Fountain Court

# Quarterly Commercial Crime Newsletter:

## RECENT UPDATES

APRIL 2023


AUTHORS

**Jacob Turner**
Call Date: 2016
Read more

**Aaron Taylor**
Call Date: 2017
Read more


This quarter's newsletter includes updates on:

- The effect of the UK sanctions regime on litigation
- The Economic Crime and Corporate Transparency Bill
- The state of crypto crime in 2023
- Developments in the service of civil fraud claims
- Fiduciaries duties of blockchain developers

### I. The effect of the UK sanctions regime on litigation

In January 2023, Cockerill J handed down a significant judgment on the interpretation of the UK sanctions regime: *PJSC National Bank Trust, PJSC Bank Otkritie Financial Corporation v Mints & Ors* [2023] EWHC 118 (Comm). The judgment addresses the issue of access to justice, and interprets the '*owned or controlled*' provisions of the relevant sanctions regime.

In the underlying claim, two banks seek US$850 million in damages from a prominent Russian businessman and his associates in relation to an alleged fraud perpetrated against the banks. The applications addressed by this judgment arose from the sanctions imposed by the UK Government on various individuals and entities connected with Russia.

The UK's sanctions regime is contained in the Sanctions and Anti-Money Laundering Act 2018 ("**SAMLA**") and regulations made under it, including for present purposes the Russia (Sanctions) (EU Exit) Regulations 2019. As Cockerill J noted at [3], the regime has two central features. The first is that all the assets of a designated person are frozen. This means that no person may deal in them. The second is that no person may make available any assets to a designated person. To do either of these things is a criminal offence.

Shortly after the invasion, the Secretary of State sanctioned the second claimant, Bank Otkritie, by adding it to the UK Government's list of 'designated persons'. A group of the defendants alleged that the first claimant, National Bank Trust ("**NBT**") was also subject to an asset freeze because it is *"owned or controlled"* by at least two designated persons: President Putin, and Ms Elvira Nabiullina (the governor of the Central Bank of Russia of which NBT is a 99% owned subsidiary).

There were two main issues in the case: first, the effect of a party being sanctioned on ongoing litigation in the English courts; secondly, whether the sanctions regime applied to the NBT as well as Bank Otkritie, which involved determining the ambit of the *"owned or controlled"* provisions of the statutory regime: [8]. Within the first issue, Cockerill J identified four sub-issues: The first sub-issue was whether the Court could properly enter judgment on the sanctioned Claimant's claim. The remaining three relate to the ability of a sanctioned claimant to: pay an adverse costs order; satisfy an order for security for costs; and pay damages awarded in respect of a cross-undertaking in damages: [9-10].

As to the question of whether entering a judgment in favour of a person is precluded by an asset freeze, the defendants argued that the causes of action advanced by the claimants constituted *"funds or economic resources"* which were covered by an asset freeze pursuant to reg. 11 of the Regulations, and s. 60 of SAMLA, and further that the act of entering a judgment by a Court constituted the prohibited acts of either *"dealing"* in or otherwise *"making available"* such funds and/or economic resources: [78]. For the first time in a case concerning the interpretation of the Regulations, the Court gave full consideration to issues of statutory interpretation, as well as considerations of fundamental rights under the common law and the European Convention of Human Rights. The claimants ultimately accepted that a cause of action could be an economic resource: [120]. However, Cockerill J went on to rule that, although the wording used by Parliament in SAMLA and the Regulations was in theory capable of precluding the entry of judgments in favour of a party, "*the requisite level of clarity in intent to derogate from the fundamental right of access to the court for determination of rights outside designation is not demonstrated*": [134].

The Court went on to rule that the payment of an adverse costs order as well as security for costs were precluded by an asset freeze, but that such activity was licensable by the Office for Financial Sanctions Implementation ("**OFSI**"): [179] and [183]. Cockerill J noted that this view aligned with OFSI's own interpretation in its guidance on the Regulations: [181]. The Judge held also that OFSI could license the payment of damages by the claimants on a cross-undertaking given pursuant to the grant of a freezing injunction: [195].

