

WHEN COURTS DO NOT UNDERSTAND CRYPTO ASSETS AND BLOCKCHAIN TECHNOLOGIES

D'ALOIA V PERSONS UNKNOWN CATEGORY A & ORS [2025] 1 WLR 821

HANNAH YEE-FEN LIM*

In *D'Aloia*, the English High Court was presented with a crypto assets fraud dispute that was highly complex and technical, but found the evidence of both expert witnesses to be unhelpful. Neither expert witness had formal qualifications in computer science, and the court found the evidence of one expert witness to be chaotic, inconsistent and contradictory, which made it difficult for the court to apply the relevant laws cogently. This case highlights the necessity of having strong, accurate and coherent expert evidence, especially in complex cryptocurrency matters. This comment aims to expound and analyse the deficiencies in the presentation and understanding of the complicated functioning of the technology of blockchains, which impacted the court's ability to distil the correct facts, undermining its capacity to accurately apply the laws of tracing and following.

I. INTRODUCTION

The case of *D'Aloia v Persons Unknown Category A & Ors*¹ is one of the first cases heard in the UK on crypto assets that is not interlocutory and not summary and both parties were able to present arguments and be heard. The decision turned very much on the evidence of expert witnesses, but unfortunately, the court found “the evidence of both experts, particularly their reports, not to be especially helpful”.²

The facts of this case present a classic textbook example of the *modus operandi* of modern-day online scams. There were seven defendants, and the decision concerned the Sixth Defendant, Bitkub Online Co Ltd (“Bitkub”). In December 2021, the plaintiff, D'Aloia, opened an account (“Fake Account”) on a fake website³ which the plaintiff believed to be that of TD Ameritrade, a legitimate regulated US brokerage, but which was in fact operated by fraudsters alleged to be the First

* BSc (computer science), LLB, LLM (Hons), Associate Professor of Business Law, Nanyang Technological University, Singapore. The author thanks Kenneth ZH Sim for his earlier research assistance. The author is grateful to and also thanks Associate Professor Sandra Booyesen for her encouragement and the opportunity to present this work at an earlier NUS Centre for Banking and Finance Law Seminar. This research is supported by the National Research Foundation, Prime Minister's Office, Singapore under its Campus for Research Excellence and Technological Enterprise (CREATE) programme.

¹ *D'Aloia v Persons Unknown Category A & Ors* [2025] 1 WLR 821 [*D'Aloia*].

² *Ibid* at [48].

³ *Ibid* at [78].

Defendants.⁴ Subsequently, the plaintiff began transferring cryptocurrencies to wallets linked to the Fake Account.⁵ To be clear, scientifically, a cryptocurrency wallet “is a software product or physical device that stores the public and private keys to cryptocurrency accounts”⁶ so that cryptocurrencies can be sent to or received from the wallet address. In this manner, it is similar to how an email address functions and it is not to be confused with physical real wallets.

The critical transfers began on 10 January 2022 when D’Aloia transferred 999,987.1 USDTs, also known as Tether, a cryptocurrency that is pegged one-to-one to the US dollar, to crypto wallet “1dDa”, which was allegedly controlled by the First Defendants.⁷ The plaintiff became suspicious when all his open trades were closed.⁸ After an initial withdrawal request of \$1,000 failed and the Fake Account was purportedly blocked, the First Defendants repeatedly convinced him to transfer substantial sums of money to the Fake Account, including for the purpose of upgrading to a VIP account, or on the pretence that the plaintiff was under suspicion for money laundering and insider trading, amongst other offences, and requested payment of 4% or 5% of his balance each time to unblock his account.⁹ Even when the plaintiff requested all his trades be closed and all sums in his account to be transferred to him, he was told he had to pay a 30% profit tax.¹⁰ In total, about £2.5m in Tether¹¹ was transferred before the plaintiff realised that he had been defrauded.¹²

The cryptocurrencies in question were transferred through multiple crypto wallets (“Wallets”) before being withdrawn as fiat currency.¹³ In particular, the transfer dated 10 January 2022 to a Wallet controlled by the First Defendants was alleged to have undergone multiple successive transfers to different crypto exchanges.¹⁴ The plaintiff alleged that through the series of 14 transfers, some of the USDTs transferred to the First Defendants (“Identifiable USDT”) could be traced as part of a specific lot of USDT 400,000 received on 21 February 2022 by the “82e6 Wallet” that was linked to an account belonging to Ms Hlangpan (“Ms H”) held with Bitkub.¹⁵ Ms H was a “level one” customer on Bitkub¹⁶ with a declared income of THB15,000–29,999 per month¹⁷ and was thus subject to a daily withdrawal limit of THB2m;¹⁸ yet, almost the entirety of the USDT 400,000, equivalent to US\$400,000, was withdrawn on two days,¹⁹ with THB9m withdrawn in three minutes.²⁰

⁴ *Ibid* at [77]–[78].

