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. ...