Given those findings, Cockerill J's discussion of the second main topic, (whether NBT was controlled by Bank Otkritie) was *obiter*. Nonetheless, it represents to date the most detailed consideration of a topic which has caused significant difficulty for the legal industry in the UK in the past 12 months. Under the Regulations, an asset freeze applies both to the assets of the designated persons and to the assets of an entity that is controlled by the designated person. Specifically, reg. 7(4) provides for a test of control, based on whether it is reasonable, having regard to all the circumstances "*to expect that [the designated person, i.e. President Putin] would (if [the designated person] chose to) be able, in most cases or in significant respects, by whatever means and whether directly or indirectly, to achieve the result that affairs of [third party, i.e. NBT] are conducted in accordance with [the designated person's] wishes*." Again, Cockerill J considered that on a plain language reading of the Regulations, the wording appears to be extremely broad, and thus NBT would be controlled by President Putin: [232].

However, she went on to conclude "*somewhat tentatively*" [233] that it was not the intention of the legislature for every entity which Mr Putin (or a similar Russian Government official) could control within the above definition to be deemed subject to sanctions. She drew a distinction between entities in relation to which Mr Putin acted in a personal interest (which would fall under the terms of reg.7) and those in which any control he had arose by reason of his status as Head of State (which would not). She was persuaded in this regard that the common law principle against doubtful penalisation was a powerful reason for adopting a restrictive interpretation of the test under reg. 7(4). Cockerill J considered that it "*seems implausible that it was intended that such major entities as banks (or other major entities such as Gazprom) were intended to be sanctioned by a sidewind, in circumstances where they would have no notice of the sanction and be unable themselves to challenge the designation under section 38 of the Act*." She noted also the significant difficulties which would arise in practice given that "*commercial people … need to know if a particular company (say, Gazprom or NBT) is sanctioned*": [242]. In a comment which will likely be welcomed by practitioners who have struggled with the broad wording of the control test in the legislation, Cockerill J noted that guidance from OFSI: "*indicates that it is not the intent for complex investigations to have to be made or evidence*

*gathered — because the list should generally set out the persons targeted*.": [244].

Cockerill J's conclusions on the 'access to justice' question is to be welcomed. The Judge rightly recognised that access to justice is a fundamental value and that accordingly any derogations from it are to be interpreted strictly, notwithstanding the vague and uncertain ambit of broad statutory wording. On the 'control' test, her tentative conclusions arguably require further analysis. Reg. 7 is a provision that would fall to be applied by a jury in a criminal case: it is difficult to accept that Parliament envisaged anything other than the plain language of the regulation operating in that arena. Nevertheless, practitioners will welcome the weight given by the Judge to the implausible and uncommercial consequences which would be brought about by adopting a plain language interpretation of the control test, particularly in light of the strict liability that arises in respect of civil penalties for breach of sanctions under the amended terms of section 146 of the Policing and Crime At 2017. It is notable that in *Mints* both sides were fully represented by experienced legal representatives. That was not the case in some of the earlier judgments on the topic – for example *VTB v JSC Antipinsky Refinery* [2022] EWHC 2795 (Comm), in which VTB was represented by only its CEO as a result of the sanctions regime having caused its previous lawyers to come off the record.

The remaining uncertainty voiced by the Court in *Mints* concerning the issue of control might suggest that future criminal convictions and civil penalties will be open to challenge, unless and until this issue is settled at the appellate level. It is helpful, therefore, that Cockerill J granted leave to appeal against her judgment. As highlighted in our previous Commercial Crime Update (see here), significant legal and practical challenges remain for the UK sanctions regime and its impact on the justice system.

## II. Economic Crime and Corporate Transparency Bill

The Economic Crime (Transparency and Enforcement) Act 2022 was fast-tracked through Parliament in March 2022 in response to Russia's invasion of Ukraine. The Economic Crime and Corporate Transparency Bill 2022-23 is a follow-up measure, intended to strengthen the UK's response to economic crime, in particular through reform to Companies House.

Part 4 of the Bill specifically concerns crypto assets. It makes various amendments to the Proceeds of Crime Act 2002, regarding both criminal and civil recovery. As to criminal recovery, the Bill amends Parts 2 (England), 3 (Scotland) and 4 (Northern Ireland) of the Proceeds of Crime Act 2002 ("**POCA**"), by *(i)* removing the requirement in certain circumstances that a person must have been arrested before crypto assets can be seized, *(ii)* making certain changes to the search, seizure and detention powers to clarify

how they apply to crypto asset wallets, and *(iii)* providing for the destruction of crypto assets in certain circumstances.