⁵ *Ibid* at [78].

⁶ Kaspersky, “What is a crypto wallet and how to protect it” <<https://www.kaspersky.com/resource-center/definitions/what-is-a-crypto-wallet>>.

⁷ D’Aloia, *supra* note 1 at [80].

⁸ *Ibid* at [102(i)].

⁹ *Ibid* at [102(ii)]–[102(iv)].

¹⁰ *Ibid* at [102(vi)].

¹¹ *Ibid* at [2].

¹² *Ibid* at [102].

¹³ *Ibid* at [2].

¹⁴ *Ibid* at [80].

¹⁵ *Ibid* at [79].

¹⁶ *Ibid* at [86].

¹⁷ *Ibid* at [87].

¹⁸ *Ibid* at [88].

¹⁹ *Ibid* at [93].

²⁰ *Ibid* at [89].

II. DECISION

The court had an extreme number of issues before it, ranging from pleading issues²¹ to property issues²² and numerous sub-issues, such as whether Bitkub failed to comply with its Know Your Customer (“KYC”) and Anti-money Laundering (“AML”) and corporate governance duties.²³ Indeed, the claim made by D’Aloia at trial was not, in key respects, that pleaded in the Re-amended Particulars of Claim and the Re-amended Reply, making the case more complex than it already was.²⁴

The 88-page judgment saw the court traverse a wide range of matters but, at the core, the key questions revolved around the plaintiff’s claim against Bitkub in unjust enrichment and various equitable property claims alleging constructive trusts.

A. Property Issues

In order to resolve the issue of constructive trusts, the court had to decide whether USDT is property under English law, what kind of property it is and how such nature affects its ability to be the subject of equitable claims.²⁵

The court recognised USDT as a distinct form of property consistent with the Property (Digital Assets etc) Act²⁶ that received Royal Assent on 2 December 2025. Taking a similar approach as the Law Commission of England and Wales Report, *Digital Assets: Final Report*²⁷ (“Final Report”) published on 28 June 2023, upon which the Act is premised, the court affirmed that the USDT is neither a chose in action nor a chose in possession but is a form of property.

Nevertheless, in contrast to the Final Report, the High Court refused to combine all property that was neither choses in possession nor choses in action into a single third category.²⁸ It also noted that this would be “consistent” with the approach laid out in the Property (Digital Assets etc) Act.²⁹ Furthermore, it held that the “starting point” of the test for property in *National Provincial Bank v Ainsworth*³⁰ (“*Ainsworth*”) would often be decisive.³¹

The High Court followed precedent cases that had already held that Bitcoin passed the *Ainsworth* test and constituted property under English law.³² Applying these cases to USDT, USDT is similar, only with the addition of proof of reserves.³³

²¹ *Ibid* at [4].

²² *Ibid* at [5].

²³ *Ibid* at [13].

²⁴ *Ibid* at [26].

²⁵ *Ibid* at [5].

²⁶ Property (Digital Assets etc) Act 2025 (c 29) (UK).

²⁷ England and Wales (United Kingdom), The Law Commission, *Digital Assets: Final Report* (Report Law Com No 412, 28 June 2023) (Chairman: The Right Honourable Lord Justice Green).

²⁸ *D’Aloia, supra* note 1 at [153(iii)].

²⁹ *Ibid*.

³⁰ *National Provincial Bank Ltd v Ainsworth* [1965] AC 1175.

³¹ *D’Aloia, supra* note 1 at [153(iv)].

³² *Ibid* at [154].

³³ *Ibid*.

Hence, the court held that USDT also passed the *Ainsworth* test and is property under English law.³⁴ Even though USDT was not a chose in action, the authorities had shown that property rights could be granted as long as there is an “expectation with a sufficient basis”.³⁵ In the case of Bitcoin and USDT, there is “more than a mere hope that transactions will be honoured” because of the “cryptographic security” of the blockchain that is designed to ensure the transactions are honoured.³⁶

B. Property and Tracing and Following Issues

With the court holding that USDT is a recognised form of property in English law, the court then went on to consider the issue of tracing and following the plaintiff’s USDTs. For the plaintiff’s claim to succeed, he would need to show how his USDT was paid into a fraudster-controlled wallet, entered the 82e6 Wallet and was eventually converted into fiat currency; thus, an examination of the law on following and tracing was required.³⁷

