocurrency held in digital wallets. *See Handley* ("...this Court's [Orders] required Defendant to: (3) Provide the electronic access key for each cryptocurrency wallet in Defendant's Possession."). This establishes that, under existing legal precedent, cryptocurrency and its access keys (which are undoubtedly real values that can be written down and transmitted) are properly subject to turnover orders, reinforcing the applicability of section 699.040 in the enforcement of judgments involving digital assets. Indeed, the Opposition admits the digital assets can be turned over. Opp. at 3 ("Mr. Cahen promptly and completely complied with the injunction this Court ordered, including turning over to Yuga the crypto assets that were subject of the Court's injunction."). Cahen therefore concedes the argument that crypto assets cannot be turned over.

**b. Cahen's Possession, Control of, or Access to, the Wallets Is Clear.**

Cahen's mere assertion in a self-serving declaration, without any detail, that he does not own the Wallets is insufficient to rebut a record which shows Cahen transferred crypto assets from a Gemini Trust Company, LLC ("Gemini") account held in his name to the Wallets the very same day a levy was served on Gemini.

Indeed, Cahen simply declares, without any facts or supporting evidence, that he does not own, possess, or control the Wallets identified in the Motion. SThis declaration fails to answer several crucial points, including: (1) whether Cahen currently has access to the assets contained in the Wallets via a cryptographic key or other means; (2) why Cahen transferred his crypto assets that were held in his own personal Gemini account to these Wallets after a levy was served on Gemini; (3) whether any entities he controls, is involved with, or has an interest in presently has ownership, possession, control of, or access to, the Wallets; and relatedly, (4) if Cahen does not own the Wallets, who, or what, allegedly owns, possesses, or controls the Wallets and what their relationship is to Cahen. Without these answers, the declaration utterly fails to adequately explain the asset transfers and only raises further legitimate concerns about asset concealment. ...

Cahen's assertion that these transfers do not establish his ownership or control over the receiving Wallets is unavailing. Ownership in the context of cryptocurrency can be often inferred from control—specifically, the ability to initiate transfers. The fact that Cahen moved significant assets from his verified personal exchange account to specific Wallets, during a time when his account was subject to a levy, demonstrates he owns the assets now located within these Wallets. Moreover, no evidence has been presented to suggest that any third party directed or had access to Cahen's exchange account or the Wallets themselves. In the absence of any alternative explanation, the pattern of transfers is consistent with an intent to shield assets he continued to control. The Court can appropriately order that Cahen provide the levying officer all cryptographic keys in his possession which will provide access to the assets identified in the Gemini records.

## NOTES AND QUESTIONS

1. After the turnover motion was briefed, but before it was argued or decided, the Ninth Circuit reversed the trial court's grant of summary judgment in

favor of Yuga Labs on its trademark claims. This mooted the turnover motion, as there was no longer a monetary judgment against the defendants subject to collection.

2. Is a cryptocurrency "property" that can be "tak[en] into custody? Is it "documentary evidence of title to property?"
3. Look closely at the list of things for which turnover was rejected in the cases cited by Cahen: a "right to payment" (*Ally Financial)*, a "a domain name registration" (*Palacio Del Mar*), and "an account receivable and a deposit account" (*Pacific Decision Sciences*). What kinds of things are these? How (if at all) would you take them into possession? Do you think that the California legislature intended for them not to be subject to turnover *at all*, or not to be subject to turnover *using this procedure*? Does this exercise shed any light on how cryptocurrencies should be treated?

## AA V. PERSONS UNKNOWN

England and Wales High Court (Commercial Court)
[2019] EWHC 3556 (Comm)

*Mr. Justice Bryan:*

### Introduction

1. There is before me today an application made by an applicant, an English insurer who requests to be anonymised, against four defendants. Those four defendants are: the first defendant, persons unknown who demanded Bitcoin on 10th and 11th October 2019; the second defendant, persons unknown who hold/controls 96 Bitcoins held in a specified Bitfinex Bitcoin address; the third defendant, iFINEX Inc trading as Bitfinex; and the fourth defendant, BFXWW INC also trading as Bitfinex.

### Background

2. The application relates to the hacking of a Canadian insurance company that I will refer to simply as the Insured Customer. What happened in relation to that company is that a hacker managed to infiltrate and bypass the firewall of that insured customer, who happens to be an insurance company, and installed malware called BitPaymer. The effect of that malware was that all of the insured customer's computer systems were encrypted, the malware having first bypassed the system's firewalls and anti-virus software. The Insured Customer then received notes which were left on the encrypted system by the first defendant. In particular, there was a communication from the first defendant as follows:

> Hello [insured customer] your network was hacked and encrypted. No free decryption software is available on the web. Email us at [...] to get the ransom amount. Keep our contact safe. Disclosure can lead to impossibility of decryption. Please use your company name as the email subject.

3. The Insured Customer is insured with the applicant, (an English insurer), whom I shall refer to as "the Insurer"/"the Applicant". ... The Insurer instructed, as is common in such cases, what is known as an Incident Response Company (IRC) that specialises in the provision of negotiation services in relation to crypto currency ransom payments. The Insured Customer is insured with the Insurer against cyber crime attacks.

4. That entity, IRC, then was instructed by the Insurer to correspond with the first defendant on behalf of it and the Insured Customer so as to negotiate the provision of the relevant decryption software (the tool) which would allow the Insured Customer to re-access its data and systems. Following initial emails from IRC asking the first defendant: "*To relay your terms of decryption*" the first defendant stated "*Hello, to get your data back you have to pay for the decryption tool, the price is $1,200,000 (one million two hundred thousand). You have to make the payment in Bitcoins.*" [The price was negotiated down to $950,000, to be paid by sending Bitcoin to a specified address. The Insurer made the transfer and the hacker provided the decryption tool.] ...

11. The tool was a click through application that had to be executed on each of the Insured Customer's encrypted systems. The time it took to decrypt the data varied from system to system due to the quantity of the files on each system and the system's own resources, like processor and memory. The information before me is that it took decryption of 20 servers of the Insured Customer five days and 10 business days for 1,000 desktop computers.

12. Following the payment of the ransom and the provision of the decryption tool, further investigations were undertaken on behalf of the Insurer by an employee ...

13. Those investigations involved contacting a specialist company who is a provider of software to track payment of crypto currency. That company is Chainalysis Inc, which is a blockchain investigations firm operating in New York, Washington DC, Copenhagen, and London. ...

14. In the present case, it was possible to track the Bitcoins that had been transferred as a ransom. Whilst some of the Bitcoins was transferred into "fiat currency" as it is known, a substantial proportion of the Bitcoin, namely, 96 Bitcoins, were transferred to a specified address. In the present instance, the address where the 96 Bitcoins were sent is linked to the exchange known as Bitfinex operated by the third and fourth defendants.

15. The Insurer is unable to identify the second defendant from the Bitcoin address referred to but that is information which is either held or likely to be held by the third and fourth defendants, to comply with their Know Your Customer ("KYC"), an anti-money laundering requirement.

**APPLICATION FOR HEARING TO BE IN PRIVATE ...**

21. It is well established, as is acknowledged in this case by the Insurer, that the general principle that hearings be held in public is not to be lightly departed from in respect of civil proceedings. It is submitted, however, that there are compelling grounds, supported by credible and cogent evidence, as to why in this particular, and unusual, case the hearing should be held in private ...

22. I am satisfied that this is an appropriate case for the hearing to be heard in private ... . First of all, I am satisfied ... that publicity would defeat the object of the hearing. It would potentially tip off the persons unknown to enable them to dissipate the Bitcoins; secondly, there would be the risk of further cyber or revenge attacks on both the Insurer and the Insured Customer by persons unknown; there would be a risk of copycat attacks on the Insurer and/or the Insured Customer and I am satisfied that in all the circum-

stances it is necessary to sit in private so as to secure the proper administration of justice. ...

36. I also consider it is appropriate to anonymise the Insurer in the terms that I have identified, again because of the risk of retaliatory cyber attacks upon the Insurer just as much as upon the Insured Customer.

37. It is likely that once the first and second defendants are served and/or the property is protected, I will lift the privacy in respect of this judgment so that it can be publically reported. It has been drafted in terms that will allow that to be done. The public reporting of judgments is an important aspect of the principle of open justice. ...

**PROPRIETARY INJUNCTION APPLICATION ...**

52. ... The Insurer has paid out the sum of $950,000, that $950,000 is property belonging to the Insurer, that was used to purchase Bitcoin and the proceeds of that money can be traced into the accounts with Bitfinex, so says Mr. Connell. Those Bitcoins are being held by Bitfinex as constructive trustee on behalf of the Insurer and/or the Insurer has restitutionary claims against the third and fourth defendants who are actually holding and have possession of property which belongs to the Insurer and to which they have no right to themselves and, equally, against the first and second defendants, who are the account holders of those accounts, who have wrongfully extorted that money and have no right to the money that belongs to the Insurer. ...

55. Turning then to the relevant principles in relation to the granting of a proprietary injunction, the first and perhaps fundamental question that arises in relation to this claim for a proprietary injunction is whether or not in fact the Bitcoins, which are being held in this account of the second defendant with the third or fourth defendants are property at all. Prima facie there is a difficulty in treating Bitcoins and other crypto currencies as a form of property: they are neither chose in possession nor are they chose in action. They are not choses in possession because they are virtual, they are not tangible, they cannot be possessed. They are not choses in action because they do not embody any right capable of being enforced by action. That produces a difficulty because English law traditionally views property as being of only two kinds, choses in possession and choses in action.

59 ... I consider that a crypto asset such as Bitcoin are property. They meet the four criteria set out in Lord Wilberforce's classic definition of property in *National Provincial Bank v Ainsworth* [1965] 1 AC 1175 as being definable, identifiable by third parties, capable in their nature of assumption by third parties, and having some degree of permanence. That too, was the conclusion of the Singapore International Commercial Court in *B2C2 Limited v Quoine PTC Limited* [2019] SGHC (I) 03 [142].

60. There are also two English authorities to which my attention has been drawn where crypto currencies have been treated as property, albeit that those authorities do not consider the issue in depth. They are, and I have already mentioned them, in *Vorotyntseva v Money -4 Limited t/a as Nebeus .com* [2018] EWHC 2598 (Ch) the decision of Birss J, where he granted a worldwide freezing order in respect of a substantial quantity of Bitcoin and Ethereum, another virtual currency, and the case of *Liam David Robertson* (unreported 15th July 2019), where Moulder J granted an asset preservation order over crypto currencies in that case. ...

61. I am satisfied for the purpose of granting an interim injunction in the form of an interim proprietary injunction that crypto currencies are a form of property capable of being the subject of a proprietary injunction.

62. I therefore turn to the applicable principles in relation to a proprietary injunction. The basis upon which proprietary injunction is sought in respect of stolen funds is summarised in McGrath Commercial Fraud in Practice, 2nd edition, at paragraph 6.247 to 6.261. As Lord Browne-Wilkinson noted in *Westdeutsche Landesbank v Islington LBC* [1996] AC 669, when property is obtained by fraud equity imposes a constructive trust on the fraudulent recipient, the property is recoverable and traceable in equity. As confirmed by Scott J in *Poly Peck International PLC v Nadir (No.2)* [1992] 4 All ER 769, the *American Cyanamid* principles apply to a proprietary injunction. First there must be a serious issue to be tried, secondly, if there is a serious issue to be tried, the court must consider whether the balance of convenience lies in granting relief sought. The balance of convenience involves consideration of the efficacy of damages as an adequate remedy, the adequacy of the cross- undertaking as to damages, and the overall balance of convenience, including the merits of the proposed claim.

63. As I say and for the reasons I have given, I am satisfied at least to the level required for the purposes of this application for interim relief that Bitcoins constitute property. I am satisfied that the test for a proprietary injunction against each of the four defendants, is also satisfied, that there is a serious issue to be tried as between the insurer and each of the four defendants in relation to the proprietary claims which I have identified, in relation to that Bitcoin which represents the proceeds of the monies paid out by the Insurer. Clearly, the ultimate strength of the claim against each of the four defendants is not a matter for determination before me today. I am satisfied that there is at least a serious issue to be tried against all four defendants. I should say that so far as the first and second defendants are concerned, I consider that the claims are very strong because those would appear to be those defendants who in fact committed the extortion and blackmail and obtained by way of ransom the sums concerned.

64. The position is less clear in relation to the third and fourth defendants who may simply have got mixed up in another's wrongdoing but certainly they are, as I understand it, holding Bitcoin which belongs to the claimant which has (arguably) come into their possession in the furtherance of a fraud and in circumstances where they have no entitlement to retain that Bitcoin if the claimant demonstrates it is entitled to the relief which it seeks.

65. Therefore, I am satisfied that there is at least a serious issue to be tried which is all that is requited at this stage for an interim injunction. I am satisfied that the balance of convenience lies firmly in favour of granting relief in furtherance the Insurer's claimed proprietary rights. Equally I am satisfied that damages would not be an adequate remedy in circumstances where the 96 Bitcoins could be dissipated and I am satisfied that the insurer has a strong claim to the Bitcoins in question. ...

66. However, in addition to a proprietary injunction, there is also ancillary relief as is usual in terms of providing information so that location of assets etc and where monies have moved to, for example, can be obtained. That is particularly apposite in the case of the first and second defendants, of course,

because some of the money has in fact been converted into fiat currency but, equally, it may well be the case that because of the very rapid speed at which Bitcoins could be moved, that by the time this injunction is obtained that in fact some or all of the Bitcoins may have moved from the particular exchange or the particular account within that exchange and ancillary information in relation to that is needed. ...

81. The other aspect of the injunction, the proprietary injunction, is an application that information be provided both in terms of the identity and address of D3 and D4 and that applies to all four defendants, i.e. that D3 and D4 identify D1 and D2, equally D1 and D2 have to identify themselves, including their address, and any associated information that D3 and D4 may have in relation to D1 and D2. I am satisfied that that information is necessary to police the proprietary injunction that I have granted for the reasons that I have said and also I consider that the associated information would also be appropriate to be provided by way of pre-action disclosure in the action which the claimant is undertaking to commence forthwith against all four defendants. I will hear counsel in terms of the finalisation of the precise form of information to be provided. ...

# C. Ownership

**UNIFORM COMMERCIAL CODE [CONTROLLABLE ELECTRONIC RECORDS]**
art. 12: Controllable Electronic Records (2022)

**§ 12-102 – *Definitions.***

(a) ***Article 12 definitions.*** In this article:

(1) "Controllable electronic record" means a record stored in an electronic medium that can be subjected to control under Section 12-105. The term does not include a controllable account, a controllable payment intangible, a deposit account, an electronic copy of a record evidencing chattel paper, an electronic document of title, electronic money, investment property, or a transferable record. [Ed: these are all terms defined elsewhere in the UCC or other statutory commercial law, and which are subject to their own specific legal regimes.]

(2) "Qualifying purchaser" means a purchaser of a controllable electronic record or an interest in a controllable electronic record that obtains control of the controllable electronic record for value, in good faith, and without notice of a claim of a property right in the controllable electronic record.

**§ 12-104 – *Rights in Controllable Account, Controllable Electronic Record, and Controllable Payment Intangible. ...***

(c) ***Applicability of other law to acquisition of rights.*** Except as provided in this section, law other than this article determines whether a person acquires a right in a controllable electronic record and the right the person acquires.

(d) ***Shelter principle and purchase of limited interest.*** A purchaser of a controllable electronic record acquires all rights in the controllable electronic record that the transferor had or had power to transfer, except that a purchaser of a limited interest in a controllable electronic record acquires rights only to the extent of the interest purchased.

(e) ***Rights of qualifying purchaser.*** A qualifying purchaser acquires its rights in the controllable electronic record free of a claim of a property right in the controllable electronic record. ...

(f) ***Limitation of rights of qualifying purchaser in other property.*** Except as provided in subsections (a) and (e) for a controllable account and a controllable payment intangible or law other than this article, a qualifying purchaser takes a right to payment, right to performance, or other interest in property evidenced by the controllable electronic record subject to a claim of a property right in the right to payment, right to performance, or other interest in property. ...

**§ 12-105 – *Control of Controllable Electronic Record.***

(a) ***General rule: control of controllable electronic record.*** A person has control of a controllable electronic record if the electronic record, a

record attached to or logically associated with the electronic record, or a system in which the electronic record is recorded:

(1) gives the person:

(A) power to avail itself of substantially all the benefit from the electronic record; and

(B) exclusive power, subject to subsection (b), to:

(i) prevent others from availing themselves of substantially all the benefit from the electronic record; and

(ii) transfer control of the electronic record to another person or cause another person to obtain control of another controllable electronic record as a result of the transfer of the electronic record; and

(2) enables the person readily to identify itself in any way, including by name, identifying number, cryptographic key, office, or account number, as having the powers specified in paragraph (1).