As to civil recovery, the Bill amends Part 5 of POCA (inserting new Chapters 3C-3F), by: *(i)* giving law enforcement search and seizure powers in relation to crypto assets, *(ii)* enabling law enforcement to recover crypto assets (where they are 'recoverable property') from third party holders, *(iii)* providing 'crypto wallet freezing orders' and *(iv)* enabling crypto assets to be released in cash, or destroyed, in certain circumstances.

These may prove very significant reforms in the fight against economic crime being committed through crypto assets. This part of the Bill is certainly to be welcomed for bringing POCA up to date with these technologies.

## III. The state of crypto crime in 2023

In February 2023, the blockchain consultancy Chainalysis released its annual highly respected Crypto Crime Report (free to download here). The report contains some stark findings:

1. The total value of cryptocurrency received by illicit addresses in 2022 was $20.6 billion – the highest figure to date, and up by some $2.5 billion from 2021. That figure is likely to be a very low estimate of the total criminal activity involving crypto assets: it only reflects on-chain activity (such as ransomware, or stolen cryptocurrency), and excludes both non-crypto-native crimes (such as drug trafficking using cryptocurrency as payment) and fraudulent off-chain activity by crypto companies (such as is alleged against FTX).

2. A study of three major crypto companies sanctioned by OFAC (for money laundering and terrorism financing) shows very different responses to the sanctions. In the case of Hydra, a darknet marketplace, the OFAC sanctions in April 2022 coincided with an affective shut-down by police in Germany (where its servers were located). In the case of Tornado Cash, a decentralised mixing service sanctions in August 2022, inflows dropped significantly after the sanctions were imposed (partly because the website that had proved easy access to the service was taken down) but did not disappear altogether. In the case of Guarantex, a Russia-based crypto exchange which caters predominantly to Russian users, sanctioned in April 2022, activity *increased* significantly following the imposition of sanctions – especially activity relating to the darknet and crypto scams.

3. Revenue from ransomware was $475 million in 2022, down from $765 million in both 2020 and 2021. The Report explains that this is not a result of any drop in the number of ransom

attacks, but rather an increase in the number of victims refusing to pay ransoms. In some cases, that appears to be out of a concern that the hackers are, or are related to, sanctioned entities (such as the Conti ransomware group, which was linked to Russia's FSB shortly after the invasion of Ukraine). In other cases, victims are seeking to recover their property with the assistance of Western law enforcement. A third, significant factor, is the increasing difficulty in obtaining cyber insurance that will cover ransomware attacks, and the resulting decrease in ransom payments by insurers.

4. $23.8 billion in illicit cryptocurrency was laundered in 2022 – up from $14.2 billion in 2021 and $8.5 billion in 2020. As the Report explains, *"mainstream centralized exchanges were the biggest recipient of illicit cryptocurrency, taking in just under half of all funds sent from illicit addresses. That's notable not just because those exchanges generally have compliance measures in place to report this activity and take action against the users in question, but also because those exchanges are fiat off-ramps, where the illicit cryptocurrency can be converted into cash."* The exception to this is for cryptocurrency stolen by hackers, a majority of which is sent to decentralised finance protocols (frequently because the stolen assets are not listed on any other exchange, so have to be traded for more liquid crypto assets such as ETH or USD-linked stablecoins).

5. The total value of stolen (hacked) cryptocurrency was $3.8 billion in 2022, up from $3.3 billion in 2021. Over the past two years, decentralised financial protocols have become the primary target of hackers, accounting for more than 80% ($3.1 billion) of stolen cryptocurrency in 2022. Of that sum, nearly two-thirds (c.$2 billion) was stolen from cross-bridge protocols – i.e. applications that enable users to exchange crypto assets held on one blockchain for assets held on another. And of that sum, more than half ($1.1 billion) was attributable to North Korea-linked hackers such as the Lazarus group. That represents a large part of the $1.65 billion in cryptocurrency thefts linked to North Korea in 2022, which is widely believed to be a significant source of funding for the country's nuclear weapons programme.