The court noted that Bitkub’s counsel argued that the plaintiff had only expressly pleaded following and not tracing in its submissions, and this was accepted by plaintiff’s counsel in qualified terms but the High Court felt it remained an issue for determination.³⁸ The High Court cited *Foskett v McKeown*³⁹ and agreed that following and tracing were two different concepts.⁴⁰ Following was the process of following the same asset as it moved, while tracing looked at replacements for the previous asset.⁴¹ However, the High Court disagreed with Bitkub’s counsel regarding the plaintiff’s pleadings.⁴² The plaintiff’s Re-amended Reply contained references to “substitutes” and “substitute assets”, which imply tracing.⁴³ Furthermore, the Supreme Court had noted in *Byers v Saudi National Bank*⁴⁴ that tracing and following are commonly referred to as tracing collectively or interchangeably,⁴⁵ and given this, it would be strange if following had to be restricted to its strict meaning.⁴⁶

The court embarked on a long discussion of the case law of tracing but concluded that English law still recognises separate regimes for tracing in equity and at common law; thus it was bound by the case of *Agip (Africa) Ltd v Jackson*⁴⁷ which held tracing through a mixed fund at common law was not possible.⁴⁸

³⁴ *Ibid.*

³⁵ *Ibid* at [155].

³⁶ *Ibid.*

³⁷ *Ibid* at [174].

³⁸ *Ibid* at [175].

³⁹ *Foskett v McKeown* [2001] 1 AC 102 at 127B.

⁴⁰ *D’Aloia, supra* note 1 at [176].

⁴¹ *Ibid.*

⁴² *Ibid* at [178].

⁴³ *Ibid* at [179].

⁴⁴ *Byers v Saudi National Bank* [2024] AC 1191 at [68].

⁴⁵ *D’Aloia, supra* note 1 at [180].

⁴⁶ *Ibid* at [181].

⁴⁷ *Agip (Africa) Ltd v Jackson* [1991] Ch 547 at 566B [*Agip*].

⁴⁸ *D’Aloia, supra* note 1 at [200].

Tracing in equity was possible and the court spent more than 15 pages discussing methods of tracing. It was unclear what method of tracing the plaintiff's expert witness had employed, but it appeared that he had not used any one of the three established methods of First In First Out ("FIFO"), *pari passu* distribution or the rolling charge methodology, but rather a modified form of FIFO.⁴⁹

The High Court cited the Privy Council case of *Federal Republic of Brazil v Durant International Corporation*,⁵⁰ which highlighted the increasing complexity of money laundering schemes and emphasised that equity should correspondingly focus on substance and not form.⁵¹ Thus, with this, the High Court held it was open to a plaintiff, especially in a case of fraud, to use a tracing method other than the three recognised methodologies "provided that it treated all innocent claimants and potential claimants comparably and was properly evidenced".⁵²

The plaintiff's expert witness, Moore, had relied on third-party software systems for the purposes of tracing and it was unclear how the two systems function and moreover, they gave inconsistent results which were not explained. The High Court criticised Moore's evidence for being "chaotic and, ultimately, contradictory".⁵³ Moore claimed to have used methodologies "taught by Crystal Blockchain and TRM Labs".⁵⁴ These methodologies were not disclosed and no evidence was presented evidencing these methodologies.⁵⁵ It was not surprising then that the court was not satisfied as to why Moore's approach could be relied on.⁵⁶ Thus, the High Court held that Moore's evidence failed to prove that the plaintiff's funds factually entered the 82e6 Wallet.⁵⁷ Given the sketchy evidence on the methodology, it could not be shown that all potential innocent victim claimants were treated equally.⁵⁸ Thus, any claims based on tracing were factually defeated.⁵⁹

Regarding the claim on following, the court upheld that common law does not allow following through mixed funds for two reasons, as set out succinctly by the court in *Agip*.⁶⁰ First, only physical assets can be followed, not choses in action. Second, money can be followed at common law into and out of a bank account so long as it does not cease to be identifiable by being mixed with other money in the bank account derived from another source. Thus, the court held that money that flows into a mixed fund loses its identifiability and cannot be followed.⁶¹

As for the treatment of USDT for the purposes of following, the court noted that it preferred the second analysis, the "persistent thing analysis" set out in the Final Report: that is, the transfer of USDT preserves the identity of the crypto asset and

⁴⁹ *Ibid* at [214]–[217].

