**DIFC SEMINAR**

**Issues in Crypto Currency Claims**

**13 November 2023**

**Mark Pelling KC**[1]

Good morning and thank you for asking you to talk about current trends and issues in the crypto field in England and Wales. As always everything I say in the next few minutes represent personal views and are not those of the Judiciary of England and Wales collectively.

Many of you will be only too familiar with the joys of Smart Contracts, block chain, distributed ledgers, wallets, crypto assets and currencies, Public keys and Private keys and exchanges. For those of you who are not as familiar as you would like to be, or wish to undertake a refresher course on these issues, I recommend three publications: The Legal Statement on Crypto assets and Smart Contracts published by the UK Jurisdiction Taskforce in November 2019; Law Commission Paper No 401 entitled "*Smart legal Contracts – Advice to Government*" published in November 2021 and most recently Law Commission Paper 412 entitled "*Digital Assets; Final* report", published earlier this year. They provide an invaluable insight into this world and should be read by all practicing law in this field, irrespective of the jurisdiction in which the reader practices.

What the Law Commission has to say about the common law world as it exists in England and Wales is that generally no legislative reform is necessary and that the common law is well able to facilitate and support these emerging technologies. Whilst maintaining that general position in its final report, and reporting its view that "*… the law in this area is now relatively certain…"* it nonetheless notes that there are remaining areas that are "*… highly nuanced and complex …"*. As you will I am sure all appreciate, this technology is rapidly evolving. Thus I remain sceptical about the conclusion that primary legislation will not be necessary in the future.

What then is the primary business of the English courts in the crypto world. Although the primary focus initially of those interested in this area was on smart contracts and block chain payment as a new means of doing business, particularly across borders, that has not been what has occupied the courts in England so far. Almost exclusively, the claims that have come before the courts have been fraud cases. As you might imagine, these frauds have almost exclusively been internet generated with increasingly sophisticated and convincing but entirely fraudulent schemes being promoted with the promises of very rapid and substantial gains for those who participate. Such schemes are attractive to those who peddled such schemes both because that investment environment meant there was a ready market of

[1] His Honour Judge Pelling KC, Judge in Charge, London Circuit Commercial Court, a constituent court of the Business and Property Courts of England and Wales, a group of specialist courts and lists within the High Court of England and Wales.

victims and because of the enormous gains that could be made by fraudsters stealing bitcoin purchased using victims' fiat currency, particularly in a strongly rising market.

The problems posed by these frauds are acute and for many victims can be life changing. Attempts to recover what has been lost pose very significant procedural and jurisdictional difficulties with the same common themes arising in most if not all cases. At this moment of acute anxiety, victims are faced with finding lawyers to attempt to recover what has been lost and to do so in a legal environment that is technically and legally difficult. In the next few minutes I am going to highlight a few of the major issues that have arisen and how the Courts in England have attempted to solve them. In considering them please bear in mind this context – in most of these cases the principal actors will be or are likely to be located outside England and Wales, as will the exchanges that administer the wallets into or through which the victims' assets have passed. In most cases therefore the victim of a cyber currency fraud domiciled and resident in England, or who has suffered losses in England will be faced with the need to seek information disclosure orders against those who administer the relevant wallets and a worldwide freezing and/or proprietary freezing order, usually against fraudsters who cannot be identified, who are almost certainly located in offshore jurisdictions and for whom the only known contact details are the email addresses used to carry the fraud into effect. The problems that arise are generally ones of identification and jurisdiction in relation to those who have engineered the fraud, those to whom assets belonging to the victims have been transferred and received either unconscionably or otherwise and those who can provide relevant information about the identity of those responsible for the fraud or the whereabouts of the victim's assets or their traceable equivalent.

Most of these frauds follow a similar pattern. Those instigating the fraud advertise the availability of an apparently very attractive investment opportunity via social media or an internet site. The victim makes contact with the fraudsters typically via email or phone or both. The victim is encouraged to buy a crypto currency using their fiat currency savings or borrowings and then give those apparently offering a legitimate investment service access to the relevant wallets to which the victim's crypto assets are credited by supplying the private key or giving access to the victim's PC. The ostensible purpose of this access is to allow the victim's crypto assets to be used by the ostensible advisor to invest or otherwise add value to the assets. There are a number of schemes that are said to enable this to be done. One involves active arbitrage trading between different crypto currencies. Another involves transferring crypto currency belonging to multiple different people in order to enable investment gains to be obtained that would not be available to those holding smaller parcels of the crypto asset concerned. Often these fraudulent schemes involve the generation of sham trading account statements suggesting substantial gains have been made. The existence of a fraud comes to light when the victim seeks to transfer some or all of the assets back to the victim's control when there will first be various excuses, then perhaps an invitation to make a further payment in order to secure release of the victim's assets and then no responses at all. However claims have included claims to recover ransoms paid in crypto currency to remove malware[2], to recover crypto currency invested in fictitious investment