6. Revenue from crypto scams fell in 2022, down from $10.9 billion in 2021 to $5.9 billion in 2022. This is probably predominantly attributable to the decline in cryptocurrency values, since revenue from most scams closely tracks the price of major cryptocurrencies such as bitcoin. All of the top ten crypto scams (by revenue) were investment scams, but the largest category by average deposit size was romance scams.

## IV. Developments in the service of civil fraud claims

### The gateways for service out of the jurisdiction

The gateways for the service of civil proceedings out of the jurisdiction – contained in paragraph 3.1 of Practice Direction 6B of the Civil Procedure Rules – were substantially amended with effect from 1 October 2022. There are several points of significance for cyber- and crypto-fraud claims:

1. *Applications for information from non-parties*. The most significant change is the addition of a new gateway 25, which applies to *Norwich Pharmacal* Orders and *Bankers Trust* Orders. This permits service out of the jurisdiction where:

> (25) A claim or application is made for disclosure in order to obtain information —
>
> (a) regarding:
>
> (i) the true identity of a defendant or a potential defendant; and/or
>
> (ii) what has become of the property of a claimant or applicant; and 11
>
> (b) the claim or application is made for the purpose of proceedings already commenced or which, subject to the content of the information received, are intended to be commenced either by service in England and Wales or pursuant to CPR rule 6.32, 6.33 or 6.36.

In many fraud claims, especially crypto-fraud claims, the identity of the suspected fraudster, and the location of any misappropriated assets, is unknown. However, with the assistance of an expert in blockchain analysis, the claimant is often able to follow and trace the misappropriated funds, on the blockchain, into intermediaries such as crypto exchanges or trading platforms (although it is typically not possible to follow or trace funds after they have entered the exchange/platform, which maybe off-chain). The claimant may also have other useful information, including details of NFTs or other crypto-assets purchased with the proceeds of the appropriated funds, email address or social media accounts which appear to be linked to the fraudster, and/or bank accounts through which the proceeds of the misappropriated funds appear to have passed.

Where the claimant has information of those kinds, it is likely to seek information from the associated (typically, innocent) third party, which can help him or her to identify the fraudster, understand how the fraud occurred, and locate the traceable proceeds of his or her assets. In the case of banks or exchanges, this may include *(i)* details of transactions on the account, including the flow of the misappropriated sums in and out of the account, and *(ii)* KYC documents in respect of the account holder.

Such information orders – in broad terms, *Norwich Pharmacal* orders for the identification of the fraudster or other information required to bring the claim, and *Bankers Trust* orders for following and tracing assets – are routinely given in domestic fraud claims, especially against banks (and more recently, crypto exchanges) which frequently take a neutral stance in such applications. However, under the gateways as they stood before last October, it had been established at first instance that only *Bankers Trust*, and not *Norwich Pharmacal* orders, could be served on respondents outside the jurisdiction. That created a lacuna, which was especially acute in crypto-fraud cases (given that the relevant third parties are almost always foreign-domiciled), as noted in an influential July 2022 speech by HHJ Pelling KC, who heard several of the early crypto-fraud cases (see here).

The new gateway 25 removes that lacuna, enabling fraud claimants a direct route to service out without having to shoehorn their claim into an existing gateway (such as the "necessary and proper party" gateway), and without having to construct a proprietary claim (in order to claim Bankers Trust relief) where one does not naturally suit the facts of the case.

Perhaps unsurprisingly, the first reported case in which the new gateway was used was a high-profile crypto-fraud claim, *LMN v Bitflyer Holdings* [2022] EWHC 2954 (Comm) (Butcher J). The claim was brought by an English-domiciled cryptocurrency exchange, which had fallen victim to a hack. The exchange sought *Bankers Trust* orders against 26 recipient exchanges, to which (its expert evidence indicated) some proceeds of the hack had been transferred, seeking KYC information and transfer records. The order was granted, and service out permitted using the new gateway.