⁵⁰ *Federal Republic of Brazil v Durant International Corporation* [2016] AC 297.

⁵¹ *D'Aloia*, *supra* note 1 at [219].

⁵² *Ibid* at [221].

⁵³ *Ibid* at [58].

⁵⁴ *Ibid* at [59].

⁵⁵ *Ibid*.

⁵⁶ *Ibid* at [263]–[264].

⁵⁷ *Ibid* at [264].

⁵⁸ *Ibid* at [261].

⁵⁹ *Ibid* at [263]–[264].

⁶⁰ *Ibid* at [201].

⁶¹ *Ibid*.

the token as a notional quantity unit that can be tracked as it passes through the system.⁶² However, the High Court noted that this was “difficult to reconcile” with *Piroozzadeh v Persons Unknown* (“*Piroozzadeh*”),⁶³ where the extreme difficulty of tracing (or following) USDT swept into a hot wallet was noted as a “‘possibly impossible’ exercise”.⁶⁴

Nevertheless, the court found that in line with the conclusions of the Final Report, since USDT is persistent across transfers, theoretically it can be followed.⁶⁵ However, in this case, there was a lack of evidence that would allow following of the USDT as Moore had testified he was not in a position to say with certainty how much, if anything, of any given sum was D’Aloia’s USDT.⁶⁶

C. Unjust Enrichment and Know Your Customer and Anti-money Laundering Issues

The court nevertheless went on to consider the unjust enrichment issue and, within examining this, the court considered a number of sub-issues and relevant defences. First, the court considered whether Bitkub failed to comply with its KYC/AML and corporate governance duties. On this, the court went into detail about the circumstances surrounding Ms H’s receipt of the USDT 400,000.⁶⁷ Ms H opened her account with Bitkub in May 2021.⁶⁸ The associated 82e6 Wallet was purportedly a custodial wallet whose private key was held by Bitkub.⁶⁹ Thus, Ms H would have to instruct Bitkub to execute any transactions relating to the 82e6 Wallet.⁷⁰ However, from the facts set out in the judgment, it seems that it may not have been a custodial wallet as the judgment referred to Ms H being able to withdraw THB9m in three minutes.⁷¹ If it was a custodial wallet, it would not have been possible for so much to be withdrawn in only three minutes, because instructions would have had to be given to Bitkub to action the instruction, and Bitkub would have had the further obligations to ensure the daily limits were not exceeded, but it appears none of this happened.

One of the Bitkub witnesses was Ms Vijitpinyo (“V”), an assistant KYC manager at Bitkub, who gave evidence via video link through a translator and was noted to be “very cautious in her answers” to the point that counsel put it to her that she was being evasive.⁷² Apart from Bitkub’s processes, V did not have much evidence to give.⁷³

⁶² *Ibid* at [204].

⁶³ *Piroozzadeh v Persons Unknown Category A and others* [2023] EWHC 1024 (HC, Eng) [*Piroozzadeh*].

⁶⁴ *D’Aloia*, *supra* note 1 at [208].

⁶⁵ *Ibid* at [210].

⁶⁶ *Ibid* at [212].

⁶⁷ *Ibid* at [76]–[80].

⁶⁸ *Ibid* at [82].

⁶⁹ *Ibid* at [81].

⁷⁰ *Ibid*.

⁷¹ *Ibid* at [89].

⁷² *Ibid* at [41]–[42].

⁷³ *Ibid* at [42].

She was not involved in the relevant transactions.⁷⁴ At one point, she was questioned on a Thai law that had been translated to English then back to Thai, questions that the High Court noted even a lawyer would have had difficulty answering. Hence, the High Court accepted the submission by plaintiff's counsel that V's evidence was of limited assistance.⁷⁵

Significantly, the High Court noted that during cross-examination of V, the plaintiff's counsel had put to V that Bitkub's daily withdrawal limits were for AML purposes. V claimed she did not know why Bitkub implemented daily withdrawal limits. The High Court did not believe this.⁷⁶ V described herself as being in a "senior manager role"⁷⁷ in Bitkub's AML system and was part of the team that performed customer due diligence.⁷⁸ Thus, she ought to have known the rationale. Furthermore, the High Court believed V had actual knowledge of the said rationale. V's evidence showed familiarity with Bitkub's different customer categories and the need for increased scrutiny if a customer wanted withdrawal limits raised. She also disclosed how Bitkub's systems assessed customer risk, how due diligence takes longer for higher-risk customers, and even highlighted that details of these processes could not be explained as doing so would violate the Thai Anti-money Laundering Act.⁷⁹ Hence, the High Court found that Bitkub's daily withdrawal limits were for AML purposes, and V just did not admit it.⁸⁰