[2] AA v. PU [2019] EWHC 3556

schemes[3], to recover bitcoin removed using fraudulently obtained login details[4], to recover NFT unlawfully removed from an unlawfully accessed wallet belonging to the claimant[5], to recover crypto assets alleged to have been stolen following illicit removal of private key information from a CEO's computer[6] and to recover crypto currency that the claimant had been fraudulently induced to transfer[7].

In purely domestic fraudulent claims, where a UK commercial bank has been the innocent intermediary for example in a authorised push fraud[8] obtaining information is relatively straight forward. The solicitors acting for the victim will typically first issue a Part 8 claim seeking against the financial institution or institutions concerned either a Norwich Pharmacal[9] or Bankers Trust[10] order. Now is not the time to describe the detail in relation to these applications, Broadly however each is a judicially created common law remedy where an order is obtained addressed to the third party innocent intermediary requiring the delivery up of information in the possession of the intermediary (typically KYC[11]and destination account information in the possession of the bank) that will enable the claimant either to identify those who have taken its assets without authority (primarily the purpose of the Norwich Pharmacal jurisdiction) or to locate its assets or their traceable equivalent (primarily the purpose of the Bankers Trust jurisdiction). Typically orders will be sought without notice to the bank, will take effect typically 14 days after service with the bank being able to apply to set aside the order prior to that date (in which case the order will be suspended until the bank's application is determined) and will contain ante tipping off provisions that apply until either a fixed time after the date when the information is provided or the order is set aside. UK banks and foreign registered banks with UK based operations have well established procedures for handling such orders once received and almost invariably now these are dealt with after service on the bank by negotiation with the claimant's solicitors. It is a relatively cheap and effective mechanism for tracing fraudsters and the proceeds of fraud.

In the crypto fraud context however the position is significantly more difficult and as with much else the problem starts at the border. This is not just a problem that faces the English courts but will face any state court that obtains its jurisdiction by service. Even where that is not so there is in any event a real practical problem posed by compliance or enforcement.

---

[3] Ion Science v. PU (Unreported)
[4] Fetch.ai v. PU [2021] EWHC 2254 (Comm)
[5] Osborne v. PU [2022] EWHC 1021 (Comm)
[6] Tulip Trading Ltd v. Van de Laan [2022] EWHC 667 (Ch)
[7] D'Aloia v. PU [2022] EWHC 1723 (Ch)
[8] Where a fraudster tricks a victim into making a payment to the fraudster by posing as a creditor, usually by gaining unauthorised access to an email account
[9] Norwich Pharmacal Co. v. Customs and Excise Commissioners [1974] A.C. 133. The criteria that must be satisfied if an order is to be obtained are those summarised in Mitsui & Co v Nexen Petroleum UK Limited [2005] EWHC 625 (Ch), 3 All ER 511 at paragraph 21 (Lightman J)
[10] Bankers Trust Co v. Shapiro [1980] 1 WLR 1275. This form of order is available to assist in locating assets in which a proprietary interest is claimed. The criteria that must be satisfied if an order is to be obtained are those summarised in Kyriakou v Christie's [2017] EWHC 487 (QB) at paragraphs 14 – 15 (Warby J as he then was).
[11] "Know your Customer"

A word now about how the English court gets jurisdiction. The jurisdiction of the English court depends upon being able to lawfully serve a defendant with originating process. Serving defendants in England and Wales poses no real difficulties for obvious reasons. Where a defendant is located outside England and Wales, the English court will get jurisdiction only if the claimant is able to get permission from the English court to serve proceedings on a defendant, wherever he she or it is located. This will generally be given only if the claimant is able to satisfy three tests:

(i) there is a serious issue to be tried as between the claimant and the relevant defendant;
(ii) there is a good arguable case that the claim passes through one or more of the jurisdictional gateways set out in PD6B paragraph 3.1; and
(iii) England and Wales is the most appropriate forum for the dispute to be determined[12].

Until recently, the common law had arrived at the unfortunate position that whilst permission could in principle be obtained to serve applications for Bankers Trust orders[13] such permission could not be obtained where what was sought was a Norwich Pharmacal order[14]. This unfortunate outcome was removed by amendment to CPR PD6B with the addition of a further gateway permitting the service of proceedings outside England and Wales where the claim is for information regarding the true identity of a defendant or potential defendant or what has become of the property of the claimant.