(b) ***MEANING OF EXCLUSIVE.*** ... a power is exclusive under subsection (a)(1)(B)(i) and (ii) even if:

(1) the controllable electronic record, a record attached to or logically associated with the electronic record, or a system in which the electronic record is recorded limits the use of the electronic record or has a protocol programmed to cause a change, including a transfer or loss of control or a modification of benefits afforded by the electronic record; ...

## NOTES AND QUESTIONS

1. Article 12 was adopted in 2022 to provide some baseline coverage of cryptocurrencies and other blockchain (or "distributed ledger") assets. (As of 2026, it has been enacted in 34 jurisdictions.) Does the definition of "controllable electronic record" in § 12-101(a)(1) do a good job of scoping the article?
2. Like much of the UCC, Article 12 is dense and not at all self-explanatory. The key passage is § 12-104(e): a good-faith purchaser provision that adopts the rule of *Miller v. Race*. Do you see how that rule follows from the text of the subsection? Once you do, read the definition of "qualifying purchaser" in § 12-102(a)(1) to understand who qualifies for the rule's protection.
3. Notice that Article 12 uses the concept of "control" rather than possession. "Control" is defined in § 12-105(a). Does the definition get the concept right? Should this definition apply to other digital intangibles? Notice also that control must be "exclusive," § 12-105(a)(1)(B), but that "exclusive" does not have to be completely exclusive, § 12-105(b)(1). What kinds of situations might have prompted the drafters of Article 12 to specify these details?
4. If Article 12 had been the law of the relevant jurisdictions, would it have changed the outcome or analysis in *Howell*, *Yuga Labs*, or *AA v. Persons Unknown*?

**IN RE CELSIUS NETWORK LLC**
647 B.R. 631 (Bankr. S.D.N.Y. 2023)

*Martin Glenn, Chief United States Bankruptcy Judge:*

Who owns the cryptocurrency assets deposited in Earn Accounts (defined below) by Celsius's account holders before the July 15, 2022 petition date? This is a gating issue at the center of many disputes in this case. As explained below, the Court concludes, based on Celsius's unambiguous Terms of Use, and subject to any reserved defenses, that when the cryptocurrency assets (including stablecoins, discussed in detail below) were deposited in Earn Accounts, the cryptocurrency assets became Celsius's property; and the cryptocurrency assets remaining in the Earn Accounts on the Petition Date became property of the Debtors' bankruptcy estates.

At the Petition Date, Celsius had approximately 600,000 accounts in its Earn program. These Earn Accounts held cryptocurrency assets with a market value of approximately $4.2 billion as of July 10, 2022. Included in the Earn Accounts at the Petition Date were a type of cryptocurrency known as stablecoins, valued at $23 million as of September 2022.

The issue of ownership of the assets in the Earn Accounts is a contract law issue. The Debtors and Committee argue that the cryptocurrency assets deposited in Earn Accounts were owned by the Debtors and are now property of the Estates. Many Earn account holders argue that the Account Holders, rather than Celsius, own the cryptocurrency assets in the Earn Accounts and that cryptocurrency assets should promptly be returned to them. ...

If the cryptocurrency assets in the Earn Accounts are owned by the Debtors, the Account Holders are unsecured creditors and their recovery depends on the distributions to unsecured creditors under a confirmed chapter 11 plan, or under the Bankruptcy Code's priority rules in the event of liquidation. A fundamental principle of the Bankruptcy Code is equality of distribution. There simply will not be enough value available to repay all Account Holders in full. If only some Account Holders prevail with their arguments that they own the cryptocurrency assets in their accounts, they hope to recover 100% of their claims, while most of the Account Holders are left as unsecured creditors and may recover only a small percentage of their claims. ...

## II. LEGAL STANDARD

### A. Property of the Bankruptcy Estate Under the Bankruptcy Code

The Debtors contend that the Earn Assets are property of the Estates. Section 541 of the Bankruptcy Code provides, in relevant part, that:

> (a) The commencement of a case under section 301, 302, or 303 of this title creates an estate. Such estate is comprised of all the following property, wherever located and by whomever held:
>
> (1) Except as provided in subsections (b) and (c)(2) of this section, all legal or equitable interests of the debtor in property as of the commencement of the case.

11 U.S.C. § 541(a)(1).

The Estates therefore consist of all legal or equitable interests of the debtor in property as of the commencement of the case.

## III. DISCUSSION ...

### A. Ownership of Earn Assets

[The court held that the Celsius terms of service formed a valid and enforceable contract with users.]

#### *3. The Terms of Use Unambiguously Transfer Ownership of Earn Assets to the Debtors*

Having established that a valid contract was formed between the Debtors and its Account Holders, the Court's next inquiry is if the Terms of Use are unambiguous with respect to whether Account Holders retained ownership or transferred ownership of cryptocurrency assets by depositing the assets into Earn Accounts. ...

Terms Version 5 introduced the transfer of title clause that has been the subject of scrutiny in this matter. Every version of the Terms of Use beginning with Terms Version 5 includes a clause that Account Holders "grant Celsius ... all right and title to such Digital Assets, including ownership rights." Account Holders who agreed to Terms of Use Version 5 or later, whether by signing up for the first time or by continuing to use the platform with an existing account, entered a contract which contained unambiguous and clear language regarding transfer of title and ownership of assets in Earn Accounts. At the hearing on this matter, Blonstein testified that 90% of Account Holders representing 99% of Earn Assets had assented to Terms Version 6 or later. Thus, the Court finds that title to and ownership of all Earn Assets unequivocally transferred to the Debtors and became property of the Estates on the Petition Date.

The crux of many objections to the Amended Motion is that Celsius's ubiquitous use of the word "loan," "lending," and other variations sits in direct conflict with the singular clause transferring all title and rights of ownership to the Debtors. These responses argue that this creates an ambiguity within the four corners of the contract. But the use of the term "loan," or variations of that term, do not contradict transfer of ownership of cryptocurrency assets to Celsius. The Account Holders argue that a layperson's understanding of the term "loan" means the Account Holder retains ownership of their Earn Assets but temporarily allows the use of the assets by the Debtors—but the Court cannot ignore the plain and clear language in the Transfer of Title Clause.

Further, even if the Court found that Account Holders loaned digital assets to Celsius, Account Holders would still be unsecured creditors. It is blackletter law that a loan of money or property to another creates a debtor-creditor relationship. *In re Masterwear Corp.*, 229 B.R. 301, 310 (Bankr. S.D.N.Y. 1999) ("Under New York law, a bank and its depositor stand in a debtor-creditor relationship that is contractual in nature. The bank owns the deposit, the depositor has a claim to payment against the bank, and the bank has a corresponding obligation to pay its depositor. Accordingly, a bank's temporary freeze of an account, without more, is neither a taking of possession of the depositor's property nor an exercising of control over it, but merely a refusal to perform its promise.") And absent a perfected security interest in tangible or intangible property, in the event of the debtor's bankruptcy, the creditor holds only an unsecured claim. ...

But, more importantly:

> By current definition, cryptocurrency is not money because it is not a medium of exchange created, authorized, or adopted by a domestic or foreign government, or by an intergovernmental organization or by agreement between two or more countries. Moreover, since cryptocur-

> rency, NFTs and other digital assets are intangible and therefore not capable of possession, a security interest currently can be perfected only by the filing of a financing statement in the digital asset as a general intangible.

Lorraine S. McGowen, *Transferring Digital Assets (Inclluding Cryptocurrencies) Under Proposed Amendments to the Uniform Commerical Code*, THE QUARTERLY JOURNAL OF INSOL INTERNATIONAL, 4th Quarter 2022, at 16 (discussing proposed amendments to the Uniform Commercial Code, creating a new Chapter 12 to govern the transfer (whether as a sale or as a financing) of digital assets, including cryptocurrency, digital tokens and non-fungible tokens).

Thus, even if the parties' contract purports to provide the creditor with a security interest in property, unless the security interest is perfected under applicable non-bankruptcy law, a trustee can assert strong-arm power under section 544(a) of the Bankruptcy Code to avoid the lien. 11 U.S.C. § 544(a). *See also In re Castle Ventures, Ltd.*, 167 B.R. 758, 765 (Bankr. E.D.N.Y. 1994) ("However, section 544(a) of the Code, also referred to as the 'strong arm' clause, allows a trustee in bankruptcy to avoid liens and security interests against the debtor's estate which were not properly perfected under state law prior to the debtor's bankruptcy filing.").

Here, the language in the Terms of Use transferring all ownership interest to Celsius in the cryptocurrency assets deposited in the Earn Accounts makes it very clear that no ownership interest or lien in favor of the Account Holders was intended.[37] And certainly no lien in favor of the Account Holders was perfected. *U.S. v. Joyeros*, 410 F. Supp. 2d 121, 125 (E.D.N.Y. 2006) ("General, unsecured creditors lack a particularized interest in specific assets. Although general creditors can claim an interest in their debtors' estates, they cannot claim an interest in any *particular* asset that makes up that estate." (emphasis added)); *see also In re Castle Ventures, Ltd.*, 167 B.R. at 765 ("If an unperfected security interest is avoided by the trustee, the secured creditor loses the lien and is reduced to the status of a general unsecured creditor.").

To read the Terms of Use such that "loan" overrides the unequivocal language transferring title and ownership of assets deposited into Earn Accounts to Celsius would be to read the Transfer of Title Clause out of the contract entirely. As the Committee notes, "it is a bedrock principle of contract interpretation that courts should not adopt an interpretation of a contract that has the effect of rendering at least one clause superfluous or meaningless, but rather, to the extent possible, should seek to read contractual provisions in harmony."

The Court can read "lend" in harmony with the Transfer of Title Clause, and the transfer of title and the creation of a loan are not mutually exclusive concepts. As an example, the Committee notes that, in the securities context, it is common for a loan of securities to a broker to also constitute a transfer of title thereto (or the incidents of ownership thereof) so that the broker can sell, lend, hypothecate, or rehypothecate the securities. In that instance, title to the securities is transferred to the securities broker, and the securities broker has a contractual obligation to return equivalent securities (but not the exact same securities) to the initial transferor.

---

37 See Terms of Use Version § 4.D (not granting a security interest to users and, to the contrary, providing that "once such Eligible Digital Assets are received by Celsius ... they shall be Celsius' property, in every sense and for all purposes.")

Therefore, notwithstanding the frequent use of the word "loan" in the Terms of Use and the colloquial interpretation of a "loan" as a transaction in which the entity making the loan (here, the Account Holder) retains ownership over the asset being loaned (here, the cryptocurrency), the Terms Versions 5 and later are consistent and clear: Account Holders granted Celsius "all right and title to such Eligible Digital Assets, including ownership rights." (Terms § 13.)

### NOTES AND QUESTIONS

1. This is not a book about bankruptcy law, but it never hurts to know the basics. *Celsius Network* states the basic blackletter rule: as of the filing of a bankruptcy petition, all of the debtor's property becomes property of the bankruptcy estate, held on trust for the benefit of its creditors. "Secured" creditors, who have a "security interest" in particular identified property and have taken steps to "perfect" that security interest, have priority in that property and can generally recover it. All other creditors are "unsecured" and the remaining property is distributed to them *pro rata*—generally at a substantial discount to the face value of their claims—according to a complicated system of priorities based on the nature of the debts.
2. How is *Celsius Network* consistent with traditional banking principles? How is it different?
3. Would you recommend any legislative reforms to banking law or the Bankruptcy Code in light *Celsius Network* and cases like it? *See generally* Adam J. Levitin, *Not Your Keys, Not Your Coins: Unpriced Credit Risk in Cryptocurrency*, 101 TEX. L. REV. 877 (2023) (arguing that existing regulatory regimes are insufficient to protect consumer deposits at cryptocurrency exchanges).

## CELACARE TECHNOLOGIES, INC. V. CIRCLE INTERNET FINANCIAL, LLC

766 F.Supp.3d 237 (D. Mass. 2025)

*Stearns, District Judge:*

Plaintiff Celacare Technologies, Inc. (Celacare) filed this lawsuit against Circle Internet Financial, LLC (Circle) seeking enforcement of a negotiable instrument, 6 Del. C. § 3-309 (Count I), replacement of a lost or destroyed securities certificate, 6 Del. C. § 8-405 (Count II), and the return of "money had and received" under Delaware law (Count III). Circle moves to dismiss all counts pursuant to Federal Rule of Civil Procedure 12(b)(6). For the following reasons, the court will allow the motion.

#### BACKGROUND

Circle is a Delaware limited-liability company, headquartered in Boston, Massachusetts, that issues a digital asset called USD Coin (USDC) stored on the Ethereum blockchain. Compl. USDC is a "stablecoin" tied in value to the U.S. Dollar (USD) at a 1-1 exchange rate—for every USDC issued and placed in circulation, Circle promises to Users to hold either one USD or an equivalent amount of USD-denominated assets in User accounts segregated from Circle's corporate accounts. More than 34 billion USDC currently circulate worldwide.

Information regarding USDC is available on Circle's website, including its USDC Terms, which are attached as Exhibit A to the Complaint. The USDC Terms contain provisions governing the redemption of USDC for USD. Only Circle Mint tier customers may directly purchase and redeem USDC through Circle—all other Users must redeem their USDC through third-party facilitators. *See* USDC Terms § 2 ("You may not redeem USDC with Circle unless and until you open a Circle

Mint account."). Ultimately, Circle retains "sole discretion" over whether to redeem a User's USDC. *Id.* § 17.

The USDC Terms also provide that blockchain transactions "[are] irreversible and Circle does not have the ability to reverse or recall any transaction once initiated." *Id.* § 13. Pertinent to this case, the USDC Terms state that Users "accept all consequences of sending USDC." *Id.* The Terms warn Users that "[o]nce you send USDC to an address, you accept the risk that you may lose access to, and any claim on, that USDC indefinitely or permanently." *Id.* The Terms provide as an example that "an address may have been entered incorrectly and the true owner of the address may never be discovered." *Id.* Users are notified that they "bear all responsibility for any losses that might be incurred as a result of sending USDC to an incorrect or unintended USDC address." *Id.*

Additionally, the USDC Terms include provisions governing a User's third-party USDC transactions. USDC Users "understand and agree that Circle does not control any products or services sold or offered by third parties using the USDC Services," and that "Circle is not liable for any losses or issues that may arise from such third-party transactions." *Id.* § 14. Any losses or issues experienced by USDC Users who do not hold Circle Mint accounts must be handled "directly with the third-party seller." *Id.*

The relevant transactions in this case were conducted through a third party, Coinbase, Inc., the United States' largest cryptocurrency asset exchange. Coinbase and Circle are separate, unrelated entities. Coinbase, which is not named as a defendant in this Complaint, hosts a third-party platform on which customers can buy, hold, and trade cryptocurrency assets, such as USDC. To buy and sell cryptocurrency on the platform, customers must create an account and agree to the Coinbase User Agreement, which is attached to the Complaint as Exhibit C. If Coinbase Users deposit USD to a Coinbase account, they can elect to credit the account either with USD or with USDC. Compl. If Coinbase Users elect to credit USDC to their account, Coinbase possesses the USDC on their behalf and commits to dispose of that USDC according to the Users' orders. Like the USDC Terms, the Coinbase User Agreement warns that "Digital Asset Transfers cannot be reversed once they have been broadcast to the relevant Digital Asset network." Coinbase User Agreement §§ 4.1, 4.4.

In May of 2024, Celacare opened an institutional securities account at Coinbase. Compl. On July 3, 2024, Celacare gave Coinbase one million USD in exchange for one million Circle USDC. Celacare intended to transfer the USDC to an unnamed "contract counter-party" at an Ethereum wallet address. However, later that day, Celacare's President and CEO, Kenneth Yates, mistyped the recipient's address, transcribing a "B" as an "8," causing the one million USDC to be sent by Coinbase to the wrong Ethereum wallet address. The one million USDC remain in that wallet today.

Celacare alleges that because of the cryptography underlying the Ethereum blockchain, no one will ever be able to access these one million USDC again. On August 14, 2024, Celacare's counsel sent a message to the wallet address where the USDC was deposited, via a non-fungible token, requesting that any person with control of the wallet address prove that control by transferring an arbitrary (and small) amount of USDC to an arbitrary address. As of its filing of the Complaint, counsel had not received any response.

The following day, on August 15, 2024, Celacare sent Circle a draft Complaint and letter demanding a refund of one million USD for its lost USDC. After Circle

declined to place the wallet that held the mistakenly transferred USDC on an "access denial" list, which would have forbidden it from being used in future transactions, Celacare filed this suit on September 9, 2024, naming Circle as the sole defendant. ...

## DISCUSSION

### Count I

In its opposition brief, Celacare requests that its alternative claim to enforce its USDC purchase as a "negotiable instrument," 6 Del. C. § 3-309, be dismissed without prejudice. The court will accordingly dismiss Count I.