The evidence given was that a block would have been triggered on Ms H's account immediately before the receipt of the USDT 400,000,⁸¹ but Bitkub had produced no witnesses who could explain why or how the block on Ms H's account had been removed or why there was no block and why no withdrawal limit was set, a lacuna that appeared to the High Court to have occurred through Bitkub's own act or omission.⁸²

Significantly, regardless of the conduct of Bitkub, it could not be ascertained that Bitkub was subject to Thai KYC/AML law, and determining its compliance with said laws would require expert evidence to be introduced and pleadings to be amended. However, a Chancery master had refused permission for the former, and a High Court judge had refused permission for the latter.⁸³ Thus, the opening of Ms H's account with Bitkub was held not to raise KYC concerns.⁸⁴ The court, however, found that the withdrawal limits that Ms H breached were part of Bitkub's AML policy, such that any breaches of the limits represented an AML concern from Bitkub's perspective.⁸⁵ As such, the court found that Bitkub could not rely on the

⁷⁴ *Ibid* at [41].

⁷⁵ *Ibid* at [42].

⁷⁶ *Ibid* at [43].

⁷⁷ *Ibid* at [41].

⁷⁸ *Ibid* at [44].

⁷⁹ *Ibid*.

⁸⁰ *Ibid* at [45].

⁸¹ *Ibid* at [46].

⁸² *Ibid*.

⁸³ *Ibid* at [84].

⁸⁴ *Ibid* at [85].

⁸⁵ *Ibid* at [311(iii)].

defence of a good faith purchaser for value without notice.⁸⁶ Not only was there no block imposed and no alarms raised on Bitkub's systems, putting Bitkub on notice before the receipt of USDT 400,000 said to contain D'Aloia's funds, but Bitkub also allowed Ms H to pay those funds away; hence, Bitkub had actual notice of the risk that Ms H's account was being used for money laundering.⁸⁷

D. *Unjust Enrichment and Tracing*

On the issue of whether there was enrichment at the expense of the plaintiff, the High Court returned to its finding that as a matter of law, the plaintiff cannot trace through a mixed fund in support of his unjust enrichment claim.⁸⁸ The court had found that D'Aloia did not demonstrate that his funds could be traced to the 82e6 Wallet as a matter of fact, and, because of this, the argument of unjust enrichment failed on both ways of connecting the enrichment to the plaintiff, that is, through sham and tracing.⁸⁹

E. *Equitable Proprietary Claim*

The plaintiff also pursued equitable proprietary claims against Bitkub, arguing that a constructive trust could arise in four ways.⁹⁰ However, again, the finding that the funds belonging to the plaintiff could not be traced to the 82e6 Wallet as a matter of fact proved to be the insurmountable hurdle.

The High Court found a constructive trust against the First Defendants that arose over the funds they received from the plaintiff at the point of transfer⁹¹ but found no constructive trust on Bitkub because factually, the plaintiff could not prove that his funds reached Bitkub.⁹²

III. ANALYSIS

There are several troubling aspects to the decision, both in terms of the reasoning and conclusions and in the understanding of the technology that led the court down the path of misapplying the relevant laws. While it could be said that poor evidence from the expert witnesses of both parties played a critical role in causing the English High Court to misstep, the court, however, did make decisions of its own accord that were internally inconsistent. There are salient lessons to be learnt from this decision for parties, counsel and the judiciary.

⁸⁶ *Ibid* at [379].

⁸⁷ *Ibid* at [379]–[380].

⁸⁸ *Ibid* at [270].

⁸⁹ *Ibid* at [278].

⁹⁰ *Ibid* at [332].

⁹¹ *Ibid* at [341].

⁹² *Ibid* at [342], [378].

A. *Expert Witnesses Without Computer Science Qualifications*

First, neither party's expert witness had any training or background in computer science; rather, their backgrounds were in policing and military communications,⁹³ which may not be terribly relevant to a high-technology case such as this. This era of computer forensics calls for expert witnesses to be specially trained in computer science, in particular, those with significant experience in blockchain technology. The experts must have a thorough understanding of blockchain technology and how the third-party software systems for tracing crypto assets function. As will be highlighted below, part of the problem lay with the erroneous expert witness evidence of Moore when he gave inaccurate evidence that resulted in incorrect facts on technology and muddled reasoning and conclusions. Moore had also relied on two third-party tracing services, but it was clear that he was unable to explain how the results were derived, to the point that the court said that his expert evidence was inconsistent and "contradictory".⁹⁴ Indeed, the court said that Moore's "methodology was described in three different places and in three different, contradictory ways".⁹⁵