*Nik Yeo acted for the fifth defendant in the LMN case.*

2. *Unlawful interference*. There are three new sets of gateways, which apply in cases where the claim against the relevant foreign defendant is for unlawfully assisting in a civil wrong. The new gateways 15A and 15C, permit service out in respect of "a claim for unlawfully causing or assisting in" a breach of trust or fiduciary duty (respectively), where the underlying claim for breach of trust or fiduciary could be served out of the jurisdiction (under PD6B, paragraphs 3.1(12)-(12C), 3.1(12E), or 3.1(15), as regards breach of trust, and paragraphs 3.1(15A)-(15B) as regards a breach of fiduciary duty). There are parallel new gateways in respect of unlawfully causing or assisting in a breach of contract (gateway 8A) and unlawfully causing or assisting in a breach of confidence or misuse of private information (gateway 23).

3. *Contempt applications*. There is a new gateway 24, permitting service out of contempt applications, *"whether or*

*not, apart from this paragraph, a claim form or application notice containing such an application can be served out of the jurisdiction"*. This might apply, for example, to a contempt application against the director of a company, arising out of a claim against the company taking place before the English courts.

4. *Further reform?* The Minutes of the Civil Procedure Rule Committee dated 13 May 2022 record that the Committee discussed the potential adoption of anew gateway specifically for claims involving crypto assets. Ultimately, the Committee considered that any such reform should await the Law Commission's recently-announced project entitled "Digital Assets: which law, which court?". That project, an assessment of how private international law rules apply to emerging technologies, was launched in October 2022, is currently at the pre-consultation phase; a consultation paper is expected in the second half of 2023.

**Service of claims by non-fungible token**

In the latest sign of the High Court's willingness to adapt its procedures in order to assist the victims of cyber- and crypto-fraud, it has in recent cases permitted the service of such proceedings by non-fungible token (NFT) (being "alternative means" under CPR 6.15(1)). In such cases, the relevant court documents are typically uploaded to an online document depository (sometimes in redacted form), and a new NFT minted which contains a web link to the depository. That NFT is then 'airdropped' (i.e. transferred electronically) into the wallet understood to be controlled by the hacker.

Service of a *Bankers Trust* order by NFT (as well as email) was first permitted in *D'Aloia v Persons Unknown* [2022] EWHC 1723 (Ch), crypto-fraud case in which the claimant was allegedly fraudulently induced to send USD-linked stablecoins to a fraudster's wallet. Then, in *Jones v Persons Unknown* [2022] EWHC 2543 (Comm), the court permitted service of a summary judgment (in respect of a pool of stolen bitcoin held on constructive trust) on the defendants by NFT (and email/WhatsApp).

Most recently, the court has permitted service by NFT alone, in *Osbourne v Persons Unknown* [2023] EWHC 39 (KB); [2023] EWHC 340 (KB). *Osbourne* concerns the alleged theft (by hacking) of two *"Boss Beauties"* NFTs. The claimant was able to trace the NFTs to two wallets at the exchange OpenSea, and obtained injunctions over the NFTs, as well as information orders against OpenSea. The claimant was then able to identify email addresses and social medal accounts linked to the user of one of the enjoined wallets, and to identify the operator of those accounts, who was added as a named defendant to the proceedings. Following unauthorised movement of the

NFTs (which were put up for auction on a crypto asset marketplace) the claimant sought further injunctions, and permission to serve the injunction on three wallets (the original wallet into which the NFTs had been transferred, and the two wallets then holding each of the two NFTs), as well as the named defendant. In respect of the wallets, she sought permission to serve only by NFT. That order was granted by Lavender J *ex parte*, and continued by James Healy-Pratt (sitting as a Deputy High Court Judge) at the return date.

## V. Fiduciaries duties of blockchain developers

In a much-anticipated judgment (*Tulip Trading v Van der Laan* [2023] EWCA Civ 83), the Court of Appeal has held that it is arguable (to the standard of a 'serious issue to be tried') that the developers of bitcoin software owe fiduciary duties to owners of bitcoin.

The claimant is a company associated with Dr Craig Wright, who claims to be the inventor of bitcoin (i.e. the pseudonymous 'Satoshi Nakamoto' who wrote the seminal 2008 white paper 'Bitcoin: a Peer-to-Peer Electronic Cash System'). Dr Wright alleges that he owns bitcoin worth some $4 billion, held at two private addresses, the keys to which were stolen in a hack. He alleged that the developers who (he says) control and operate the relevant bitcoin networks, have the ability to secure his assets by implementing various software patches so as to enable them to transfer the assets to a safe address. Since Dr Wright required permission to serve his claim outside the jurisdiction, he was required to satisfy the court that there is a 'serious issue to be tried' (in addition to having a 'good arguable case' as to an applicable gateway, and satisfying the *forum conveniens* test). At first instance, Falk J held that there was no 'serious issue to be tried'; that decision was reversed by the Court of Appeal, and the claim allowed to continue.