### Count II

Count II asserts a claim for replacement of a lost or destroyed securities certificate under 6 Del. C § 8-405. This statute requires the issuer of a "certificated security" to issue a new certificate to the owner of a certificated security that has been lost, destroyed, or wrongfully taken if that owner: (1) so requests before the issuer has notice that the certificate has been acquired by a protected purchaser; (2) files a sufficient indemnity bond; and (3) satisfies other reasonable requirements imposed by the issuer. "Certificated security" means "a security that is represented by a certificate." 6 Del. C. § 8-102(a)(4). "Security" is defined under Article 8 of the Delaware Uniform Commercial Code (UCC) as:

> an obligation of an issuer or a share, participation, or other interest in an issuer or in property or an enterprise of an issuer:
>
> (i) which is represented by a security certificate in bearer or registered form, or the transfer of which may be registered upon books maintained for that purpose by or on behalf of the issuer;
>
> (ii) which is one of a class or series or by its terms is divisible into a class or series of shares, participations, interests, or obligations; and
>
> (iii) which:
>
> (A) is, or is of a type, dealt in or traded on securities exchanges or securities markets; or
>
> (B) is a medium for investment and by its terms expressly provides that it is a security governed by this Article.

6 Del. C. § 8-102(a)(15).

Celacare alleges that USDC is a securities certificate because it is an "obligation" of Circle as an "issuer" represented to be in "bearer form." Celacare claims that USDC is an "obligation" because the USDC Terms, attached to the Complaint, give anyone who holds USDC the "right to redeem" USDC for USD funds.

The court interprets Circle's USDC Terms in accordance with familiar canons of contract interpretation. Thus, where the terms are unambiguous, they are given their plain, ordinary, and natural meaning. Here, Circle's USDC Terms unambiguously state that Circle does not promise to redeem USD to anyone who possesses USDC—only a "Holder" of USDC has "the right to redeem USDC for USD funds." USDC Terms § 2. A Holder "may not redeem USDC with Circle unless and until [it] open[s] a Circle Mint account." *Id.* § 2; *see also id.* ("For the avoidance of doubt, if a Holder is not eligible to register a Circle Mint account, or fails to do so, such Holder is not entitled to redeem USDC with Circle ... USDC does not itself generate any interest or return for holders of USDC and only represents your right to redeem USDC for an equivalent amount of USD through your account with

Circle."). Circle's USDC Terms also provide that its obligation to redeem USDC is conditioned on, among other things, the User's "possession of a corresponding amount of USDC associated with a registered Circle Mint account." *Id.* § 13.

Here, Celacare has not pled that it holds a Circle Mint account or that it possesses the minimum offset of one million USDC—rather, in its Complaint, it admits that the one million USDC presumably remain in an anonymous third-party's Ethereum wallet that Celacare cannot access. Nor does it allege that it conducted any transactions directly with Circle—rather, it dealt exclusively with Coinbase.[3] Celacare acknowledges in its Complaint that Circle and Coinbase are separate entities, with Circle retaining full control of its USDC business. For the reasons above, Circle is not obligated to redeem Celacare's missing USDC.

**COUNT III**

In the alternative to Counts I and II, Count III asserts a common-law claim for "money had and received." However, "money had and received" is "no longer a legally cognizable claim" under Delaware law and instead is "subsumed by modern law regarding breach of contract." *St. Search Partners, L.P. v. Ricon Int'l, L.L.C.*, 2005 WL 1953094, at *4 (Del. Super. Ct. Aug. 1, 2005). Celacare does not allege that it has a contractual right to recover from Circle and thus cannot avail itself of any contractual remedy.

Even if the court were to entertain an action for "money had and received," Celacare does not plausibly state such a claim. At common law, "money had and received" allowed recovery "wherever a man has in his hands money belonging to another which he cannot equitably retain and he either promises or the law can raise an implied promise to pay it." *Guthrie v. Hyatt,* 1 Del. 446, 447 (Del. Super. Ct. 1834). The claim, however, could not be brought "against third parties who did not receive money from the plaintiff." *St. Search Partners, L.P.,* 2005 WL 1953094, at *4. Here, the Complaint does not plausibly allege that Circle received any money or other things of value from Celacare.

---

3 Celacare also claims that pursuant to Coinbase's User Agreement, Coinbase and its Users expressly agree that all assets traded on its platforms are "securities" within the meaning of UCC Article 8, that these assets are held in a "securities account," and that Coinbase is a "securities intermediary" within the meaning of the UCC. *See* Coinbase User Agreement § 2.7.2. However, Celacare's claim that "on information and belief, Circle also agreed" to treat USDC as "securities" as defined by the UCC is conclusory, and bears no persuasive weight.

In its opposition brief, Celacare attempts to recast its "money had and received" claim in equity as one of unjust enrichment. However, Celacare is not permitted to amend its Complaint by way of a reply brief in opposition to a motion to dismiss.[6]

### NOTES AND QUESTIONS

1. What is a stablecoin? What are Circle and Coinbase's respective roles with respect to USDC?
2. Who could have prevented the problem that led to this case? Now that it has happened, who is capable of cleaning up its consequences?
3. Is this a hard case or an easy one?

## D. Regulation

### IN THE MATTER OF MUNCHEE INC.

Administrative Proceeding File No. 3-18304 (S.E.C. Dec. 11, 2017)

**I.**

The Securities and Exchange Commission deems it appropriate that cease- and-desist proceedings be, and hereby are, instituted pursuant to Section 8A of the Securities Act of 1933 against Munchee Inc. ("Munchee" or "Respondent").

**II.**

In anticipation of the institution of these proceedings, Respondent has submitted an Offer of Settlement (the "Offer") which the Commission has determined to accept. ...

**III.**

On the basis of this Order and Respondent's Offer, the Commission finds that: ...

**Summary**

Munchee is a California business that created an iPhone application ("app") for people to review restaurant meals. In October and November 2017, Munchee offered and then sold digital tokens ("MUN" or "MUN token") to be issued on a blockchain or a distributed ledger. Munchee conducted the offering of MUN tokens to raise about $15 million in capital so that it could improve its existing app and recruit users to eventually buy advertisements, write reviews, sell food and conduct other transactions using MUN. In connection with the offering, Munchee

---

6 Even if the court were to consider it, Celacare has not sufficiently pled a claim for unjust enrichment. Unjust enrichment is "the unjust retention of a benefit to the loss of another, or the retention of money or property against the fundamental principles of justice or equity and good conscience." *State ex rel. Jennings v. Monsanto Co.*, 299 A.3d 372, 390 (Del. 2023). To support a claim for unjust enrichment, a plaintiff must plead: (1) an enrichment; (2) an impoverishment; (3) a relationship between them; (4) the absence of justification; and (5) the absence of a remedy provided by law.

As previously discussed, Circle has not been enriched by Celacare's mistaken USDC transfer—the one million USDC that Celacare transferred on Coinbase's platform presumably remains at the erroneous wallet address that Celacare provided. Nor has Celacare plausibly alleged that Circle did anything to knowingly facilitate the alleged accidental transfer. ...

described the way in which MUN tokens would increase in value as a result of Munchee's efforts and stated that MUN tokens would be traded on secondary markets.

Based on the facts and circumstances set forth below, MUN tokens were securities pursuant to Section 2(a)(1) of the Securities Act. MUN tokens are "investment contracts" under *SEC v. W. J. Howey Co.*, 328 U.S. 293 (1946), and its progeny, including the cases discussed by the Commission in its Report of Investigation Pursuant To Section 21(a) Of The Securities Exchange Act of 1934: The DAO (Exchange Act Rel. No. 81207) (July 25, 2017) (the "DAO Report"). Among other characteristics of an "investment contract," a purchaser of MUN tokens would have had a reasonable expectation of obtaining a future profit based upon Munchee's efforts, including Munchee revising its app and creating the MUN "ecosystem" using the proceeds from the sale of MUN tokens. Munchee violated Sections 5(a) and 5(c) of the Securities Act by offering and selling these securities without having a registration statement filed or in effect with the Commission or qualifying for exemption from registration with the Commission. On the second day of sales of MUN tokens, the company was contacted by Commission staff. The company determined within hours to shut down its offering, did not deliver any tokens to purchasers, and returned to purchasers the proceeds that it had received.

**Facts**

1. Munchee is a California business that created an app (the "Munchee App") for use with iPhones. The company began developing the app in late 2015 and launched the app in the second quarter of 2017.
2. The Munchee App allows users to post photographs and reviews of meals that they eat in restaurants. The Munchee App is available only in the United States.
3. Munchee and its agents control the content on multiple web pages, including but not limited to its website (the "Munchee Website"), an additional site where it posted Munchee's "white paper" (the "MUN White Paper"), a Twitter account, a Facebook page, and posts on various message boards (collectively, the "Munchee Web Pages").

**Munchee Offers To Sell MUN To The General Public**

4. By Fall 2017, Munchee had developed a plan to improve the Munchee App during 2018 and 2019 that included raising capital through the creation of the MUN token and incorporating the token into the Munchee App. The MUN is a token issued on the Ethereum blockchain. Munchee created 500 million MUN tokens and stated that no additional tokens could be created.

5. On or about October 1, 2017, Munchee announced it would be launching an "initial coin offering" or "ICO"[1] to offer MUN tokens to the general public. Munchee posted the MUN White Paper that described MUN tokens, the offering process, how Munchee would use the offering proceeds to develop its business, the way in which MUN tokens would increase in value, and the ability for MUN token holders to trade MUN tokens on secondary markets. Munchee posted information about the offering and the MUN White Paper through posts on the Munchee Web Pages, including on a blog, Facebook, Twitter, BitcoinTalk, and the Munchee Website.
6. MUN tokens were to be available for purchase by individuals in the United States and worldwide through websites and social media pages including, but not limited to, the Munchee Web Pages.
7. Pursuant to the MUN White Paper, Munchee sought to raise about $15 million in Ether by selling 225 million MUN tokens out of the 500 million total MUN tokens created by the company. Purchasers of MUN tokens in the earlier stages of the offering were offered discounts of 15% and 10% on the offering price. Munchee said it would keep the remaining 275 million MUN tokens and use those MUN tokens to support its business, including by paying rewards in the Munchee App with MUN tokens, paying its employees and advisors with MUN tokens, and "facilitating advertising transactions in the future." In the MUN White Paper and elsewhere, Munchee said that it would spend 75% of the offering proceeds to hire people for its development team and to market and promote the Munchee App, use 15% "for maintenance and to ensure the smooth operation of the MUN token ecosystem" and use 10% for "legals to make sure Munchee is compliant in all countries." Munchee described a timeline that provided for various development milestones in 2018 and 2019, including the development of a smart contract on the Ethereum blockchain to integrate "in-app" use of the MUN token and setting up in-app wallets for end-users.
8. The MUN White Paper referenced the DAO Report and stated that Munchee had done a "Howey analysis" and that "as currently designed, the sale of MUN utility tokens does not pose a significant risk of implicating federal securities laws." The MUN White Paper, however, did not set forth any such analysis.

---

1. An "initial coin offering" or "ICO" is a recently developed form of fundraising event in which an entity offers participants a unique digital "coin" or "token" in exchange for consideration (most commonly Bitcoin, Ether, or fiat currency). The tokens are issued and distributed on a "blockchain" or cryptographically-secured ledger. Tokens often are also listed and traded on online platforms, typically called virtual currency exchanges, and they usually trade for other digital assets or fiat currencies. Often, tokens are listed and tradeable immediately after they are issued.

   Issuers often release a "white paper" describing the particular project they seek to fund and the terms of the ICO. Issuers often pay others to promote the offering, including through social media channels such as message boards, online videos, blogs, Twitter, and Facebook. There are websites and social media feeds dedicated to discussions about ICOs and the offer, sale and trading of coins and tokens.

**Munchee's Plan To Create An "Ecosystem" And Take Other Steps To Increase The Value Of MUN**

9. Munchee offered MUN tokens in order to raise capital to build a profitable enterprise. Munchee said that it would use the offering proceeds to run its business, including hiring people to develop its product, promoting the Munchee App, and ensuring "the smooth operation of the MUN token ecosystem."

10. While Munchee told potential purchasers that they would be able to use MUN tokens to buy goods or services in the future after Munchee created an "ecosystem," no one was able to buy any good or service with MUN throughout the relevant period.

11. On the Munchee Website, in the MUN White Paper and elsewhere, Munchee described the "ecosystem" that it would create, stating that it would pay users in MUN tokens for writing food reviews and would sell both advertising to restaurants and "in-app" purchases to app users in exchange for MUN tokens. Munchee also said it would work with restaurant owners so diners could buy food with MUN tokens and so that restaurant owners could reward app users – perhaps those who visited the restaurant or reviewed their meal – in MUN tokens. As a result, MUN tokens would increase in value. ...

13. Munchee intended for MUN tokens to trade on a secondary market. In the MUN White Paper, Munchee stated that it would work to ensure that MUN holders would be able to sell their MUN tokens on secondary markets, saying that "Munchee will ensure that MUN token is available on a number of exchanges in varying jurisdictions to ensure that this is an option for all token-holders." ...

**Munchee Promoted MUN Tokens And Purchasers Had A Reasonable Expectation Of Obtaining A Future Profit**

14. Purchasers reasonably would have viewed the MUN token offering as an opportunity to profit. ... Purchasers would reasonably believe they could profit by holding or trading MUN tokens, whether or not they ever used the Munchee App or otherwise participated in the MUN "ecosystem," based on Munchee's statements in its MUN White Paper and other materials. ...

15. For example, Munchee published a blog post on October 30, 2017 that was titled "7 Reasons You Need To Join The Munchee Token Generation Event." Reason 4 listed on the post was "As more users get on the platform, the more valuable your MUN tokens will become" and then went on to describe how MUN purchasers could "watch[] their value increase over time" and could count on the "burning" of MUN tokens to raise the value of remaining MUN tokens. ...

17. In addition, Munchee made public statements or endorsed other people's public statements that touted the opportunity to profit. For example, on or about October 25, 2017, Munchee created a public posting on Facebook, linked to a third-party YouTube video, and wrote "199% GAINS on MUN token at ICO price! Sign up for PRE-SALE NOW!" The linked video featured a person who said "Today we are going to talk about Munchee. Munchee is a crazy ICO. If you don't know what an ICO is, it is called an initial coin offering. Pretty much, if you get into it early enough, you'll prob-

ably most likely get a return on it." This person went on to use his "ICO investing sheet" to compare the MUN token offering to what he called the "Top 15 ICOs of all time" and "speculate[d]" that a $1,000 investment could create a $94,000 return.

18. Munchee and its agents targeted the marketing of the MUN tokens offering to people with an interest in tokens or other digital assets that have in recent years created profits for early investors in ICOs. This marketing did not use the Munchee App or otherwise specifically target current users of the Munchee App to promote how purchasing MUN tokens might let them qualify for higher tiers and bigger payments on future reviews. Nor did Munchee advertise the offering of MUN tokens in restaurant industry media to reach restaurant owners and promote how MUN tokens might let them advertise in the future. Instead, Munchee and its agents promoted the MUN token offering in forums aimed at people interested in investing in Bitcoin and other digital assets, including on BitcoinTalk.org, a message board where people discuss investing in digital assets. These forums are available and attract viewers worldwide, even though the Munchee App was only available in the United States. ...

**MUN Token Purchasers Reasonably Expected They Would Profit From The Efforts Of Munchee And Its Agents**

21. Purchasers would reasonably have had the expectation that Munchee and its agents would expend significant efforts to develop an application and "ecosystem" that would increase the value of their MUN tokens.

22. Munchee highlighted the credentials, abilities and management skills of its agents and employees. For example, in the MUN White Paper and elsewhere, Munchee highlighted that its founders had worked at prominent technology companies and highlighted their skills running businesses and creating software.

23. As discussed above, Munchee said in the MUN White Paper that the value of MUN tokens would depend on the company's ability to change the Munchee App and create a valuable "ecosystem" that would inspire users to create new reviews, inspire restaurants to obtain MUN tokens to reward diners and pay Munchee for advertising, and inspire users to obtain MUN tokens to buy meals and to attain higher status within the Munchee App. Munchee said that it and its agents would undertake that work during 2018 and 2019. ...