The criticisms of the expert witnesses were not just levelled against Moore but also against Bitkub's expert witness, Pinto. The court found that:

Reconciling the times of different transactions within Mr Pinto's report was difficult, if not impossible, since what seem to be the same Hops are described with different time stamps in different tables. Equally, wallet addresses in places appeared to be incorrect and in one case (Hop 12), Mr Pinto identified two different transactions as the same Hop. Payments in the table analysing the Hop 1 transaction are described as 'Inbound (non-claimant)' yet appear to come from Mr D'Aloia's Coinbase account. Finally, Mr Pinto used the term Hop to describe both the movement of funds and the origin or destination of those funds. For example, he described Hop 2 simply as 'Hop 2', but the next transaction as 'Hop 2 to Hop 3 transaction'. It would have been clearer had he been consistent.⁹⁶

Thus, given the importance of expert witness evidence in blockchain and crypto asset cases to assist the usually non-technologically trained court, parties should ensure their expert witnesses are truly qualified and competent in scope and breadth and have the requisite computer science expertise.

B. *The High Court's Internally Inconsistent Reasoning*

Second, the court appears to be internally inconsistent in its reasoning processes. Many aspects of the judgment relied on one of the core findings in the decision that the USDT could not be traced in a mixed fund at common law. Implicit in this is the acceptance that because the fund is a mixed fund, the USDT therefore ceases to be

⁹³ *Ibid* at [47].

⁹⁴ *Ibid* at [58].

⁹⁵ *Ibid* at [259].

⁹⁶ *Ibid* at [50].

identifiable. Certainly, this was one reason why the court proceeded to undertake the long examination of tracing in equity. However, when the court examined following the USDT, it said that the “evidence before me suggests that the identity of the USDT was preserved despite mixing and could be evidenced. On that basis it seems to me that following should, in principle, be an option”.⁹⁷ On the one hand, the court felt that the identification of the USDT was lost in the mixture of a mixed fund for tracing, but on the other hand, for the issue of following, the court appears to accept that the identification of the USDT was preserved even in a mixed fund, both from the evidence before it and from relying on the Final Report.⁹⁸

C. *Inaccurate Expert Testimony*

Third, the High Court was unfortunately hindered by the poor expert witness evidence and equally poor understanding of technology by the legal counsel. There are a number of instances of this, the most critical being during the cross-examination of Moore by Bitkub’s counsel during which Moore categorically gave evidence that it is not possible to identify individual USDT and then qualified it by stating that Tether themselves were the only people who could do so:

Q. You are not in a position to distinguish within the 200,000 where the 99-

A. No.

Q. - are located.

A. No. The only people who can do that, for example, is Tether themselves.⁹⁹

This evidence is simply incorrect, as evidenced by the Tether White Paper which the court also cited. Indeed, the court cited the relevant portions of the Tether White Paper being that “the transactional history of USDT is ‘publicly auditable’ (page 9)”.¹⁰⁰ Blockchains all rely on public key cryptography to function, and public key cryptography has scientifically been proven to be publicly auditable, with clear identifiability.¹⁰¹ The fact that it is publicly auditable means two things and this has been well documented in computer science and in legal literature.¹⁰² First, *anyone* can audit; hence the word “publicly” is used by the Tether White Paper, and not just the people who issue Tether, as Moore had incorrectly testified. Second, it is auditable meaning that all kinds of tracing can be done along with obtaining other information; this has been well documented and explained, and it is a general

⁹⁷ *Ibid* at [210].

⁹⁸ *Ibid*.

⁹⁹ *Ibid* at [205].

¹⁰⁰ *Ibid* at [206].

¹⁰¹ Yee Fen Lim, “Digital Signatures, Certification Authorities: Certainty in the Allocation of Liability” (2003) 7(1) *Sing JICL* 183 available in CommonLII, [2003] *SGJIntCompLaw* 9; Ying-Chang Liang, *Dynamic Spectrum Management: From Cognitive Radio to Blockchain and Artificial Intelligence* (Singapore: Springer Nature, 2020) at 122–127, 140, 142.