The relevant factual background to the claim is set out in the judgment of Birss LJ at [26]-[30] and [40]. In short, the case concerns four bitcoin networks, which are variants of the original bitcoin network. Each network is supported by 'client software', the underlying code for which is publicly available (i.e. 'open-source') on a database called GitHub. Participants in a network run that publicly-accessible code, which embodies the rules applicable to the network. Anyone can propose a change to this software: however a change can only be implemented by someone with the relevant electronic password for the particular code database on GitHub. Dr Wright argues that the developers (the defendants) are in control of that software on the grounds that they hold the relevant passwords and decide what amendments (if any) are to be made to the software. As a consequence, he alleges, the defendants exercise control over bitcoin owned by the users of the network, and consequently owe fiduciary duties to the true owners of that bitcoin.

That characterisation of the defendants' position was disputed (although it was assumed to be correct for the purposes of the service out application), because it appears to undermine the concept of decentralisation, which is at the heart of the bitcoin white paper (but which had been challenged in influential academic writing cited by the Court of Appeal). At paragraph 34 of her judgment Falk J explained:

*The defendants challenge this, portraying (particularly in the case of the BTC developers) a decentralised model in which, to the extent that they are or continue to be involved in software development for the Networks (which is disputed for some of them), they are part of a very large, and shifting, group of contributors without an organisation or structure. Further, any change that they were able to propose to address [Tulip's] complaint would be ineffective, because miners would refuse to run it and instead would continue to run earlier versions of the software. What [Tulip] sought went against the core values of bitcoin as a concept. A disagreement could lead to a 'fork' in the Networks, resulting in the creation of additional networks rather than a resolution of the issue. The fifteenth and sixteenth defendants also claim that if they attempted to make the changes sought to the BCH ABC Network it would have a severely detrimental effect on their reputations, and participants would refuse to adopt them.*

At both levels, the courts adopted Millett LJ's well-known definition of fiduciaries from *Bristol and West Building Society v Mothew* [1998] Ch 1, at the core of which is a duty of single-minded loyalty. Falk J had held that the defendants, being a fluctuating and unidentified pool of people, could not owe such a duty, and could not be obliged to remain as developers or make any future updates of the kind envisaged by the claim. She accepted in principle that the developers might be obliged not to introduce features or bugs into the software which applied solely for their own personal benefit, but doubted whether that obligation was fiduciary in nature. She noted in particular that the software patch which Tulip sought to require would be for its sole benefit, and therefore perhaps to the detriment of other users (at [78]-[79]): *"It is uncontroversial that a fundamental feature of the Networks, at least in their existing form, is that digital assets are transferred through the use of private keys. [Tulip] effectively seeks to bypass that. … [S]ome users may not agree that a system change that allowed digital assets to be accessed and controlled without the relevant private keys, contrary to their understanding of how the system is intended to operate, accords with their interests, even if made only following an order of the English court declaring that [Tulip] owns those assets."*

The Court of Appeal disagreed. It is worth setting out the key passages from Birss LJ's judgment in full:

*72. The unusual factual feature of the present case is that literally all there is, is software. A physical coin has properties which exist outside the minds*

*of people who use it and in that sense is tangible. Bitcoin is similar. It also has properties which exist outside the minds of individuals, but those properties only exist inside computers as a consequence of the bitcoin software. There is nothing else. And crucially, asserts Tulip, it is the developers who control this software. On Tulip's case that control is very significant. […]*

*73. A further aspect of Tulip's case is to examine the manner in which the developers exercise their control over the software. Focussing on a software bug, if a third party identifies such a problem and the developers agree it should be fixed, then the developers will no doubt act to introduce a change in the source code in the relevant GitHub account, and computers on the network will update the software they are running (absent a fork, which again can only be a matter for trial). In other words the fulfilment of their role as developers involves taking active steps to update the code. It is not limited to such active steps, because the developers can also decline to update the code, but the role has a clear positive element.*