**Legal Analysis**

28. Under Section 2(a)(1) of the Securities Act, a security includes "an investment contract." *See* 15 U.S.C. § 77b. An investment contract is an investment of money in a common enterprise with a reasonable expectation of profits to be derived from the entrepreneurial or managerial efforts of others. *See SEC v. Edwards*, 540 U.S. 389, 393 (2004); *SEC v. W.J. Howey Co.*, 328 U.S. 293, 301 (1946); *see also United Housing Found., Inc. v. Forman*, 421 U.S. 837, 852-53 (1975) (The "touchstone" of an investment contract "is the presence of an investment in a common venture premised on a reasonable expectation of profits to be derived from the entrepreneurial or managerial efforts of others."). This definition embodies a "*flexible rather than a static principle*, one that is capable of adaptation to meet the countless and variable schemes devised by those who seek the use of the money of others on the

promise of profits." *Howey*, 328 U.S. at 299 (emphasis added). The test "permits the fulfillment of the statutory purpose of compelling full and fair disclosure relative to the issuance of 'the many types of instruments that in our commercial world fall within the ordinary concept of a security.'" *Id.* In analyzing whether something is a security, "form should be disregarded for substance," *Tcherepnin v. Knight*, 389 U.S. 332, 336 (1967), "and the emphasis should be on economic realities underlying a transaction, and not on the name appended thereto." *Forman*, 421 U.S. at 849.

29. As the Commission discussed in the DAO Report, tokens, coins or other digital assets issued on a blockchain may be securities under the federal securities laws, and, if they are securities, issuers and others who offer or sell them in the United States must register the offering and sale with the Commission or qualify for an exemption from registration.

***A. The MUN Tokens Were Securities***

30. As described above, the MUN tokens were securities as defined by Section 2(a)(1) of the Securities Act because they were investment contracts.

31. Munchee offered and sold MUN tokens in a general solicitation that included potential investors in the United States. Investors paid Ether or Bitcoin to purchase their MUN tokens. Such investment is the type of contribution of value that can create an investment contract.

32. MUN token purchasers had a reasonable expectation of profits from their investment in the Munchee enterprise. The proceeds of the MUN token offering were intended to be used by Munchee to build an "ecosystem" that would create demand for MUN tokens and make MUN tokens more valuable. Munchee was to revise the Munchee App so that people could buy and sell services using MUN tokens and was to recruit "partners" such as restaurants willing to sell meals for MUN tokens. The investors reasonably expected they would profit from any rise in the value of MUN tokens created by the revised Munchee App and by Munchee's ability to create an "ecosystem" – for example, the system described in the offering where restaurants would want to use MUN tokens to buy advertising from Munchee or to pay rewards to app users, and where app users would want to use MUN tokens to pay for restaurant meals and would want to write reviews to obtain MUN tokens. In addition, Munchee highlighted that it would ensure a secondary trading market for MUN tokens would be available shortly after the completion of the offering and prior to the creation of the ecosystem. Like many other instruments, the MUN token did not promise investors any dividend or other periodic payment. Rather, as indicated by Munchee and as would have reasonably been understood by investors, investors could expect to profit from the appreciation of value of MUN tokens resulting from Munchee's efforts.

33. Investors' profits were to be derived from the significant entrepreneurial and managerial efforts of others – specifically Munchee and its agents – who were to revise the Munchee App, create the "ecosystem" that would increase the value of MUN (through both an increased demand for MUN tokens by users and Munchee's specific efforts to cause appreciation in value, such as by burning MUN tokens), and support secondary markets. Investors had little choice but to rely on Munchee and its expertise. At the time of the offering and sale of MUN tokens, no other person could make changes to the

Munchee App or was working to create an "ecosystem" to create demand for MUN tokens.

34. Investors' expectations were primed by Munchee's marketing of the MUN token offering. To market the MUN token offering, Munchee and its agents created the Munchee Website and the MUN White Paper and then posted on message boards, social media and other outlets. They described how Munchee would revise the Munchee App and how the new "ecosystem" would create demand for MUN tokens. They likened MUN to prior ICOs and digital assets that had created profits for investors, and they specifically marketed to people interested in those assets – and those profits – rather than to people who, for example, might have wanted MUN tokens to buy advertising or increase their "tier" as a reviewer on the Munchee App. Because of the conduct and marketing materials of Munchee and its agents, investors would have had a reasonable belief that Munchee and its agents could be relied on to provide the significant entrepreneurial and managerial efforts required to make MUN tokens a success.

35. Even if MUN tokens had a practical use at the time of the offering, it would not preclude the token from being a security. Determining whether a transaction involves a security does not turn on labelling – such as characterizing an ICO as involving a "utility token" – but instead requires an assessment of "the economic realities underlying a transaction." *Forman*, 421 U.S. at 849. All of the relevant facts and circumstances are considered in making that determination. See *Forman*, 421 U.S. at 849 (purchases of "stock" solely for purpose of obtaining housing not purchase of "investment contract").

***B. Munchee Offered And Sold MUN Tokens In Violation Of The Securities Act***

36. As described above, Munchee offered and sold securities to the general public, including potential investors in the United States, and actually sold securities to about 40 investors. No registration statements were filed or in effect for the MUN token offers and sales and no exemptions from registration were available.

37. As a result of the conduct described above, Munchee violated Section 5(a) of the Securities Act, which states that unless a registration statement is in effect as to a security, it shall be unlawful for any person, directly or indirectly, to make use of any means or instruments of transportation or communication in interstate commerce or of the mails to sell such security through the use or medium of any prospectus or otherwise; or to carry or cause to be carried through the mails or in interstate commerce, by any means or instruments of transportation, any such security for the purpose of sale or for delivery after sale.

38. Also as a result of the conduct described above, Munchee violated Section 5(c) of the Securities Act, which states that it shall be unlawful for any person, directly or indirectly, to make use of any means or instruments of transportation or communication in interstate commerce or of the mails to offer to sell or offer to buy through the use or medium of any prospectus or otherwise any security, unless a registration statement has been filed as to such security.

**IV.**

In view of the foregoing, the Commission deems it appropriate to impose the sanctions agreed to in Respondent's Offer.

**Accordingly, it is hereby ORDERED that:**

A. Pursuant to Section 8A of the Securities Act, Respondent Munchee cease and desist from committing or causing any violations and any future violations of Sections 5(a) and (c) of the Securities Act.

## NOTES AND QUESTIONS

1. Was the MUN ICO a scam? Was it a good investment? Why did the SEC shut it down? Was there anything that Munchee could have done differently to make the ICO acceptable? If so, why didn't it?
2. Under the second Trump administration, the SEC and CFTC have taken the view that most blockchain assets are *not* securities. *See* Application of the Federal Securities Laws to Certain Types of Crypto Assets and Certain Transactions Involving Crypto Assets, 91 Fed. Reg. 13714 (Mar. 23, 2026). Most cryptocurrencies would be classified as non-security "digital commodities" subject to CFTC rather than SEC jurisdiction, and many NFTs would be classified as "digital collectibles." There are however, some exceptions. Under this new interpretation, a "tokenized" version of a traditional security—i.e., representing its holder or holders using tokens on a blockchain—is a "digital security" subject to the securities laws. In addition, any blockchain asset could be wrapped in an investment contract "when an issuer offers it by inducing an investment of money in a common enterprise with representations or promises to undertake essential managerial efforts from which a purchaser would reasonably expect to derive profits." *Id.* at 13721. Is MUN a security under this new guidance?

## UNITED STATES V. CHASTAIN

145 F.4th 282 (2d Cir. 2025)

*Menashi, Circuit Judge:*

Nathaniel Chastain appeals his judgment of conviction for wire fraud in violation of 18 U.S.C. § 1343 and for money laundering in violation of 18 U.S.C. § 1956. A jury found Chastain guilty of those offenses based on trades he made while employed at OpenSea, an online marketplace for non-fungible tokens ("NFTs"). As head of product, Chastain selected the NFTs that the company would feature in a section of its website. When an NFT was featured, its value increased. Chastain would purchase an NFT before it was featured and sell it afterward for a profit. He made about $57,000.

The district court instructed the jury that Chastain's decision about which NFT to feature was OpenSea's property even if that information lacked commercial value to OpenSea. It further explained that the jury could find that Chastain engaged in a scheme to defraud if he "conducted himself in a manner that departed from traditional notions of fundamental honesty and fair play in the general and business life of society."

Chastain argues that the instructions were erroneous because the jury could have convicted Chastain of fraud based on unethical business dealings even if he did not intrude on anything resembling a traditional property interest of OpenSea. We agree. ...

### Background

OpenSea is an online marketplace for buying and selling NFTs. An NFT is a unique digital artifact that can be bought and sold on the blockchain. OpenSea itself does not buy or sell any NFTs that are traded on its platform. Instead, the company collects a fee of two-and-a-half percent for each transaction on the platform. In 2021, OpenSea added a section to its website that would promote user interest by highlighting specific NFTs. When an NFT was featured, the publicity typically led its price to increase. OpenSea did not receive payments from the creators of NFTs featured on the website. Nor did OpenSea engage in any trades of featured NFTs. Instead, for each transaction involving a featured NFT, OpenSea received its standard fee of two-and-a-half percent.

### I

Chastain was the first head of product at OpenSea. In that role, he was responsible for evaluating current and new features, to figure out how well they were doingHe obtained feedback and conducted user interviews about the features, and he considered new changes that could improve the site. He would help organize engineers to work on these projects and designers. He also selected the NFTs that the website would feature.

Chastain purchased approximately fifteen NFTs that were then featured on the website. Chastain generally purchased and sold the featured NFTs using anonymous accounts. For each trade, he transferred cryptocurrency from his personal account into an anonymous account that he used to purchase the NFT. The anonymous account would sell the NFT after it was featured, and Chastain transferred the proceeds back into his personal account. He made about $57,000.

Chastain did not always use anonymous accounts. On August 2, 2021, an OpenSea user noticed that Chastain had used his personal account to purchase an NFT before it was featured. The user posted to Twitter that it "[l]ooks like Nate from OS had the jump on everyone else," adding an emoji of two eyeballs. Chastain responded to the post that he "just wanted to secure one of these [NFTs] before they all disappeared tbh.".At this point, no one at OpenSea told Chastain to stop purchasing featured NFTs.

On September 14, 2021, another OpenSea user posted about Chastain's trading, this time tagging OpenSea:

> Hey @opensea why does it appear @natechastain has a few secret wallets that appears to buy your front page drops before they are listed, then sells them shortly after the front-page-hype spike for profits, and then tumbles them back to his main wallet ...?

The next day, OpenSea asked Chastain to resign. After his resignation, Chastain maintained friendly social relationships with OpenSea's co-founders.

### II

On May 31, 2022, the government filed a two-count indictment. Count One charged Chastain with wire fraud in violation of 18 U.S.C. § 1343. Count Two charged Chastain with money laundering in violation of 18 U.S.C. § 1956. The wire fraud served as the predicate crime for the money laundering count. Chastain moved to dismiss the indictment. He argued that the indictment failed to allege that the featured NFT information was OpenSea's property because it lacked commercial value to OpenSea. The district court denied the motion.

**A**

At trial, the government introduced records and testimony showing that Chastain purchased NFTs ahead of featuring them. The government also offered testimony from OpenSea's co-founders, Alex Atallah and Devin Finzer, and other OpenSea employees. Atallah testified that the "goals" of the featured NFT section were to make OpenSea's website "more dynamic," "to explain what an NFT was to the new users," and to "engage indie artists and show that OpenSea is a place for them too." Atallah further testified that OpenSea did not trade featured NFTs because doing so "was not aligned with [its] main goals as a company" and "would have kind of compromised on OpenSea's brand of neutrality." Even though profits from the featured NFT section "wouldn't have been substantial for the business," OpenSea "wouldn't have wanted people to think that OpenSea was trying to make money on its own featuring of artists, because we wanted artists to all feel they had a chance and it was a meritocracy to be selected."

Atallah testified that the process for selecting which NFTs to feature was not secretive. OpenSea posted a link on its website inviting the public to "get featured on the home page" by using OpenSea's "NFT creator tool" and then sharing a link to their NFTs on Twitter or Instagram. By soliciting proposals from the public, OpenSea hoped to convey that the company was "open to ideas from everybody" and to "help people engage with OpenSea on social media." Proposals also came from an employee-only group chat, in which OpenSea employees suggested NFTs to feature. Chastain ultimately picked the featured NFT.

The government introduced evidence suggesting that Chastain viewed it as unethical to profit from the featured NFT section. In a discussion with a co-worker, Chastain said that "our community will take us to task if we feature something we own." Chastain confided in another coworker that he "kn[ew] full well that the increased exposure would increase their price" but "deluded [himself] into thinking that because [he] was introducing them to a larger audience, it was okay that [he] was capturing some upside." Chastain also told Atallah that it "could be a problem" if the company featured an NFT that an OpenSea employee had created.

Atallah and Finzer both testified that they believed the featured NFT information was covered by the confidentiality agreement that Chastain signed when he began working at OpenSea. The confidentiality agreement required Chastain "to hold in strictest confidence, and not to use, except for the benefit of the Company ... any Confidential Information that [the employee] obtain[s], access[es] or create[s] during the term of the [r]elationship ... until such Confidential Information becomes publicly and widely known and made generally available." "Confidential Information" included "information and physical material not generally known or available outside the Company and information and physical material entrusted to the Company in confidence by third parties."s The confidentiality agreement did not reference NFTs.

When asked whether OpenSea considered the selection of the featured NFT to be confidential, Atallah said that he "considered it to be confidential information," but Finzer testified that he "hadn't thought explicitly about whether it was confidential information" prior to the "incident" with Chastain. Finzer explained that he learned about Chastain's trading after OpenSea was tagged in the September 2021 post on Twitter. Finzer was "concerned that users would believe" that Chastain had traded featured NFTs "and that they would lose trust in Nate and/or OpenSea as a result." Finzer testified that it was a "hard decision" to ask Chastain to resign. The

day after the resignation, Finzer texted Chastain that asking him to resign was "[u]ndoubtedly the most difficult call [the company] had to make." ...

**DISCUSSION ...**

The district court erred by instructing the jury that it could find Chastain guilty of wire fraud even if it found that he misappropriated information that lacked commercial value to OpenSea. The district court further erred by instructing the jury that it could find Chastain guilty if it found his conduct to have departed from "fundamental honesty and fair play in the general and business life of society."

**I ...**

**A**

To be guilty of wire fraud, a defendant must (1) "devise" or "intend to devise" a scheme (2) to "obtain money or property" (3) "by means of false or fraudulent pretenses, representations, or promises." 18 U.S.C. § 1343. "The fraud statutes do not vest a general power in the Federal Government to enforce (its view of) integrity in broad swaths of state and local policymaking." *Ciminelli v. United States,* 598 U.S. 306, 312, (2023) (alteration omitted). The fraud statutes instead "protect property rights only." *Id.* ...

The Supreme Court has explained that the phrase "money or property" encompasses "property rights" that are both "tangible" and "intangible." *Carpenter v. United States,* 484 U.S. 19, 25 (1987). In either form, however, "the wire fraud statute reaches only traditional property interests." *Ciminelli,* 598 U.S. at 316. To qualify as a traditional property interest, even an intangible right must protect "an interest that had long been recognized as property when the wire fraud statute was enacted." *Id.* at 314.

Under these standards, not all information kept confidential qualifies as property. Neither the Supreme Court nor our court has held that confidential information that lacks commercial value will qualify as property under the wire fraud statute. In *Carpenter,* the Supreme Court explained that the Wall Street Journal's prepublication content was "information acquired or compiled by [the newspaper] in the course and conduct of its business." *Carpenter,* 484 U.S. at 26.. Although it was "intangible," the prepublication "news matter" was the Journal's "stock in trade, to be gathered at the cost of enterprise, organization, skill, labor, and money, and to be distributed and sold to those who will pay money for it, as for any other merchandise." *Id.* at 25-26. The Journal's interest in its prepublication news information was therefore comparable to the property rights of another business in its goods or trade secrets.

Our court followed this precedent in holding that a law firm had a property right in confidential information that its client provided to the firm. *See United States v. Grossman,* 843 F.2d 78 (2d Cir. 1988). In *Grossman,* we upheld the conviction of an associate under the wire fraud statute when the associate misappropriated the confidential information. We explained that even though the law firm "could not commercially exploit the information by trading on it," "several partners of the firm testified" that "by maintaining confidentiality, the firm would protect or enhance the firm's reputation, with the result that it would not lose its clients and perhaps would gain more clients." *Id.* at 86. Although in *Grossman* the relationship between the confidential information and its economic value was more attenuated than in *Carpenter,* the evidence that the firm would "lose its clients"

showed that the firm would suffer commercial harm if it failed to keep the information confidential.