Unfortunately this has not made obtaining information orders materially easier or cheaper. Firstly, in order to succeed in relation to the first and third tests referred to earlier it will be necessary to deploy all the information that would be deployed in relation to the substantive claim so that in practice most claimants advisors have combined a claim for an information order against an exchange typically with a substantive claim, usually with an application for a world wide freezing order.

Secondly it assumes that if the court is persuaded to make an order, the foreign based institution to whom the order is addressed will comply. This gives rise to a number of practical difficulties. First, it is by no means guaranteed that the courts of a state other than England and Wales will enforce a Norwich Pharmacal or Bankers Trust order made by an English court; secondly there is no guarantee that an exchange with no connection to England and Wales will comply with such an order when served in it and thirdly, there is a real risk that if such an exchange is served with such an order it will tip off its customer either because it considers itself obliged to do so contractually and/or possibly because it considers itself bound to do so as a result of applicable local law. My experience as lead judge of the LCCC, where a large number of crypto fraud claims have been commenced is that initially such orders were met on one occasion with an outright refusal to recognise the jurisdiction of the English Court and

[12] – see Altimo Holdings and Investment Ltd v Kyrgyz Mobil Tel Ltd [2011] UKPC 7; [2012] 1 WLR 1804.
[13] [13] Ion Science Ltd and another v. Persons Unknown [2020] Unreported 21 December at paragraphs 19-21 (Butcher J); followed in Osborne v. PU [2022] EWHC 1021 (Comm).
[14] AB Bank Ltd v Abu Dhabi Commercial Bank PJSC [2016] EWHC 2082 (Comm) (Teare J) but see Lockton v Google Inc [2009] EWHC 3243 (QB) (Eady J).

most recently by silence and inaction from the exchange concerned. Mostly however exchanges will cooperate not because they have to but because they perceive it to be in their commercial best interests to be seen to cooperate with a state court attempting to assist a victim of fraud. Many now appoint very experienced City of London based solicitors to act on their behalf in relation to information orders granted by the Courts of England and Wales.

The next question that arises in pretty well all these cases is how to sue fraudsters whose identity is unknown and who are based outside England and probably in jurisdictions where it is likely to be impractical to serve proceedings or enforce English orders.

Again the English and common law courts in other jurisdictions have shown themselves willing to adopt pragmatic solutions. First in relation to making claims against unidentified fraudsters the courts in England have developed the practice of permitting proceedings to be commenced against persons unknown. Again this is not the place to set out the detail of the principles that apply. They are to be found in the cases set out in the footnotes to the paper I have written should you want to look at them[15]. In essence the key point is that the classes of unnamed defendant have to be defined with care so as to ensure that anyone served with or receiving notice of the issue of a claim can tell immediately if he she or it comes within any of the defined classes of defendants[16]. In a crypto fraud claim it is likely that crypto assets will have been moved multiple times ultimately to an exchange after removal from the claimant's wallet. This is usually for the purpose of enabling assets to be "cross chained" so as to render tracing more difficult or practically impossible or to facilitate the conversion of the defalcated Crypto currency into fiat currency and its transfer in a way that makes tracing impossible or practically so. It may be necessary therefore to bring proceedings against different classes of persons unknown in order to cater for these possibilities. Typically these will be (a) the individuals or companies who, without express authorisation or consent, obtained access to the victim's accounts; (b) the individuals who were knowing receivers of the claimant's crypto assets and (c) those to whom the assets are transferred and who were not aware of the claimant's interest in the assets[17]. The purpose of the third class is to enable those who have received the claimant's assets without knowing or believing the assets belonged to the claimant to be excluded from the scope of freezing orders, whilst recognising that claims against such defendants might be made for the recovery of such assets, though subject to defences such as bona fide purchase for value.

Typically, a claimant commencing proceedings in the manner described above will apply for a world wide freezing order directed to those unknown defendants falling (in the example given above) within classes (a) and (b). It may be thought that this is pointless given the likely location of those within that class. However there are potential advantages. Once such an order has been made it can then be served on third parties who will then come under an obligation not to

[15] Bloomsbury Publishing Group Limited v News Group Newspapers Ltd [2003] EWHC 1205 (Ch) [2003] 1 WLR 1633 and Hampshire Waste Service v Persons Unknown [2003] EWHC 1738 (Ch).

[16] See AA v Persons Unknown [2019] EWHC 3556 (Comm) and Fetch.AI Limited and another v. Persons Unknown (categories A, B and C) [2021] EWHC 2254 (Comm).