¹⁰² *Ibid*.

feature of blockchains.¹⁰³ Thus, USDT is also identifiable despite being “mixed” in with other USDT. This is supported by other parts of the Tether White Paper; for example, the full sentence from which the court cited states:

Tether Limited issues all tethers via the Omni Layer protocol. Omni operates on top of the Bitcoin blockchain and *therefore all issued, redeemed, and existing tethers, including transactional history, are publicly auditable* via the tools provided at [Omnichest.info](https://omnichest.info).¹⁰⁴ [emphasis added]

It appears that the court did not understand what was meant by “*publicly auditable*” because the court concluded that “Mr Moore’s answer was consistent with the Tether White Paper”¹⁰⁵ when this was clearly not the case. For completeness, the paragraph cited above mentioned the Omni Layer protocol: this is simply a protocol layer that just sits on top of the Bitcoin blockchain, just like the Internet has many layers and protocols, such as TCP/IP, FTP and HTTP.¹⁰⁶

Further, if the court, the expert witnesses and the counsel really understood that blockchain technology uses public and private key pairs as the driving cryptographic technology, it would have been abundantly clear that their mathematical and cryptographic nature inherently ensures that transactions are uniquely identifiable, transparent and publicly traceable due to the use of hash functions and public and private key pairs. Legal jurisprudence explaining the science and functioning of this has been freely and publicly available since 2003 and there is no need to re-explain this here.¹⁰⁷

It is unfortunate that the expert evidence and the court came to the erroneous conclusion on the identifiability of USDT and held that USDT when mixed with other funds becomes non-identifiable, and thus held that tracing at common law was not available. Factually, a suitable analogy for USDT in a so-called mixed fund would be making a list of the numbers on banknotes (money) and to whom each banknote belongs and placing all the banknotes into a box. While the banknotes inside the box may be mixed in the sense that several people may own the banknotes, they remain clearly identifiable because of the list of owners and banknote numbers, and hence tracing at common law would be available. On the facts, the expert witnesses may not have been helpful, but it may have been open to the court to make other orders or even to seek the appointment of an *amicus curiae*, now formally known as an Advocate to the Court in the UK. This is especially so since so much of the decision hinged on the erroneous finding that the USDT cannot be identified and cannot be traced in a mixed fund.

¹⁰³ *Ibid.*

¹⁰⁴ Tether, “Tether: Fiat currencies on the Bitcoin blockchain” <<https://assets.ctfassets.net/vyse88cgwfb/5UWgHMvz071t2Cq5yTw5vi/c9798ea8db99311bf90ebe0810938b01/TetherWhitePaper.pdf>> at 9.

¹⁰⁵ *D’Aloia*, *supra* note 1 at [206].

¹⁰⁶ BBC, “Wired and wireless networks, protocols and layers - OCR” <<https://www.bbc.co.uk/bitesize/guides/zr3yb82/revision/3>>.

¹⁰⁷ Lim, *supra* note 101.

D. *The Court's Wholesale Adoption of Technology From
Piroozzadeh v Persons Unknown*

Fourth, it was unclear why the High Court appeared simply to cite and rely on the words of Trower J in *Piroozzadeh* resulting in affirming statements that may be factually and technologically incorrect for the case at hand. The High Court did not provide any clear evidential basis for the decision to rely on Trower J's words. Given the factual and technological differences between this case and *Piroozzadeh*, the wholesale adoption of *Piroozzadeh* is troubling and problematic.

The problematic portion cited and relied upon by the High Court is:

The uncontradicted evidence adduced by the eighth defendant is that the user does not retain any property in the Tether deposited with the exchange. As it is put in Mr Quest's skeleton argument, the user's account is credited with the amount of the deposit and they are then permitted to draw against any credit balance as in a conventional banking arrangement. The Tether, like other crypto assets, are then swept into a central unsegregated pool address known as a 'hot wallet' where they are treated as part of the eighth defendant's general assets. They are not specifically segregated to be held for the sole benefit of the user from whose account they have been transferred.¹⁰⁸

The Eighth Defendant in *Piroozzadeh* was Binance Holdings Limited ("Binance").¹⁰⁹ It is clear from this paragraph that the business set-up of Binance, the defendant exchange in the case of *Piroozzadeh*, does not permit the user to retain any property in the Tether, and thus, even in the so-called hot wallet, the crypto assets are not "specifically segregated to be held for the sole benefit of the user".

This, however, is quite different from Bitkub. While it is not possible to access the User Agreement in force between 2021 and 2022, the current Bitkub User Agreement¹¹⁰ dated October 2023 sheds some light on what it may have been. In the current Bitkub User Agreement, clause 11.3 states "The User acknowledges that the Company holds The User' [sic] assets, both money and Digital Assets, in compliance with rules and conditions specified by the law." This is a clear statement that unlike Binance, the set-up on Bitkub is such that it is the user, not Bitkub, who retains property in the Tether (Digital Asset) deposited.