Because the wire fraud statute reaches only traditional property interests, we must decide whether confidential business information qualifies as a traditional property interest even if it lacks commercial value to the business.We conclude that it does not. When the Supreme Court said in *Carpenter* that "confidential business information has long been recognized as property," the Court relied on the traditional legal protections for trade secrets. 484 U.S. at 26. *Carpenter* cited case law according to which the collection of "quotations of prices on sales of grain and provisions for future delivery" was "entitled to the protection of the law" because "it stands like a trade secret." *Bd. of Trade of City of Chicago v. Christie Grain & Stock Co.,* 198 U.S. 236, 245, 250 (1905). And *Carpenter* relied on the prior holding that "commercial data" about a company's pesticides was its "property" because the data were protected as trade secrets under state law, had "many of the characteristics of more tangible forms of property," were "assignable," could serve as "the res of a trust," and could "pass to a trustee in bankruptcy." *Ruckelshaus v. Monsanto Co.,* 467 U.S. 986, 1001-04 (1984). In each of the examples, the information had commercial value to the company.

Like confidential business information, trade secrets are intangible and kept confidential but receive legal protection. A trade secret has commercial value.[2] To be sure, we have said that "[i]nformation may qualify as confidential under *Carpenter* even if it does not constitute a trade secret." *United States v. Mahaffy,* 693 F.3d 113, 135 (2d Cir. 2012). But while *Carpenter* "does not require that *all* confidential information must be of the same nature to be considered 'property,'" to merit that designation it must be that "it has long been recognized as property." *Grossman,* 843 F.2d at 86. Information that lacks commercial value has not been so recognized. "The general rule has been that ideas or information are not subject to legal protection." *Pearson v. Dodd,* 410 F.2d 701, 707 (D.C. Cir. 1969) (Wright, J.). But when "information is gathered and arranged at some cost and sold as a commodity on the market, it is properly protected as property," and when "ideas are formulated with labor and inventive genius, as in the case of literary works or scientific researches, they are protected." *Id.* at 707-08. The characteristic feature of information and ideas protected as property is that "they constitute instruments of fair and effective commercial competition," so "those who develop them may gather their fruits under the protection of the law." *Id.* at 708. Information cannot

---

2 *See* RESTATEMENT (FIRST) OF TORTS § 757 cmt. b (1939) ("A trade secret may consist of any formula, pattern, device or compilation of information which is used in one's business, and which gives him an opportunity to obtain an advantage over competitors who do not know or use it."). The examples in the Restatement—"a machine or formula for the production of an article" and "a code for determining discounts, rebates or other concessions in a price list or catalogue, or a list of specialized customers"—describe information with commercial value to the company. *Id.*; *see also* RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 39 (1995) ("A trade secret is any information that can be used in the operation of a business or other enterprise and that is sufficiently valuable and secret to afford an actual or potential economic advantage over others.").

qualify as a traditional property interest if its holder has no economic interest in its exclusive use or in otherwise keeping the information confidential.[3]

The government argues that confidential business information, as the Supreme Court described it in *Carpenter,* is only "information a company creates or acquires for a business purpose (the 'business' part) that the company considers and treats as confidential (the 'confidential' part)." But that characterization omits the full description of information that receives legal protection as property. Confidential information that is "acquired or compiled by a corporation in the course and conduct of its business is a species of property to which the corporation has the exclusive right and benefit, and *which a court of equity will protect through the injunctive process or other appropriate remedy.*" *Carpenter,* 484 U.S. at 26, 108 S.Ct. 316 (emphasis added). A court of equity will protect information from disclosure when it has commercial value to the owner. In *International News Service,* for example, the Supreme Court approved the issuance of an injunction that restrained the use by others of the news information of the Associated Press "*until its commercial value as news to the complainant and all of its members has passed away.*" *Int'l News Serv.*, 248 U.S. at 245 (emphasis in original).

The government further suggests that the decision of the Supreme Court in *Kousisis v. United States*, 605 U.S. 114 (2025), demonstrates that information may qualify as a traditional property interest even if it has no commercial value to its holder. In *Kousisis,* however, the Supreme Court held only that *actual economic loss* is not an element of a wire fraud offense. The Court reiterated that "obtaining the victim's money or property must have been the 'aim' ... of the defendant's fraud." *Id.* at 122. Whether the holder of confidential business information must suffer an economic loss is a different question from whether that information must have commercial value to the company to qualify as property. As the Court explained, the Journal in *Carpenter* did not need to have suffered a monetary loss; "that the newspaper had been deprived of its right to exclusive use'of its proprietary information" was sufficient to establish the invasion of a property interest. *Id.* at 132. In *Kousisis,* the Court did not need to address the circumstances under which information might qualify as property because the defendants aimed to obtain "tens of millions of dollars," which obviously counts as a traditional property interest. *Id.* at 123. These cases do not undermine the conclusion that confidential information does not qualify as a traditional property interest unless it has commercial value to the company that holds it.

---

3 The Supreme Court has recently emphasized that the mail and wire fraud statutes do not protect "intangible interests" in the control of information "unconnected to traditional property rights." *Ciminelli,* 598 U.S. at 312. In *Ciminelli,* the Supreme Court rejected the argument that "the right to control the use of one's assets" qualified as property under the wire fraud statute. *Id.* at 311 The Court explained that "the right to information necessary to make informed economic decisions, while perhaps useful for protecting and making use of one's property, has not itself traditionally been recognized as a property interest." *Id.* at 315 n.4. The Court concluded that "potentially valuable economic information necessary to make discretionary economic decisions is not a traditional property interest." *Id.* at 309. The conclusion that the connection between the information and a commercial interest cannot be too attenuated provides additional support for the principle that confidential information that lacks any connection to economic decision-making does not qualify as a traditional property interest.

**B**

The district court instructed the jury that the government did not need to show that OpenSea had a commercial interest in the featured NFT information as long as the information was "acquired or created by [OpenSea] for a business purpose" and OpenSea "both considered and treated that information in a way that maintained the company's exclusive right to that information." That instruction allowed the jury to return a guilty verdict for wire fraud based on the misappropriation of the company's "exclusive right" to use information that had no economic implications for the company.

The jury instructions would allow a conviction under the wire fraud statute even if OpenSea thought it was merely unseemly to reveal the planned featured NFT before it appeared on the website— and even if the evidence showed that treating the featured NFT as confidential had no commercial value. The right to exclusive use of information, without evidence that maintaining the confidentiality of the information had economic value to the company, is an "intangible interest[] unconnected to traditional property rights" that cannot qualify as property under the wire fraud statute. *Ciminelli,* 598 U.S. at 312. ...

The district court instructed the jury that it could find Chastain to have committed wire fraud if (1) he "conducted himself in a manner that departed from traditional notions of fundamental honesty and fair play in the general and business life of society," App'x 411, and (2) used information his employer kept confidential even if "the government [did not] prove that the information had [economic] value" to the employer, id. at 413. Given these instructions, the jury could have returned a guilty verdict based on a determination that it was dishonest for Chastain to trade on the featured NFT information even if that information was tangential to OpenSea's business and its misuse could not have affected the company's economic interests.

If the wire fraud statute criminalized conduct that merely departed from traditional notions of fundamental honesty and fair play, "almost any deceptive act could be criminal." *Ciminelli*, 598 U.S. at 315. That approach would "vastly expand federal jurisdiction without statutory authorization" by "making a federal crime of an almost limitless variety of deceptive actions traditionally left to state contract and tort law." *Id.* The Supreme Court long ago clarified that a conviction for fraud requires more than "merely the breach of a fiduciary duty." *United States v. O'Hagan*, 521 U.S. 642 (1997). But the standards that informed the jury instruction here—such as the condemnation of "conduct which fails to match the reflection of moral uprightness, of fundamental honesty, fair play and right dealing in the general and business life of members of society," *Blachly v. United States*, 380 F.2d 665, 671 (5th Cir. 1967), and the prohibition of a scheme that "conflicts with accepted standards of moral uprightness, fundamental honesty, fair play and right dealing," *United States v. Mandel*, 591 F.2d 1347, 1361 (4th Cir. 1979)—reflect the development of "a federal, common-law fiduciary duty" that became known as "the pre-*McNally* honest-services doctrine," *Skilling v. United States*, 561 U.S. 358, 416-18 (2010) (Scalia, J., concurring in part and concurring in the judgment). That purported duty does not supply the standard for the offense of wire fraud under § 1343.[8]

---

8 In *McNally v. United States,* the Supreme Court held that the fraud statutes are "limited in scope to the protection of property rights." 483 U.S. 350, 360 (1987).

## NOTES AND QUESTIONS

1. The fact pattern here looks much like an insider trading case. Why didn't the government prosecute Chastain for insider trading?
2. Who was Chastain dishonest with? Whose confidential information did he misuse? Who did he harm financially?

## UNITED STATES V. EISENBERG

784 F.Supp. 3d 579 (S.D.N.Y. 2025)

*Arun Subramanian, United States District Judge:*

After a nine-day trial, a jury convicted cryptocurrency investor Avraham Eisenberg of commodities fraud, commodities manipulation, and wire fraud. Eisenberg moves for relief under Federal Rule of Criminal Procedure 29, arguing that the evidence at trial was insufficient to sustain these convictions. ...

### Background

On January 9, 2023, the government charged Eisenberg in a three-count indictment for defrauding an exchange called Mango Markets and stealing over $100 million worth of cryptocurrency. Mango Markets is a platform where investors can buy and sell both the platform's native crypto token, MNGO, and a derivative product called a "MNGO Perpetual." A MNGO Perpetual is essentially a futures contract—that is, an agreement to purchase or sell a particular asset on a later date at a predetermined price. A futures contract allows investors to take positions on future values of an asset; the investor who holds the short position (i.e. agrees to sell) bets that the value of the asset will go down, while the investor who holds the long position (i.e. agrees to buy) bets that it will go up. Futures contracts can be settled by "price settlement," in which one party pays the other for the difference in the price of the underlying asset on a predetermined date without exchanging the actual asset. To use the futures contract analogy, the "asset" underlying a MNGO Perpetual is the MNGO token.

Unlike a traditional futures contract, there is no predetermined settlement date for a MNGO Perpetual. Instead, the parties can realize profits during the pendency of the contract. For example, if the price of MNGO rises from the reference price (that is, the price of MNGO when the contract was formed), then the party holding the long position will have an unrealized gain. A mechanism in the MNGO Perpetual contract allows the winning party to force the losing party to pay them that unrealized gain. After that, the parties' contract continues on with a new reference price.

For these settlement payments, the contemporaneous price of MNGO is determined by reference to a pricing "oracle." An oracle "aggregates prices across a variety of other venues" to determine the fair market value of an asset. The MNGO Perpetuals oracle pulls data from three other cryptocurrency exchanges—FTX, AscendEX, and Serum—to determine the average spot price of MNGO, and thus the parties' unrealized loss or gain.

MNGO Perpetuals have one other distinct feature. So that the futures market stays tethered to the price of the MNGO token, the parties exchange a series of payments based on the so-called "funding rate." To understand the funding rate, it helps to understand how a perpetual contract is created. One party will enter a "bid," or an offer to buy into the perpetual, at an opening reference price; the other party will enter an "ask," or offer to sell. When the terms match, the exchange creates a contract between the buyer and seller. The average midpoint of these "bids"

and "asks" sometimes deviates from the oracle price for MNGO. If the order-book mid-price is lower than the oracle price, the party holding the short position must pay the party holding the long position to induce them to bid up the order-book price. And vice versa: if the order-book mid-price is higher than the oracle price, the long position must pay the short. Those payments are exchanged in USDC. USDC is a "reserve collateralized stablecoin" pegged to the US dollar..

During the time in question, Mango Markets not only allowed investors to trade crypto assets and perpetuals but also to take out collateralized loans of cryptocurrency based on the value of their portfolio on the platform. Both digital assets (like MNGO) and derivative contracts (like MNGO Perpetuals) counted as collateral. The higher the value of an investor's portfolio, the larger a loan they could take out.

For all this complicated background, the basic contours of Eisenberg's scheme are straightforward and undisputed on this motion. On October 11, 2022, Eisenberg deposited approximately five million USDC into two wallets on Mango Markets. He used one of the wallets to sell and the other to buy the same MNGO Perpetuals, such that he held both the long and short positions. He then bought MNGO on the three exchanges that fed into the oracle, which increased the oracle price of MNGO and, by extension, the value of his long position. Eisenberg then borrowed against his long position on the Mango Markets platform. A few minutes later, he sold MNGO on the same three cryptocurrency exchanges, which caused the oracle price of MNGO to plummet and, by extension, the value of his short position to rise. He then borrowed more from Mango Markets against his short position. In total, Eisenberg borrowed and then quickly withdrew over $100 million in cryptocurrency from Mango Markets. ...

**Discussion ...**

**II. Count 2: Commodities Manipulation**

**A. Rule 29: There Was Sufficient Evidence that Eisenberg Intended to Manipulate the Price of MNGO Perpetuals**

Next, Eisenberg challenges the sufficiency of the evidence on the commodities-manipulation charge. Under the CEA, it is a felony "for ... [a]ny person to manipulate or attempt to manipulate the price of any ... swap." 7 U.S.C. § 13(a)(2). To convict Eisenberg under this provision, Eisenberg argues that the jury had to find that he intended to manipulate the "market price" of MNGO Perpetuals, meaning the price at which MNGO Perpetuals are "traded." As a reminder, MNGO Perpetuals have two prices: the "reference price" and the "settlement price." First, the reference price: Recall that to enter a MNGO Perpetual contract, one person must enter a "bid," or an offer to buy, and the other person must enter an "ask," or an offer to sell. Each party must specify the price at which they are willing to bid into the order-book to create this perpetual. When the terms match, the exchange creates a contract between the buyer and seller. That's the reference price.

Next, the settlement price. No currency is exchanged when the parties create a MNGO Perpetual. Instead, the parties make payments only if the price of MNGO rises or falls from the reference price. If the price rises, the party holding the long position will have an unrealized gain and can force the losing party to pay that unrealized gain. Same thing if the oracle price falls. In that case, the short position has an unrealized gain and can force the party holding the long position to pay. This "settlement price"—meaning the difference between the reference price of the contract and the spot price of MNGO—is determined by looking to the oracle. At

any time, the winning party can force the losing party to pay them any unrealized gain based on this settlement price, after which the perpetual continues on with a new reference price.

Eisenberg says that the evidence at trial only established that Eisenberg intended to manipulate the settlement price of his perpetuals. But in his view, the government was required to prove that Eisenberg intended to manipulate the "market price," which Eisenberg defines as "the mid-price of the order-book averaging the best bid and ask"—in other words, the average reference price of the perpetuals. Eisenberg bases this argument on the Second Circuit's decision in *In re Amaranth Natural Gas Commodities Litigation*, 730 F.3d 170 (2d Cir. 2013). There, the court explained that although the CEA doesn't define the term "manipulation," "a court will find manipulation where (1) Defendants possessed an ability to influence market prices; (2) an artificial price existed; (3) Defendants caused the artificial prices; and (4) Defendants specifically intended to cause the artificial price." *Id*. at 173.

Eisenberg argues that *Amaranth*'s reference to "market price" refers to the price at which the asset is traded, not the settlement price of the contract. But *Amaranth* itself did not draw this distinction. The distinction between a "market price" versus some other price, or even the definition of what a "market price" is, was not presented in that case. And zooming out from the cases, the statute at issue here doesn't refer to "market price." It says "price."

Nevertheless, Eisenberg points to two cases in which courts dismissed cases brought under 7 U.S.C. § 25(a)(1)(D), which creates a private right of action for claims based upon "manipulation of the price of any ... contract or swap or the price of the commodity underlying such contract or swap." *See Vitanza v. Bd. of Trade of City of New York*, 2002 WL 424699, at *4–6 (S.D.N.Y. Mar. 18, 2002); *Three Crown Ltd. P'ship v. Caxton Corp.*, 817 F. Supp. 1033, 1042–43 (S.D.N.Y. 1993). In *Vitanza*, the court held that although plaintiffs "alleged that settlement prices of[futures contracts were manipulated, ... the settlement price is not the value of the contract itself or the value of the commodity underlying the contract." 2002 WL 424699, at *5. In *Three Crown*, the court held that allegations that the defendant manipulated treasury notes couldn't sustain a claim because "Treasury notes are not the commodity 'underlying' either Treasury bill futures or Eurodollar futures." 817 F. Supp. at 1043.