[17] For an example see Fetch.AI Limited and another v. Persons Unknown (categories A, B and C) (ibid.) at paragraphs 6-7

facilitate a breach by the defendants of that order. In a domestic fraud claim for example, such an order might be served on a bank not because the bank is a wrong doer but because it will then have knowledge of the order and freeze the relevant accounts since otherwise it would be held in contempt.

This approach can be most effective where it is being alleged that the assets credited to the account represent the traceable proceeds of the claimant's property and an order can be sought against the exchange itself. However, whether that will work in any particular case is fact sensitive. Piroozzadeh v. PU[18] was concerned with the fraudulent transfer of some Tether ultimately to wallets at the defendant exchange used by the exchange's own account holders. No allegations of fraud were made against the exchange. The claimant sought to trace what had been taken to the exchanges' wallets. The key point for present purposes is that the uncontested evidence was that the users of the wallets did not retain property in the Tether deposited, which was swept into a central unsegregated "Hot wallet" where the transferred assets were treated as part of the assets of the exchange concerned and operated as a central pool. The evidence was that there have been hundreds of transactions an hour passing through each of the hot wallets. The question was whether a proprietary injunction granted against the exchange concerned should be continued.

The fundamental point was that this particular exchange operated this part of its business much as UK commercial banks do. Once the Tether had been swept into the pool, the users were then granted credit in the value of the assets concerned, which it was submitted then constituted the exchange a purchaser for value and no longer susceptible to any remedy at the suit of the claimant so long as it acted *bona fide*. The evidence that the cryptocurrency had been pooled as I have described was what enabled the exchange to assert a bona fide purchaser defence. The judge acceded to the exchange's submission. Although greeted by some as a controversial decision, because it limited the ability of the victims of fraud to recover what was their property, it is as I see it a conventional application of English law tracing rules. It is as I have said fact dependent. In a number of claims passing through the LCCC since Piroozzadeh was decided , it has been alleged this case and its conclusions can be distinguished on the basis of a promise by the exchange concerned, contained in its terms and conditions, that it will hold each depositors' assets in effect as nominee. It remains to be seen how this point develops.

Where a proprietary claim is being advanced generally two questions will arise – firstly, is a crypto asset property at all and secondly if it is where is it treated as being located for the purposes of asserting a proprietary claim over it.

As to the first of these questions, it is now reasonably clear as a matter of English law, that crypto assets will be treated as property capable of being bought, sold and held on trust[19]. This approach was not disapproved in the only Court of Appeal case to concern these issues

[18] [2023] EWHC 1024 (Ch)

[19] See Wang v Derby [2021] EWHC 3054 (Comm); AA v Persons Unknown ibid. at paragraph 57; Ion Science Ltd v Persons unknown, ibid. at paragraph 11; and Fetch.AI Limited and another v. Persons Unknown (categories A, B and C) (ibid.) at paragraphs 14-15

– see Tulip v Van der Laan[20], where the Court of Appeal recorded that there was no dispute that the cryptocurrency in issue (Bitcoin) was property, as the first instance Judge (Falk J as she then was) had concluded. This approach has been adopted in both New Zealand and Singapore[21]. This approach has also been followed both by me[22] and then Lavender J in Osbourne v. Persons Unknown[23] in relation to a claim relating to two NFTs. A similar approach has been adopted at first instance in Singapore[24]. Whilst it is likely that this approach will continue to be adopted by common law courts, it is noteworthy that the Law Commission in its final report recommended statutory confirmation that a thing will not be prevented from being the object of personal property rights by reason of it being neither a thing in action nor a thing in possession. A statutory provision to this effect to future proof this issue.

The other issue that is of practical importance concerns the location of a crypto asset. This is important in particular in relation to extra territorial claims against alleged fraudsters because the jurisdictional gateways most relevant to a proprietary claim[25] focus either on events occurring within the jurisdiction or on property located within the jurisdiction and because the location of the property the subject of the claim is likely to be determinative in identifying the governing law[26], which in turn is highly material to the question of whether England and Wales is the most appropriate jurisdiction in which to commence the claim.

Initially, the approach that has generally been adopted by the courts has been to treat crypto assets as located in the place where the person who owns it is domiciled[27]. This has recently been further relaxed and is now to be tested by reference to residence. In Tulip v Van der Laan[28], the Court of Appeal held here was a good arguable case that (a) the claimant was resident in the jurisdiction notwithstanding that it was a Seychelles registered company because England was the location of its central management and control; and (b) the property (Bitcoin) was in consequence to be treated as located in England. This issue is important for jurisdictional purposes in England because the constructive trustee gateway concerns acts or events occurring within England and Wales or which is governed by the laws of England and Wales.