Further, the User Agreement also makes reference to "Excessive Assets" as defined in clause 13.5 as the "money, Digital Assets and benefits excessively received by the User". For such Excessive Assets, clause 13.5 also explicitly provides that the "User agrees that the User does not have any rights over the Excessive Assets, including but not limited to ownership, possessory rights, retention rights, and/or right of use" and goes on to impose a duty on the user to notify Bitkub

¹⁰⁸ *D'Aloia*, *supra* note 1 at [91].

¹⁰⁹ *Piroozzadeh*, *supra* note 63.

¹¹⁰ Bitkub Exchange, "Bitkub User Agreement" <https://www.bitkub.com/en/tos?_gl=1*8t16z9*_ga*MjJwNDczNzAuMTc1NjY0MTEyNQ..*_ga_K0M1H767C1*cze3NTY2NDYzNDMkbzIkZzEkdDE3NTY2NDcxODAKajJlJGwwJGgw> (28 August 2024).

expeditiously about the Excessive Assets. The fact that such explicit clauses are needed for Excessive Assets also demonstrates that the Digital Assets held by users on Bitkub are indeed retained and owned by users and they are distinguished from the Excessive Assets.

Thus, it is clear that the Bitkub business set-up is markedly different from that of Binance; hence, it would appear to be inappropriate for the High Court to simply adopt what was stated in *Piroozzadeh* on sweeping and tracing.

It is also somewhat alarming that the High Court simply adopted what another judge said in relation to a different crypto exchange, that is, Binance, and transported it to the Bitkub exchange. Each exchange operates differently in terms of its operations and set-up and these kinds of presumptions cannot be so easily made. Further, the High Court seems to have assumed that just because the case of *Piroozzadeh* concerned USDT, it can embark on a wholesale adoption of the description of the processes and technology. The truth is, USDT currently exists on around 13 blockchains or platforms, including Ethereum and Celo blockchains.¹¹¹ Each of these blockchains is implemented differently, even as each utilises public key cryptography, and it is not a case of uniform operations, nor uniform implementation of the technology of blockchain and other aspects of the system.

IV. BROADER LEGAL SIGNIFICANCE

This case highlights the need for precise pleadings in complex cryptocurrency matters, especially involving tracing, and the necessity of having strong, accurate and coherent expert evidence. The “mixed funds” in each of the series of 14 transfers are not truly “mixed” in the way that money in bank accounts is normally mixed and should not be considered mixed funds because all the USDTs are identifiable. The “mixed fund” on Bitkub during the so-called “sweep” before withdrawal as fiat currency is also questionable, given its basis is not entirely elucidated and appears to be based on the technology and set-up of an entirely different crypto exchange. As they are not true mixed funds, common law tracing and following could have been applied by the court.

Courts, the judiciary and counsel should understand the complex technology of blockchains in an adequate way in order to ensure the facts are factually correct before applying and administering the law, including the appointment of a well-qualified *amicus curiae* where necessary.

The broader legal significance of this case underscores the essential obligation of cryptocurrency exchanges to maintain vigilance in monitoring for suspicious transactions and to address AML risks. While some significant questions regarding the liability of cryptocurrency exchanges towards victims of fraud remain unresolved, such as whether a constructive trust would be established in situations where exchanges do not fulfil their obligations, this case indicates that certain conduct by exchanges would be held against them.

¹¹¹ Tether, “Supported Protocols and Integration Guidelines” <<https://tether.to/en/supported-protocols/>>.

Ms H's account was not blocked before the receipt of the USDT 400,000, nor was there any explanation as to why no withdrawal limit was set, failures which resulted from Bitkub's own acts or omissions, and which were contrary to its own policies regarding suspicious account activity. Bitkub further breached obligations under its own AML policy to ensure the daily withdrawal limits were not exceeded. These were sufficient for the court to find that Bitkub would not have been able to rely on the defence of good faith purchaser for value without notice because it had actual notice.¹¹²

Similarly, due to the actual notice, Bitkub would also not have been able to rely on the defences of good faith change of position and ministerial receipt in the claim for unjust enrichment.¹¹³

The case is evidence that in order to successfully invoke these defences, exchanges must implement robust AML and KYC systems, as well as maintain strict compliance. Exchanges may otherwise be exposed to well-substantiated claims from victims of fraud if stolen crypto assets can be satisfactorily traced to them.

¹¹² *D'Aloia*, *supra* note 1 at [380].

¹¹³ *Ibid* at [311]–[313], [316]–[328].