Eisenberg argues that these cases reflect that the manipulation of settlement prices doesn't count under 7 U.S.C. § 13(a)(2). The Court disagrees. And it's in good company: Both the CFTC and Second Circuit have rejected this argument. *See In re DiPlacido*, CFTC No. 01-23, 2008 WL 4831204, at *31 (Nov. 5, 2008) ("Settlement prices are market prices that can be manipulated."); *DiPlacido v. CFTC*, 364 F. App'x 657, 660 n.1 (2d Cir. 2009) (affirming in relevant part the CFTC's decision and distinguishing *Vitanza*, which was "cited by DiPlacido for the proposition that a 'settlement price' is not susceptible to manipulation as a matter of law"). As the Second Circuit explained in *DiPlacido*, *Vitanza* simply held that the plaintiffs couldn't sustain a claim based on the facts of that case. Specifically, the settlement prices in *Vitanza* were based on a mathematical formula, not trading, and they just impacted account margins, and did not reflect the "value of the contract." 2002 WL 424699, at *1, *5. And as the CFTC noted, *Vitanza* expressed no opinion on the scope of any statutory provision other than the private right of action under 7 U.S.C. § 25(a)(1)(D), which isn't at issue here. *In re DiPlacido*, 2008 WL 4831204, at *30. Same thing with *Three Crown*. It didn't address the

definition of "price" or the distinction between market and settlement prices. Instead, the court based its decision on the fact that the defendants manipulated something two steps removed from the futures contracts at issue—treasury notes when the futures contracts at issue were based on treasury bills. 817 F. Supp. at 1042–43. Here, the jury had a firm basis to find that Eisenberg manipulated the settlement price of MNGO Perpetuals itself. …

In this case, there was ample evidence to conclude that Eisenberg manipulated the "price of … any swap." 7 U.S.C. § 13(a)(2). The trial evidence made clear that by manipulating the value of MNGO on the three exchanges that made up the oracle, Eisenberg intentionally manipulated the price used to value MNGO Perpetual positions. That price, in turn, is what counterparties use to figure out who pays who and how much. Nothing in the text of the statute or the cases cited by Eisenberg suggests that the "price" in the heartland of what Congress wanted to protect is somehow out of bounds.

And even if the government was required to show that Eisenberg manipulated the "market price" of MNGO Perpetuals, a reasonable juror could have concluded that the "settlement price" was a "market price," in that it represented the value of the contract. As the government explains, "no one exchanges the original, reference price; its primary role is to serve as a baseline against which to measure the settlement price." The settlement price, in turn, "determines who pays whom, and how much." So "it makes no sense to think of the reference price as the 'trading' price" of MNGO Perpetuals. …

But even if "market price" in this context necessarily refers to the order-book mid-price of MNGO Perpetuals, the jury reasonably could have concluded that Eisenberg manipulated that price. As the government points out, "a scheme to intentionally manipulate the oracle price is also a scheme to intentionally manipulate the reference price because the latter will move in response to the former," given that "the funding rate keeps the reference price of new MNGO Perpetuals close to the oracle by requiring one side or the other to make payments if there is a gap between those two metrics." Indeed, the evidence at trial showed that Eisenberg's MNGO trading caused reference prices to rise by 700% in fourteen minutes. …

### IV. COUNTS 1 AND 3: THE FRAUD CHARGES

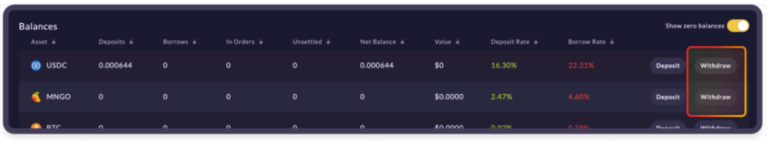
Next, Eisenberg challenges the sufficiency of the evidence on falsity and materiality for his commodities- and wire-fraud convictions.

#### A. Rule 29: There Was Insufficient Evidence of Falsity on the Wire-Fraud Charge

The essential elements of mail and wire fraud are (1) a scheme to defraud, (2) money or property as the object of the scheme, and (3) use of the mails or wires to further the scheme. The gravamen of the offense is the scheme to defraud. Establishing a scheme to defraud requires proof of a material misrepresentation. The misrepresentation can take the form of a false statement, a fraudulent omission, or a half-truth, which is a representation stating the truth so far as it goes but that is nonetheless misleading because of the failure to state additional or qualifying matter.

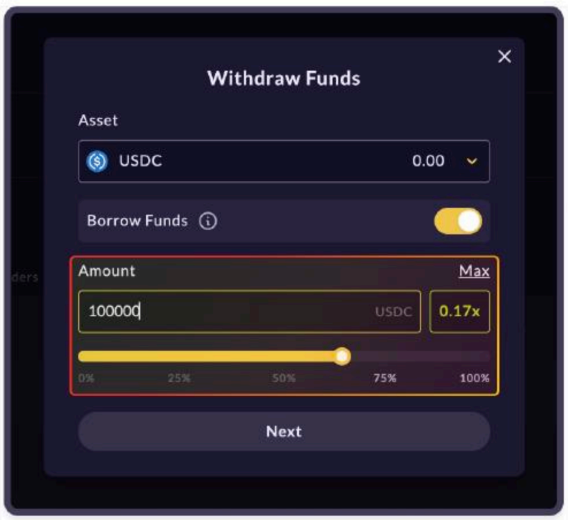
At trial, the government pointed to two alleged misrepresentations that Eisenberg made: First, he deceived Mango Markets into believing he was taking out a loan of cryptocurrency, when in fact he intended to steal it; and second, he misrepresented the value of his collateral, making Mango Markets believe it was valuable, when it was artificially inflated and worthless.

Before addressing whether there was sufficient evidence to support these alleged misrepresentations, here's a summary of what Eisenberg did. At the time in question, users on Mango Markets could take out a collateralized loan of cryptocurrency from the platform. See Tr. 309:7–310:9. *614 Instead of withdrawing cryptocurrency from their own accounts, users could "borrow" against their assets, using those assets as collateral. Tr. 311:1–6. It mechanically worked like this: A user who wanted to either withdraw their own assets, or borrow assets, would click "withdraw" or "borrow" on the following screens (clicking either would take the user to the same place):



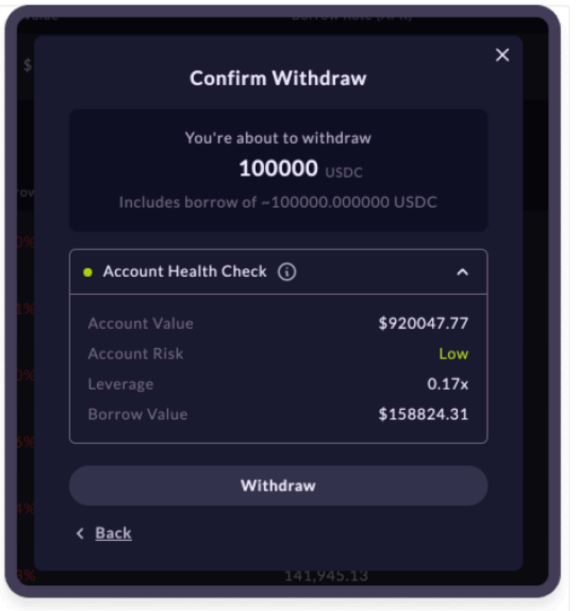

Under your account tab, scroll to balances.


GX-1011 at 78. The user would then get taken to the screen below:




This screen allowed users to withdraw their own cryptocurrency assets, or to borrow cryptocurrency from the platform. By toggling the "borrow" switch, a user could indicate that they wanted to borrow cryptocurrency—as opposed to withdrawing their own crypto—and say how much. The evidence at trial showed that when a user wanted to borrow funds, the program would automatically conduct a risk calculation based on the user's account value to "ensure that the user's withdrawal is sufficiently collateralized and covered based on the other assets in the account."

After clicking "Next," the user would be taken to this screen:




The screen indicates how much cryptocurrency is being withdrawn, how much of that is being "borrowed," and provides the user with information concerning their "account health." After clicking "Withdraw," the user gets the cryptocurrency.

At the time of Eisenberg's offense, Mango Markets had no terms and conditions, policies, or rules regarding either manipulation or the borrowing of funds. The stated consequence of not repaying a loan was liquidation. *See* GX-1011 at 148 ("Accounts must maintain a minimum 110% collateral ratio. If an account falls below the 110% threshold, a liquidator absorbs your position and becomes the new account owner."); *see also id.* at 61 ("Once a position is opened, it must maintain a Health Ratio above 0%. If an account falls to 0% it will be liquidated and funds will be lost."). So if a user borrowed funds, but then their account health dipped below 0% (meaning their account value has declined below the required collateral amount), the cryptocurrency would just be taken out of the user's account.

The government's theory of fraud was that Eisenberg, knowing his account value was artificially inflated, nevertheless toggled the "borrow" switch, which caused a "health check" to be performed to determine how much he could borrow. Because that health check was based on the inflated value of his Mango Perpetual positions, Eisenberg was able to withdraw more than he would have been allowed to absent his manipulation. Accordingly, the government says that Eisenberg "created the false impression that his MNGO Perpetual position was an extraordinarily valuable asset against which he could borrow huge sums of cryptocurrency."

Eisenberg argues that the government failed to prove that he made any material, false representation to Mango Markets. By and large, his arguments focus on the lack of any terms and conditions on the platform and the fact that Mango Markets was permissionless and automatic, so anything Eisenberg represented to the platform couldn't influence its decision to lend him cryptocurrency.

The Court agrees that there was insufficient evidence of falsity. First, the government argues that Eisenberg's act of borrowing funds when he intended to steal parallels signing a contract with no intent to honor one's obligations under that

contract, which the Second Circuit has held can be fraudulent. *U.S. ex rel. O'Donnell v. Countrywide Home Loans*, 822 F.3d 650, 658–60 (2d Cir. 2016). But the contract analogy doesn't get the government far. There was no evidence at trial that Mango Markets required any user to promise that they would repay funds as a condition of borrowing against their assets, so this isn't a case where "a contractual promise was made, but the promiser had no intent ever to perform the obligation." *Id.* at 660. To the contrary, as Eisenberg points out, the version of Mango Markets in use during Eisenberg's scheme "contained no specified terms of service, instructing users only that they were to 'use [the platform] at [their] own risk.'" Indeed, when a contributor to the platform, Brian Smith, was asked "When someone borrows from the platform, what is that user expected to do with respect to collateral," he answered that they are "generally expected to keep the collateral value positive a*nd, if not, they will be liquidated*." (emphasis added) What happens if a user borrows funds but the value of their collateral plummets? They get liquidated. There was no evidence that the "borrow" function on Mango Markets entailed an obligation to repay—or any other obligation for that matter—even if that's how the term is conventionally understood.

So while in other contexts a contractual agreement to "borrow" might give rise to a claim of fraud if an individual intentionally misrepresents or omits something relevant to the terms of the agreement or the parties' negotiations, here there were no terms and no negotiations. There was just the word "borrow." That word could have been "Access Collateral," "Utilize Assets," or anything else for that matter. Inferring a "contractual promise" from the conventional understanding about what "borrow" means—especially in the unconventional context of a cryptocurrency platform running on an algorithm—stretches *O'Donnell* too far.

The government's only case other than O'Donnell on the borrowing point is *United States v. Chanu*, 40 F.4th 528 (7th Cir. 2022). In that case, the Seventh Circuit upheld a wire-fraud conviction for defendants who placed "spoofing" orders on the CME that they did not intend to honor, a strategy intended to manipulate the price of futures contracts. The court held that the defendants had "advanced a quintessential 'half-truth' or implied misrepresentation" by publicly signaling an "intent to trade" by placing real orders while maintaining "a private intent to cancel in the hopes of financial gain." *Id.* at 541. In *Chanu*, however, "at all times relevant to the case, CME rules prohibited" traders "from placing orders that they intend to cancel before execution." *Id.* at 533. Here, by contrast, Mango Markets had no rules and no one testified that Mango Markets users understood borrowing to reflect an intent to repay. The *Chanu* district court opinion denying the defendants' Rule 29 motion further underscores the differences between that case and this one. The court held that the defendants "implicitly and falsely represented that they intended to execute the 'spoofing' orders" based on substantial evidence that the "CME's rules do not permit traders to cancel an order if their purpose for doing so is to manipulate or deceive other traders" and that "market participants understand orders in the exchange to reflect a bona fide intent to trade." *United States v. Vorley*, 2021 WL 1057903, at *3–6 (N.D. Ill. Mar. 18, 2021). That evidence is what is missing from this case.

Eisenberg also didn't make any false representations about the value of his assets on the platform. As noted above, when users on Mango Markets borrow against their collateral, the platform conducts an automated "account health check." The government argues that by prompting the borrowing process, and thus allowing Mango Markets to conduct this health check, Eisenberg created the false

impression that his collateral was valuable. But as Eisenberg points out, the platform automatically measured the actual value of his collateral, so he didn't represent anything untrue.

Of course, Eisenberg knew that the value of his portfolio was the product of his market manipulation, and he knew it wouldn't stay valuable for long. So although the value of Eisenberg's portfolio may have been technically accurate at the specific moment in time when he borrowed against it, the government argues that Eisenberg's representation about its value was deceptive. In support, the government points to testimony that the MNGO Perpetuals oracle was designed to pull data from exchanges like FTX and AscendEX because those exchanges had "some level of ... anti-manipulation protection there, such that" investors could expect the "activity and trading activity" that happened on those exchanges to reflect "organic demand." (The evidence at trial showed that while Mango Markets had no anti-manipulation rules or terms of service, FTX, AscendEX, and Switchboard, which ran the oracle, did.) The government also points to testimony from Mango Markets users that not maintaining collateral and manipulating asset values would have "mattered" to them.

Based on these expectations and beliefs, the government argues that when Eisenberg borrowed, he implicitly represented to Mango Markets that the collateral in his account had not been manipulated, and that it was in fact valuable, both of which were false. But that theory runs into the Second Circuit's decision in *United States v. Connolly*. There, Deutsche Bank (DB) submitted daily reports to the British Bankers' Association (BBA) about "the rate at which DB could borrow cash in the interbank market." 24 F.4th at 826. Defendants, who were traders at the bank, sometimes requested that the LIBOR submitters make submissions beneficial to their positions. *Id.* at 828–29. The evidence at trial included testimony from another DB employee and the LIBOR submitters themselves that "altering DB's LIBOR submissions to benefit DB trader positions was 'wrong' at the time they engaged in it." *Id.* at 830.

Among other things, the court rejected the government's argument that the submissions carried an " 'implied certification' that there had in fact been no trader influence on the submission." *Id.* at 842. Even though there was evidence that market participants understood that trader influence on LIBOR submissions was improper, the absence of any rule or instruction prohibiting that conduct was dispositive. The court observed that while the BBA later adopted rules prohibiting this kind of conduct (just like Mango Markets did after Eisenberg's scheme), "during the earlier period at issue in the present case, there were no such guidelines or prohibitions." *Id.* So while "defendants' efforts to take advantage of DB's position as a LIBOR panel contributor in order to affect the outcome of contracts to which DB had already agreed may have violated any reasonable notion of fairness," there was no actionable falsehood. *Id.* at 843; *see also id.* at 834 (noting "these federal fraud statutes are not catch-all laws designed to punish all acts of wrongdoing or dishonorable practices"). Similarly, there was no evidence at trial that Mango Markets had any rules, instructions, or guidance addressing manipulation or requiring users to maintain sufficient collateral in their accounts. *Cf. United States v. Skelly*, 442 F.3d 94, 97 (2d Cir. 2006) ("Under the wire-fraud statute, a seller or middleman may be liable for fraud if he lies to the purchaser or tells him misleading half-truths, but not if he simply fails to disclose information that he is under no obligation to reveal.").

While the government doesn't mention it, in *Connolly*, the BBA did expressly prohibit interbank collaboration on LIBOR rates, which the court held bolstered its holding that there was no implicit prohibition concerning intrabank trader influence. 24 F.4th at 842. There's of course no analog here, given that Mango Markets had no prohibition of any kind. But that's the point. On a platform with no rules, instructions, or prohibitions about borrowing, the government needed more to show that Eisenberg made an implicit misrepresentation by allowing the algorithm to measure the actual value of his collateral. ...

For these reasons, even when viewing the trial record in the light most favorable to the government, there was a failure of evidence on the element of falsity.

**B. Rule 29: There Was Sufficient Evidence of Materiality on the Commodities-Fraud Charge**

Unlike wire fraud, the commodities-fraud charge could be proven not only based on a material falsehood, but also on "a manipulative device." Indeed, the jury found Eisenberg guilty on this aspect of the charge, while it did not find him guilty on the separate material-falsehood prong.

Despite the government expressly raising this as a point of distinction between the commodities- and wire-fraud charges, Eisenberg does not argue that there was insufficient evidence for the jury to find that Eisenberg employed a "manipulative device." Accordingly, Eisenberg has waived any sufficiency challenge on his use of a manipulative device.