*74. This analysis also demonstrates that the role involves the exercise of authority by the developers, given to them by their control of access to the source code, and it is a decision-making role, in effect making decisions on behalf of all the participants in the relevant bitcoin network, including miners and also including the owners of the bitcoin. These features, of authority and of discretionary decision making, are common to fiduciary duties. […]*

*76. I agree with the judge that it is indeed conceivable that relevant individuals—when they are acting in the role of developers—should be held to owe a duty in law to bitcoin owners not to compromise the owners' security in that way. It would be a duty which involves abnegation of the developer's self-interest. It arises from their role as developers and shows that the role involves acting on behalf of bitcoin owners to maintain the bitcoin software. It is also single minded in nature at least in the sense that it puts the interests of all the owners as a class, ahead of the developer's self-interest. It is, I would say, arguably a fiduciary duty. It is difficult to see what other sort of duty it could be. […]*

*78. A further step from here is to examine whether the arguable duties arising from the role the developers have undertaken include not only a negative duty not to exercise their power in their own self-interest but a positive one to introduce code to fix bugs in the code which are drawn to their attention. It would be a significant step to define a fiduciary duty in that way, but since the developers do have the practical ability to prevent anyone else from doing this, one can see why a concomitant duty to act in that way is properly arguable. […]*

*80. […] There may well not be a consensus amongst bitcoin owners that a given bug should be fixed in a particular way or at all. But the developers will still make a decision to make a change or not, and no doubt act in good faith in doing so. The fact there may not be a consensus amongst owners does not of itself undermine the*

*conclusion that the duty of developers is fiduciary in nature. If anything it serves to underline the fact that the owners really do place trust in the developers to make good decisions on their behalf. […]*

*86. Pulling all this together, I recognise that for Tulip's case to succeed would involve a significant development of the common law on fiduciary duties. I do not pretend that every step along the way is simple or easy. However there is, it seems to me, a realistic argument along the following lines. The developers of a given network are a sufficiently well defined group to be capable of being subject to fiduciary duties. Viewed objectively the developers have undertaken a role which involves making discretionary decisions and exercising power for and on behalf of other people, in relation to property owned by those other people. That property has been entrusted into the care of the developers. The developers therefore are fiduciaries. The essence of that duty is single minded loyalty to the users of bitcoin software. The content of the duties includes a duty not to act in their own self interest and also involves a duty to act in positive ways in certain circumstances. It may also, realistically, include a duty to act to introduce code so that an owner's bitcoin can be transferred to safety in the circumstances alleged by Tulip.*

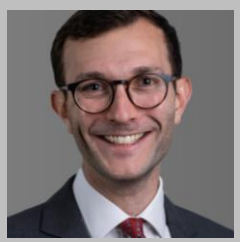
This is an important decision – albeit one reached only to the standard of arguability required in an application for service out – and one which has surprised many in the crypto industry because it appears to challenge the very idea of decentralisation. Of particular importance is Birss LJ's finding that the developers arguably owe positive duties to act to assist users, as well as negative duties not to act in their own self-interest. There can be little doubt that arguments along those lines will be made against other actors in the crypto industry – such as exchanges and trading platforms – in future cases. The substantive trial in Tulip Trading, at which these issues will fall to be determined authoritatively, will be watched very closely indeed.

## ABOUT THE AUTHORS

### Jacob Turner

Call Date: 2016

Jacob has advised individuals, corporates and sovereigns in a variety of commercial matters involving litigation and arbitration. He is described in the directories as “an outstanding junior barrister” who is “extremely engaged, responsive and hard-working”. Jacob has recently advised several clients on issues arising from the UK sanctions regime. This advice has included questions of whether entities are subject to sanctions, the preparation of licenses for submission to HM Treasury and the current practice of enforcement authorities.



### Aaron Taylor

Call Date: 2017

Aaron has a broad commercial practice, with a particular interest in civil fraud & commercial crime, and in the law relating to art & cultural property. He is currently acting for the claimants in two cases involving the misappropriation of crypto assets. Aaron was junior counsel for the defendant in *Federal Republic of Nigeria v JPMorgan Chase Bank NA* [2022] EWHC 1447 (Comm) a high-profile *Quincecare* claim. He is on the Serious Fraud Office’s “C” Panel for international proceeds of crime cases.