Finally in relation to proprietary claims, it has always to be considered whether the victim's property interest in his or her assets survives the fraud. Generally it is argued that English law imposes a constructive trust on a fraudulent recipient of property immediately on receipt[29]. Courts have generally held this principle to apply in respect of crypto assets obtained by fraud[30].

---

[20] [2023] EWCA Civ 83; [2023] 4 WLR 16

[21] see Ruscoe v Cryptopia [2020] NZHC 728 and Quoine Pte Ltd v B2C2 Ltd [2020] SGCA(I) 02

[22] [2022] EWHC 1021.(Comm)

[23] [2023] EWHC 39 (KB)

[24] Janesh s/o Rajkumar v. Unknown Person [2022] SGHC 264

[25] Practice Direction 6B, paragraphs 3.1(11) and (15)

[26] See Regulation (EC) No 864/2007 Of The European Parliament and of The Council of 11 July 2007 on the law applicable to non-contractual obligations ("Rome II"), Articles 3, 4,10 and 11.

[27] See Ion Science, ibid. at paragraph 13, followed in Fetch. AI Limited (ibid) at paragraph 14. In Tulip Trading (ibid.) the corporate entity was registered in the Seychelles but operated by an individual resident in England. The Judge held that the *lex situs* of the crypto asset concerned was to be tested by reference to residence.

[28] [2023] EWCA Civ 83; [2023] 4 WLR 16

[29] Westdeutsche Landesbank Girozentrale v London Borough of Islington [1996] AC 668 at 716C-D (Lord Browne-Wilkinson)

[30] See CMOC v Persons Unknown [2018] EWHC 2230 (Comm) at paragraphs 76-77, AA, ibid at paragraph 62, Ion Science, ibid. at paragraph 14; and Fetch. AI Limited (ibid) at paragraph 15.

So far example a victim's Bitcoin was credited to a particular wallet and was removed without the victim's consent this principle would apply. It becomes more difficult at least potentially where the victim transferred fiat or crypto currency to a fraudster under a contract that the victim had been induced to enter by fraud. In English law, title passes to the recipient until the contract is rescinded[31], at which point the recipient then holds the sums received on constructive trust for the transferor but without retrospective effect. This gives rise to a potentially difficult jurisdictional issues that the courts in England have not so far had to grapple with because those with an interest in arguing the point have not come forward to do so.

Finally, I should say a little about service. Generally English law requires service on defendants located out of jurisdiction in a way that complies with local law. Again this is not the place or time to go into the detail but there are exceptions and English procedural rules permit service by an alternative means where that is considered appropriate. Many countries round the world have acceded to the Hague Service convention. Where that is so, to permit service otherwise that required by the convention in relation to a particular country would conflict with convention rights. In order to cater for this, the case law in England requires that a court should permit service otherwise than as required by the convention only if there is an exceptional reason for so doing[32] and in non convention cases where there is a good reason for so doing. In relation to the categories of Person Unknown defendants I have referred to there is usually no practical way of serving proceedings other than by an alternative means. By definition a court will not know if the defendant is located in a Hague Convention state or not. In those circumstances English Courts have been willing to permit service by a variety of alternative means – usually by email to the email addresses that those who perpetrated the fraud used for that purpose[33] but also by service on the Exchange administering wallets used by the fraudsters and also by NFT to wallets associated with the defendants[34]. In relation to parties against whom freezing orders and information provision orders have been made, it has become routine to permit service by alternative means because of the immediate effect of such orders or the short time scale within which compliance is required.

The English courts will I think continue to develop common law principles in order to cope with the challenges posed by a largely unregulated economic sector. There will continue to be real difficulties about protecting those who need protecting unless the sector internationally applies itself to developing systems that are capable of operating across frontiers and which will enable relatively speedy and inexpensive enforcement. It is possible that will turn out to be some form of generally approved arbitral system available for use by third parties seeking information or other orders against exchanges embedded in an internationally recognised set of terms that all in the sector are willing to accede to. Merely national regulation I suspect will not provide an answer.

---

[31] See e.g. LIA v. Credit Suisse International [2021] EWHC 2684 (Comm) at [117]-[119].

[32] Olympic Council of Asia v Novans Jets LLP [2022] EWHC 2910 (Comm) at [16-18]

[33] AA v. PU (ibid.); Ion Science v. PU (ibid.); Fetch ai v. PU (ibid.) ; Osborne v. PU (ibid.)

[34] Osborne v. PU (ibid.); D'Aloia v. PU (ibid.)