As for materiality, Eisenberg doesn't address this issue in the context of a "manipulative device." But because his manipulation of the settlement price of MNGO Perpetuals directly impacted Mango Markets' calculation of the amount Eisenberg was permitted to borrow from the platform, there was sufficient evidence of materiality even under Eisenberg's chief authority, *United States v. Rigas*, 490 F.3d 208 (2d Cir. 2007). In that case, the court considered whether the defendants committed bank fraud by misrepresenting their leverage ratios to banks to obtain loans at lower interest rates. *See id.* at 217–18. For the defendants' misrepresentations about their leverage ratios to be "material," the court explained that "they had to be capable of influencing a decision that the bank was able to make." *Id.* at 235. And "[t]he only 'decisions' that the bank could make, in the case the government presented to the jury, involved how much interest would be charged—an objective decision cabined by" a contractual formula set forth in the "Co-Borrowing Agreements." *Id.* The Co-Borrowing Agreements "tied the interest rate of a loan to a range of leverage ratios; changes in the leverage ratios within the range did not alter the interest rate." *Id. at 232.* Accordingly, where the Co-Borrowing Agreements "provided that a higher interest rate would be charged if the leverage ratio was above 5.0," and the evidence showed that defendants had submitted a leverage ratio of 4.98 instead of 5.01 to the bank, the court held that misrepresentation was material.

As the court explained in a footnote, the entire process was both contractually mandated and automated. *See id.* at 234 n.35 ("Referring to the bank's discretion to charge a different interest rate is not an entirely accurate description of what actually occurred under the Co-Borrowing Agreements. A leverage ratio above 5.0 on the CCH Co-Borrowing Agreement, for example, would automatically require the co-borrowers to pay a higher interest rate on the term loan component than one that was below 5.0."). In that context, the defendants' misrepresentation about their leverage ratio was material because, under the governing formula, the false input resulted in a different output. See id. at 235 ("The misrepresentation was

material only if the jury could have concluded that the fraudulent leverage ratio resulted in the co-borrowers being in a different interest category that they would have been had the accurate leverage ratio been reported.").

The evidence at trial permitted the jury to reach the same conclusion here: Eisenberg's manipulation increased the value of his collateral on Mango Markets, which in turn caused the platform's algorithm to permit him to borrow and withdraw far more cryptocurrency than he otherwise would have been allowed to. Eisenberg's argument for acquittal on the commodities-fraud charge fails.

### NOTES AND QUESTIONS

1. "Mango Markets had no rules." Is that this case in a nutshell? If so, why would anyone ever trade on Mango Markets? If not, what safeguards are there?
2. Who was Eisenberg dishonest with? Whose confidential information did he misuse? Who did he harm financially?

## VAN LOON V. DEPARTMENT OF THE TREASURY

122 F.4th 549 (5th Cir. 2024)

*Don R. Willett, Circuit Judge:*

The International Emergency Economic Powers Act, an integral part of the modern U.S. sanctions regime, authorizes the President to freeze the assets of, and prohibit transactions with, any foreign actor determined to be a threat to America's national security. This sweeping delegated power is carried out by the Treasury Department's Office of Foreign Assets Control (OFAC), which oversees various economic-based sanctions programs. In late 2022, OFAC sanctioned Tornado Cash, an open-source, crypto-transaction software protocol that facilitates anonymous transactions by obfuscating the origins and destinations of digital asset transfers. OFAC blacklisted Tornado Cash for its role in laundering virtual currency for malicious cyber actors—for example, a North Korea-linked hacking group that used Tornado Cash to launder the proceeds of cybercrimes. By adding Tornado Cash to the list of Specially Designated Nationals and Blocked Persons (SDN), OFAC imposed an across-the-board prohibition against any dealings with Tornado Cash "property," which OFAC defined to include open-source computer code known as "smart contracts." Tornado Cash's crypto-mixing smart contracts offer two prized attributes: privacy (by anonymizing digital transactions) and immutability (as the software code is unownable, uncontrollable, and unchangeable—even by its creators).

The six plaintiffs-appellants are users of Tornado Cash. They argue that Tornado Cash's inclusion on the SDN list exceeded OFAC's statutory authority. The district court disagreed, granting summary judgment to the Department and finding Tornado Cash subject to OFAC's sanctioning authority. Van Loon and the other plaintiffs appealed, making the same principal argument here—that Tornado Cash's open-source, self-executing software is not sanctionable under the Act (as opposed to the rogue persons and entities who abuse it). OFAC's concerns with illicit foreign actors laundering funds are undeniably legitimate. Perhaps Congress will update IEEPA, enacted during the Carter Administration, to target modern technologies like crypto-mixing software. Until then, we hold that Tornado Cash's immutable smart contracts (the lines of privacy-enabling software code) are not the "property" of a foreign national or entity, meaning (1) they cannot be blocked under IEEPA, and (2) OFAC overstepped its congressionally defined authority. ...

## I

Before getting to the legal analysis, we first offer a primer on cryptocurrency and blockchain.

Unlike traditional fiat currencies, such as the U.S. dollar, cryptocurrency is a decentralized and fully digital form of currency. Like fiat currencies, there are many kinds of cryptocurrency, and each is associated with a unique "coin" that serves as its record of value. These coins, like fiat currencies, can be traded, transferred, invested, and used to pay for goods and services.

Cryptocurrency's value is recorded on a "blockchain." Blockchains function like a bank's ledger in that they record all transfers of data—including, as relevant to this case, transactions. But unlike a bank ledger, blockchains are public, permanent, permissionless, and maintained through a decentralized network of independent computers or online users. In essence, each transaction is a stored on a "block" added to the "chain" of all prior transactions—and is publicly viewable forever.

Cryptocurrency users hold their coins in "wallets." Wallets have both public and private identifiers: addresses (which are public account identifiers) and keys (which function like passwords). Each time a user transacts with cryptocurrency, the transaction is posted to the blockchain and is visible to anyone. After a validation process, the blockchain displays the sender's address, the recipient's address, and the amount of cryptocurrency exchanged.

The addresses are, in theory, pseudonymous, and thus only the cryptocurrency user typically knows the transaction is his or hers. However, de-anonymization is not impossible. Onlookers can identify transaction participants if they can match a public address to an identifiable person. And once that happens, the blockchain reveals other transactions that belong to the same person and potentially reveals sensitive information about that person based on how they transfer their coins. As a result, some cryptocurrency users want additional options to keep their transactions private.

### A

One type of cryptocurrency coin is Ether (ETH), created and used in the Ethereum blockchain network. There are two kinds of Ethereum accounts: externally owned accounts and smart contracts.

An externally owned account is a wallet that can be controlled by anyone with the address and corresponding private key. So if a person wants to initiate a transaction from the wallet they control, they send a request to the Ethereum blockchain and pay a transaction fee—referred to as gas fees—in Ether. An individual known as a validator then verifies and executes the transaction by editing the blockchain to reflect the sending and receiving accounts' new balances. Only individuals who stake significant amounts of Ether as collateral may become validators, to ensure the blockchain's edits are legitimate.

The second type of account, a smart contract, is a software or computer program that is uploaded onto the blockchain network. These accounts do not require validators. Instead, the software is programmed to automatically perform tasks, such as executing transactions, transferring cryptocurrency assets, and creating new smart contracts, once prompted by a user. Once a smart contract is deployed on the blockchain, it is assigned a public address with which any user can interact. As an example, a "simple vendor smart contract" could create and assign ownership of some digital asset once a user sends Ether to a specified recipient's address.

Like all other transactions, a transaction using a smart contract incurs a gas fee, which varies depending on the smart contract's complexity.

Smart contracts come in two forms: "mutable" and "immutable." A mutable smart contract is one which is managed by some party or group and may be changed. An immutable smart contract, on the other hand, cannot be altered or removed from the blockchain. Importantly, a mutable contract may be altered to become immutable. But that is an irreversible step; once a smart contract becomes immutable, no one can reclaim control over it.

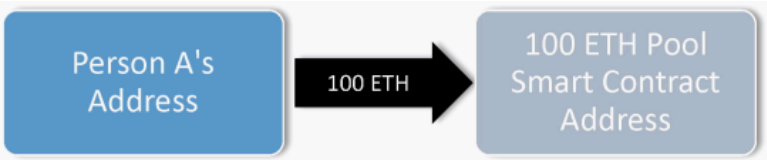
**B**

Enter Tornado Cash.

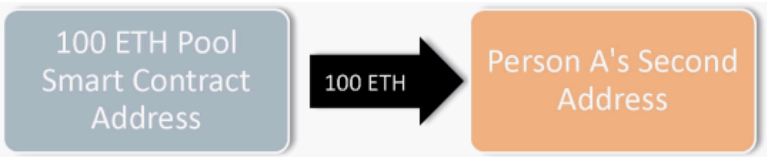
Tornado Cash is a decentralized, open-source software project developed by a group of contributors who uploaded a series of smart contracts to the Ethereum blockchain in 2019. Some of the developers included Roman Storm and two Russian nationals, Alexey Pertsev and Roman Semenov. Pertsev, who has provided material and technological support to the Federal Security Service of Russia, was arrested by Dutch authorities on money-laundering charges. And the U.S. indicted Storm and Semenov on similar money-laundering charges.

As of 2022, the Tornado Cash software included both mutable and immutable smart contracts, all of which are open-source and stored on the Ethereum blockchain. Relevant to this appeal are a set of Tornado Cash-developed smart contracts that provide increased anonymity by "collect[ing], pool[ing], and ... shuffl[ing] the cryptocurrencies deposited by many users." These smart contracts, like other software codes that perform similar tasks, are called "mixers."

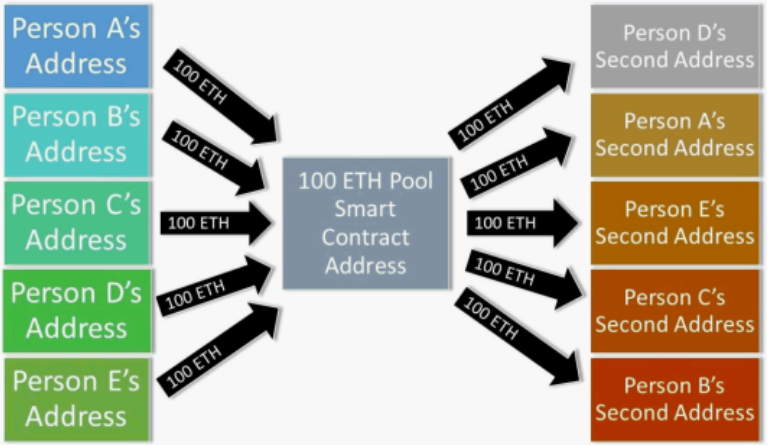
So how do these smart contracts work in practice? Users first deposit crypto into a specific "pool" smart contract based on the amount and type of crypto they want to mix. For example, someone who wants to deposit and withdraw 100 Ether would start by sending 100 ETH to the "100 ETH Pool Contract." That transaction would look something like this:




Depositors then receive keys or a password entitling the holder to withdraw the same amount from a given pool, and this withdrawal can be made to an entirely different wallet than the depositing wallet, thus "sever[ing]" "any public link between the deposit and withdrawal addresses." The software code that forms the pool smart contract will trigger a withdrawal from the pool only after it verifies the password. So when the person goes to withdraw the amount to a second address, the second transaction would look something like this:




These two transactions form the foundation of the Tornado Cash mixing process. And the entire process occurs automatically—with no human intervention.




But the Tornado Cash pool smart contracts depend on "a critical mass of users concurrently depositing and withdrawing transactions to obfuscate links between deposit and withdrawal addresses." The more users deposit coins in a pool, the more anonymous it is. So if only one person were using the 100 ETH pool smart contract to mix their transfer, the transaction would be easily traceable:

But if even five people were using the 100 ETH pool smart contract, it becomes more difficult to trace any transfer of 100 ETH to a particular address:

Now imagine this complexity amplified with thousands of users. The result: a highly obfuscated blockchain that is much harder to trace and consequently renders the transactors far more anonymized.

Although some of the Tornado Cash-developed smart contracts were immutable from the start, the developers initially retained the ability to update the pool smart contracts' codes—in other words, the pool smart contracts were originally mutable. But in 2020, the developers announced a "trusted setup ceremony" in which they would eliminate their control over the pool smart contracts. In that ceremony, more than 1,100 users participated, and at least twenty smart contracts—including the pool smart contracts—became irreversibly immutable. Consequently, the pool smart contracts became self-executing and could no longer be altered, removed, or controlled.

**C**

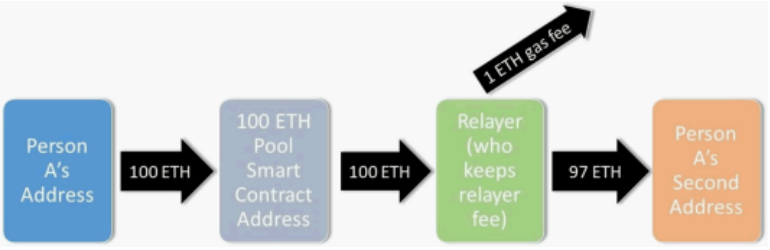
After the pool contracts became immutable, the original developers of Tornado Cash announced the creation of a decentralized autonomous organization (DAO) and a new crypto token called TORN, which can be transferred and sold on the blockchain like any other crypto asset. There are currently 1.5 million TORN tokens in circulation, and owning TORN allows, but does not require, individuals to vote on a limited subset of DAO governance issues. In fact, TORN holders must register their TORN tokens to be able to vote on any of those issues. To register their TORN tokens, individuals must lock their TORN into another mutable "governance" smart contract. Most TORN token holders have never taken these steps.

The DAO can only vote to implement new projects and change certain optional Tornado Cash features. It cannot vote on or make any changes to immutable smart contracts, such as the pool smart contracts.

D

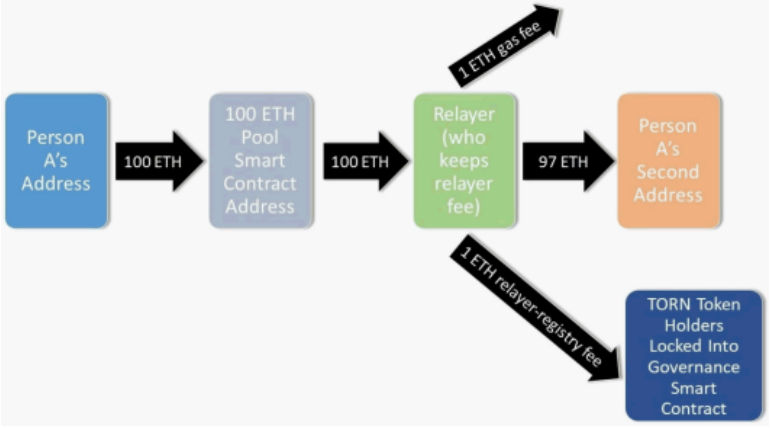
Even though the pool smart contracts help to anonymize transactions, those transactions aren't fully anonymized because they still incur gas fees. The withdrawing account must pay the gas fee to the Ethereum network to extract Ether from a pool. And "sending Ether to the withdrawal account prior to withdrawal might create a link between the user's deposit and withdrawal accounts"—the existence of which the Tornado Cash pool smart contracts are designed to obscure. For example, if the gas fee was 1 ETH, the transaction would still be traceable, as seen in the example below:

To combat this problem, Tornado Cash developers continued to develop additional anonymity tools, such as the use of relayers, which are mutable smart contracts operated by third parties. Relayers function like middlemen who pay the gas fees from their own accounts, deducting the cost of those fees—as well as their own relayer fees—from the amount withdrawn from the pool. Relayers never have custody over users' Ether, as the smart contract ensures that withdrawn Ether are only ever sent to the user's withdrawal account. The relayers then send the remaining amount to the account receiving the withdrawal. Thus, the relayers can eliminate any link between the deposit and withdrawal accounts. For example, if the gas fee was 1 ETH and the relayer fee was 2 ETH, the (simplified) complete transaction would look something like this:




The Tornado Cash developers created a mutable smart contract that maintains a registry of relayers, separate from the immutable pool smart contracts. Anyone can become a relayer for Tornado Cash by staking a specified amount of TORN, at which point they are added to the relayer registry.

For most (though not all) transactions processed by a third-party relayer, the mutable relayer-registry smart contract collects a fee from the relayer and pays it to the TORN token holders who have locked their TORN into the mutable governance smart contract. This fee is separate from the gas fee paid to the Ethereum network. For example, if the gas fee was 1 ETH, the relayer fee was 1 ETH, and the relayer-registry fee was 1 ETH, the complete transaction would look something like this:



The use of relayers—and the mutable relayer-registry smart contract—is entirely optional. Indeed, not all users of the immutable pool smart contracts use relayers.

**E**

The use of mixers like the Tornado Cash immutable smart contracts is, well, mixed. For example, law-abiding cryptocurrency users employ mixers to maintain anonymity concerning their net worth, spending habits, and donations to political causes. Mixers can also be used to thwart criminals that would use this information to identify potential victims or set up phishing schemes. For example, plaintiff Joseph Van Loon sought to use Tornado Cash to run a blockchain service without falling prey to malicious cyberattacks. Plaintiff Tyler Almeida used Tornado Cash to anonymously donate to the Ukrainian war effort because he was worried that Russian hacker groups would target him specifically if they were able to easily trace the donation back to him. Plaintiff Kevin Vitale turned to Tornado Cash after learning that someone had linked his crypto activities to his physical address. Plaintiff Alexander Fisher used Tornado Cash to develop code that improved the uses of the Ethereum blockchain network. And plaintiff Nate Welch used Tornado Cash to protect his privacy and to avoid harassment from malicious actors.

However, mixers are also "go-to tool[s] for cybercriminals" seeking to launder stolen cryptocurrency. Nearly a quarter of funds sent to mixers in 2022 were tied to money laundering efforts. Most relevant to this case, North Korea, through one of its cybercriminal organizations known as the Lazarus Group, has hacked and stolen just shy of one billion dollars' worth of cryptocurrency. And all of that dirty money needed to be laundered before it could be cashed out for traditional (and far more liquid) fiat currencies. So North Korean hackers turned to mixers. More than 65 percent of North Korea's dirty crypto went through mixers in 2021, "up from 42 percent in 2020 and 21 percent in 2019." And how does North Korea use this laundered money? To fund its weapons of mass destruction and ballistic missile programs.

**II**

We now turn to the relevant statutory authority and agency action.

The International Emergency Economic Powers Act allows the President to exercise extraordinary economic powers after "declar[ing] a national emergency with respect to" "any unusual and extraordinary threat, which has its source in whole or substantial part outside the United States, to the national security, foreign policy, or economy of the United States." 50 U.S.C. § 1701(a). This includes blocking "any property in which any foreign country or a national thereof has any interest." *Id.* § 1702(a)(1)(B) Similarly, the North Korea Sanctions and Policy Enhancement Act permits the President to "designate ... any person that [he] determines" is engaged in certain prohibited activities with respect to North Korea. 22 U.S.C. § 9214(a), (b). Once the President designates a person, they are listed as an SDN, and the President may "exercise all of the powers granted to [him] under the International Emergency Economic Powers Act" "to the extent necessary to block and prohibit all transactions in property and interests in property of [that] person." 22 U.S.C. § 9214(c)(1)

President Obama invoked these Acts in two executive orders relevant to this case. [One related to persons supporting North Korea's nuclear program, the other to persons supporting its cyber-espionage. The orders delegated authority to the

Department.] The Department, in turn, delegated authority to block persons under these orders to one of its internal agencies, the Office of Foreign Assets Control (OFAC).

OFAC issued regulations through these delegations, including definitional regulations for the words "person," "entity," "property," and "interest." It also provided avenues for those affected by blocking designations to present a challenge, and it sometimes grants licenses to engage in transactions involving blocked property.

**A**

On August 8, 2022, OFAC designated as entities the website tornado.cash, 37 Tornado Cash smart contracts (including at least twenty immutable smart contracts), and an address that was used to accept donations, citing North Korea's use of Tornado Cash to commit cybercrimes like the laundering of stolen crypto. Three months later, OFAC withdrew the August 8 designation and issued a new designation, which included 53 Ethereum addresses associated with the Tornado Cash software. The designations identified Tornado Cash as an entity organized by and under its DAO, and in doing so blocked "all real, personal, and other property and interests in property" of the designated Tornado Cash entity subject to U.S. jurisdiction. OFAC does not claim that Tornado Cash software is itself a product of North Korea or in any way owned or controlled by North Korea—but rather that some transactions using Tornado Cash software involved the North Korean Lazarus Group. The Lazarus Group had already been added to the SDN list. After it added Tornado Cash to the SDN list, OFAC issued notices reminding Tornado Cash users that they could request licenses to retrieve funds trapped within Tornado Cash pools and made clear that people could interact with its open-source code, just not with its transaction and pooling functions.

Six Tornado Cash users sued the Department under three theories. Their primary theory, and the only one advanced on appeal, asserts that OFAC violated the Administrative Procedure Act. [The other two theories were that OFAC's actions violated the First and Fifth Amendments.] They claim that OFAC lacked the authority to designate Tornado Cash as an SDN because (1) Tornado Cash is not a foreign "national" or "person," (2) the immutable pool smart contracts are not "property," and (3) Tornado Cash cannot have a property "interest" in the immutable smart contracts. The district court granted the Department's motion for summary judgment and denied that of the Tornado Cash users, concluding: (1) Tornado Cash is an "entity that may be properly designated as a person under IEEPA," (2) that smart contracts constitute "property," (3) and that the DAO, which runs Tornado Cash, has an "interest" in its smart contracts because it derives profits from its crypto mixing and relaying services that run on smart contracts.

The Tornado Cash users timely appealed.

**III ...**

Because the actions of the Treasury Department in designating Tornado Cash are governed by the judicial review provisions of the APA, we must affirm if OFAC's actions were not arbitrary and capricious, and were based on substantial evidence.

**IV**

The International Emergency Economic Powers Act and the North Korea Sanctions and Policy Enhancement Act vest the President with the authority to regulate (or block) "property," 50 U.S.C. § 1702(a)(1)(B); 22 U.S.C. § 9214(c)(1), (2), in which a foreign "national" or "person" (or "entity"), 22 U.S.C. § 9214(a)-(c); 50

U.S.C. § 1702(a), has an "interest," 50 U.S.C. § 1702(a)(1)(B); 22 U.S.C. § 9214(c)(1), (2). Van Loon argues that the district court erred in giving "heightened deference" to OFAC's definition of "property" and in finding that the immutable smart contracts met that definition. We agree. And because that element is dispositive, we need not address the other elements. ...

**B ...**

Under the International Emergency Economic Powers Act, the President is permitted to "block ... any property in which any foreign country or a national thereof has any interest." 50 U.S.C.A. § 1702(a)(1)(B). Although the statute does not define "property," property has a plain meaning: It is capable of being owned.

First, take dictionary definitions contemporaneous with the statute's passage in 1977. Property includes "everything which is or may be the subject of ownership, whether a legal ownership, or whether beneficial, or a private ownership." *Property*, BLACK'S LAW DICTIONARY 1095 (5th ed. 1979). Similarly, it is "the condition of being owned by or belonging to some person or persons," *Property*, OXFORD ENGLISH DICTIONARY (2d ed. 1989), and encompasses "the right to possess, use, and dispose of something," *Property*, WEBSTER'S NEW WORLD DICTIONARY OF THE AMERICAN LANGAUGE 1167 (college ed. 1968). It also includes the right "to exclude everyone else from interfering with it." *Property*, BLACK'S LAW DICTIONARY 1382 (4th ed. 1968). ...

The immutable smart contracts at issue in this appeal are not property because they are not capable of being owned. More than one thousand volunteers participated in a "trusted setup ceremony" to "irrevocably remove the option for anyone to update, remove, or otherwise control those lines of code." And as a result, no one can "exclude" anyone from using the Tornado Cash pool smart contracts. In fact, because these immutable smart contracts are unchangeable and unremovable, they remain available for anyone to use and "the targeted North Korean wrongdoers are not actually blocked from retrieving their assets," even under the sanctions regime. Simply put, regardless of OFAC's designation of Tornado Cash, the immutable smart contracts continue operating. And furthermore, because the software continues to operate regardless of the sanctions, and the blockchain technology "allows peer-to-peer transfers ... without requiring the recipient to consent to transfer," some users may become liable whenever someone transfers them digital assets via Tornado Cash, even without their knowledge or consent.

Sure, some smart contracts are capable of being owned in the sense that Tornado Cash developers can create new smart contracts and disconnect old mutable contracts. In theory, should Tornado Cash developers choose to comply with sanctions on mutable smart contracts, those developers could disconnect those mutable smart contracts to make them inaccessible and unusable by anyone on the Ethereum blockchain. But they cannot discard, change, disconnect, or control smart contracts that are immutable—like the ones currently listed on OFAC's SDN list and at issue in this appeal. Even with the sanctions in place, "those immutable smart contracts remain accessible to anyone with an internet connection."

**C**

Our inquiry could end here: The plain meaning of "property" in the Act does not support the Department's designation of Tornado Cash. But the Department points us to "OFAC's longstanding regulatory definition of 'any property,' " which includes "contracts of any nature" and "services of any nature," and suggests that OFAC's definition supports the smart contracts' status as "property" under the

Act. ... (1) [E]ven under OFAC's definitions, the immutable smart contracts still must be ownable; (2) they aren't contracts; and (3) they aren't services. And accordingly, the immutable smart contracts are outside the scope of OFAC's designation authority.

***1***

Assuming we were to consider OFAC's regulatory definition of "property," the immutable smart contracts cannot qualify because they are incapable of being owned. Indeed, OFAC's regulatory definition embraces the plain meaning of "property," as OFAC merely provides a laundry list of "illustrative examples, all of which are items typically understood as belonging to individuals or entities."[53] For example, according to OFAC, "[t]he terms property and property interest include money, checks, drafts, ... services of any nature whatsoever, contracts of any nature whatsoever, and any other property, real, personal, or mixed, tangible or intangible, or interest or interests therein, present, future, or contingent." Common sense agrees—everything from money, mortgages, and merchandise to debts, debentures, and deeds is ownable. Even "contracts of any nature whatsoever" and "services of any nature whatsoever" are intangible things in which individuals or organizations may own rights. **...**

To evade this requirement of "ownership," the Department conflates a separate element of the statute, "interest," with "property" to suggest that "Tornado Cash profits from—and therefore has an interest in—the smart contracts that embody the mixing service it provides" and are thus analogous to patents and copyrights, which are undisputedly within the scope of OFAC's definition of property. But Tornado Cash smart contracts are different from patents and copyrights in two important ways.

First, Tornado Cash doesn't profit from the immutable smart contracts at issue in this appeal. Some relayers and TORN token holders may receive fees from using the mutable relayer-registry smart contracts, but not from the immutable pool smart contracts. The Department has failed to provide us with evidence that any foreign nationals chose to stake their TORN and thus receive relayer fees. Nor does the record suggest that Tornado Cash itself, which is the designated "entity," receives fees from transactions through either mutable or immutable contracts. And none of the immutable smart contracts entitle the smart-contract creators to a benefit.

---

53 *See* 31 C.F.R. § 510.323 ("The terms property and property interest include money, checks, drafts, bullion, bank deposits, savings accounts, debts, indebtedness, obligations, notes, guarantees, debentures, stocks, bonds, coupons, any other financial instruments, bankers acceptances, mortgages, pledges, liens or other rights in the nature of security, warehouse receipts, bills of lading, trust receipts, bills of sale, any other evidences of title, ownership, or indebtedness, letters of credit and any documents relating to any rights or obligations thereunder, powers of attorney, goods, wares, merchandise, chattels, stocks on hand, ships, goods on ships, real estate mortgages, deeds of trust, vendors' sales agreements, land contracts, leaseholds, ground rents, real estate and any other interest therein, options, negotiable instruments, trade acceptances, royalties, book accounts, accounts payable, judgments, patents, trademarks or copyrights, insurance policies, safe deposit boxes and their contents, annuities, pooling agreements, services of any nature whatsoever, contracts of any nature whatsoever, and any other property, real, personal, or mixed, tangible or intangible, or interest or interests therein, present, future, or contingent.").

Second, patents and copyrights are ownable, just like everything else in OFAC's regulatory definition. Though they are intangible, someone owns the right to the protections and benefits offered by patents and copyrights. The same cannot be said for these smart contracts. …

*2*

OFAC's definition of property includes "contracts of any nature whatsoever," but contrary to the Department's argument (and the misleading name of the software), the immutable smart contracts are not contracts.

The Department contends—and the district court agreed—that the immutable smart contracts "are merely a code-enabled species of unilateral contracts," and "Tornado Cash promoted and advertised the contracts and its abilities and published the code with the intention of people using it—hallmarks of a unilateral offer to provide services." But in so finding, the district court ignored basic principles of black-letter contract law: Unilateral or not, contracts require an agreement between two or more parties. Immutable smart contracts have only one party in play.

Compare mutable and immutable smart contracts. Mutable smart contracts "could, at most, facilitate the creation of a contract between the smart contract's operator and a third party" through use of the smart contract, "but the smart contract is not itself a contract." For example, if a mixer was mutable—or in other words, controllable or custodial—the mixer's operator or owner could offer to mix deposits, which a third-party user could accept by transferring Ether to the operator's mixer-smart contract. The operator controlling the smart contract would use the mixer-smart contract to fulfill the contract by taking control of the third-party user's deposit, mixing the third-party user's deposit with others in the pool, then withdrawing the deposit to another account, as determined by the third-party user. In that case, someone is always handling the Ether.

On the other hand, when choosing to use or interact with an immutable smart contract, a third-party user could make an offer, but there is no smart-contract operator on the other side of the transaction to accept or make a counteroffer—just software code. Because no one can control immutable smart contracts (or the Ether deposited in the pools), there is no party with which to contract.

Furthermore, unilateral contracts can be revoked at any time until performance has been completed by the offeree. Even assuming the Tornado Cash developers made an offer by creating the smart contracts and publicizing the code to be used for mixing and pooling, they revoked their offer—and any role in it—by changing the code to be immutable, thus running independently and autonomously. And regardless of whether Tornado Cash advertises the immutable smart contracts on its website, that does not change the simple fact that Tornado Cash does not—and cannot—own or control them.

The district court analogized to a vending machine to find the immutable smart contracts are unilateral contracts. But even if the immutable smart contracts were, at some point, a "vending machine," they are no longer. For example, a vending machine has an owner—or counter-party—who can exercise some control over it. He can update or remove inventory or can unplug, move, or, if he so chose, destroy the vending machine. And the vending machine's owner can revoke the open offer to purchase snacks or drinks at a set price (by turning off the vending machine). But here, Tornado Cash has no control over these immutable smart contracts. It cannot change the code, delete the code, or remove the code from the Ethereum blockchain network. In other words, Tornado Cash cannot "unplug" the

immutable smart contracts. Even if Tornado Cash did not want North Korea, the Lazarus Group, or anyone else, for that matter, using the immutable smart contracts that the Tornado Cash developers created, Tornado Cash—let alone the Department—would be powerless to stop them. Though there is a potential argument that there were revocable offers prior to 2020—though we see none—the offers were revoked permanently when the smart contracts became immutable and the Tornado Cash developers removed any ability to control or own those smart contracts. ...

The Department points to some state laws that have been passed to ensure "[n]o contract relating to a transaction shall be denied legal effect, validity, or enforceability solely because that contract is executed through a smart contract."[71] But those laws seem to target automatic operation of a contract (how smart contracts operate) between two willing parties through software, rather than supposed "contracts" with a software. Indeed, those laws do not recognize the difference between mutable smart contracts—in which there is a party controlling the software, and thus, a party with which to contract—and immutable smart contracts—in which there is no party with which to contract.

Accordingly, the immutable smart contracts—regardless of their misleading name—are not "contracts" under OFAC's definition of "property."

*3*

The Department also contends that the immutable smart contracts qualify as "services of any nature whatsoever." But the immutable smart contracts "provide ... services"; they are not services themselves.

In the Department's view, a service is the performance of some useful act or series of acts for the benefit of another, us[ually] for a fee." But according to Black's Law Dictionary, "[i]n this sense, service denotes an intangible commodity in the form of human effort, such as labor, skill, or advice." *Service*, BLACK'S LAW DICTIONARY (12th ed.). No human effort is expended by the immutable smart contracts. And even by the Department's definition, the immutable smart contracts, which are nothing more than lines of code, are less like a "service" and more like a tool that is used in performing a service. That is not the same as being a service.

The software codes here—the twenty Tornado Cash addresses for immutable smart contracts—are tools used in providing a service of pooling and mixing the deposited Ether prior to withdrawal. Indeed, the immutable smart contract provides a "service" only when an individual cryptocurrency owner makes the relevant input and withdrawal from the smart contract; at that point, and only at that point, the immutable smart contract mixes deposits, provides the depositor a withdrawal key, and, when provided with that key, sends the specified amount to the designated withdrawal account. In short, the immutable smart contract begins working only when prompted to do so by a deposit or entry of a key for withdrawal.

More importantly, Tornado Cash, as defined by OFAC, does not own the services provided by the immutable smart contracts. A homeowner may own the right to trash-removal services and a client may own the right to legal services performed by a lawyer, but neither the homeowner nor the client owns the person performing the trash-removal services or the lawyer—for good reason. Similarly, Tornado Cash as an "entity" does not own the immutable smart contracts, separate

---

71 TENN. CODE. ANN. § 47-10-202(c).

and apart from any rights or benefits of the services performed by the immutable smart contracts. ...

### NOTES AND QUESTIONS

1. What consequences does designating Tornado Cash under the IEEPA actually have? What is the Department of the Treasury trying to do here?
2. Could Tornado Cash be property without having an owner?
3. After *Van Loon*, *Is* Tornado Cash unregulable, or does Congress have other options here?