TL4 Essay Competition Submission

Author: Nataliya Yankovska

Firm: PCB Byrne LLP

Position: Associate

Admission Date: 14/10/2022

Final Word Count: 2709

Topic: *How Should Courts and Practitioners Adapt Enforcement Strategies to Address the Challenges of Tracing and Recovering Digital Assets?*

Introduction

There is no doubt that digital assets are no longer merely peripheral components of the financial ecosystem. In fact, they have become part of corporate workflows, cross-border commercial activities, and daily business operations.

However, the attributes that make digital assets so attractive to individuals and businesses alike (speed, decentralisation, and pseudonymity) make it extremely difficult for victims of fraud to locate and recover misappropriated assets. In today's digital world, where transfers are often made in seconds, wallets more often than not do not correspond to specific individuals, and most systems lack a central authority that can reverse transactions, courts and practitioners are faced with a significant challenge in applying established principles of property, equitable tracing, and evidence in a landscape fundamentally different from the quintessential banking environment in which those legal principles were originally established.

Nevertheless, English courts have demonstrated remarkable adaptability in handling disputes involving digital property, despite digital assets being a relatively novel concept. It is now a well-established principle that crypto assets such as Bitcoin *"meet the four criteria set out in Lord Wilberforce's classic definition of property"* in *National Provincial Bank v Ainsworth*[1], a principle that underpins the enforcement of proprietary claims in this area[2]. Further, several recent cases, including *D'Aloia v Persons Unknown*[3] and *Crypto Open Patent Alliance v Craig Steven Wright*[4], illustrate that familiar doctrines of equity and evidence can be readily applied to digital contexts. Having said that, these judgments also reveal the practical limitations in enforcement strategies, particularly in tracing digital transactions and dealing with evidential complexity.

Consequently, this essay will address the doctrinal basis for enforcement and the practical challenges that arise, before moving on to the essay's primary purpose: how courts and practitioners may adapt their enforcement strategies in light of these circumstances.

---

[1] [1965] 1 AC 1175.
[2] AA v Persons Unknown [2019] EWHC 3556 (Comm).
[3] [2024] EWHC 2342 (Ch).
[4] [2024] EWHC 1198 (Ch).

Enforcement of Digital Assets: The Foundation

It is now firmly established that cryptoassets can attract property rights under English law. As a result of *AA v Persons Unknown*, Bitcoin was found to meet the criteria in *National Provincial Bank v Ainsworth*: it is *"definable, identifiable by third parties, capable in [its] nature of assumption by third parties, and [has] some degree of permanence."* As a result of this conclusion, practitioners are now able to exercise all of the traditional proprietary remedies, including injunctions, tracing, following, constructive trusts and unjust enrichment claims.

The same reasoning was broadly applied in *D'Aloia* in respect of Tether (USDT). Although USDT is *"neither a chose in action nor a chose in possession, but rather a distinct form of property not premised on an underlying legal right"*, the Court held that it nevertheless constitutes property. Specifically, its proprietary nature stems from its *"transactional functionalities",* particularly the ability of a private-key holder to effect valid transfers through the system. Notably, the Court confirmed that this proprietary interest attaches to the token itself, not merely to the ability to control it. Therefore, proprietary claims may be brought even against unidentified wrongdoers, provided that the claimant can establish that the misappropriated asset has a sufficiently strong proprietary basis.

In combination, these developments provide a coherent framework for applying orthodox proprietary principles to digital assets. As a result, the law has developed the ability to recognise digital tokens as property, to analyse them within familiar boundaries of equitable ownership, and to allow claims to be brought even when the ultimate recipient of the misappropriated asset cannot be determined. What remains challenging, however, is whether existing enforcement mechanisms can keep pace with the technological and evidential realities of digital-asset transfers.

By examining the recent decisions in *D'Aloia* and *COPA v Wrigh*t, it becomes apparent that this issue is one of the most pressing.

***D'Aloia v Persons Unknown*: Tracing, Evidence, and the Limits of Exchange-Based Enforcement**

The case of *D'Aloia v Persons Unknown* illustrates both the strengths and limitations of applying traditional proprietary remedies to digital assets. In this case, the claimant alleged that he had been induced by fraud to transfer substantial amounts of USDT, which were then moved through a series of 14 transactions (hops) before USDT 400,000 reached a Bitkub wallet held by Ms Hlangpan, of which USDT 46,291 was alleged to represent USDT belonging to Mr D'Aloia or *"their traceable proceeds"*. These funds were then transferred to Bitkub's hot wallet, converted into fiat currency (Thai Baht) and withdrawn in violation of the daily withdrawal limit.

It was held by the Court that USDT falls within the definition of property under English law, that it may be traced, and that in principle, tracing may be carried out through mixed funds. However, the claimant failed, as a matter of evidence, to demonstrate that any of his funds in fact reached the 82e6 wallet: his expert's methodology departed from first in, first out principle (FIFO) without a clear, properly evidenced alternative, and no trace was attempted based on Tether Ltd's own records. A lack of evidential support was fatal to the tracing and unjust enrichment claims, since no evidence of *"at the expense of the claimant"* and certainty of subject matter could be properly established.

The Court acknowledged that a constructive trust arose against the fraudsters when they obtained the claimant's USDT under the fraudulent *td-finan* contract, and noted that, if that conclusion had been wrong, the rescission of the fraudulent agreement would have in principle

given rise to a constructive trust against them from the date of rescission. Nevertheless, no constructive trust was imposed directly on Bitkub for two decisive reasons. First, the claimant's tracing analysis was insufficient to establish that Bitkub ever received the claimant's funds. Further, even if the receipt had been established, the USDT reported to have reached the 82e6 wallet had already been paid out, leaving no remaining asset at Bitkub on which a proprietary constructive trust could be attached. This second difficulty might not have been fatal had the claimant pleaded a knowing receipt claim, but no such claim was advanced.

In this regard, *D'Aloia* highlights the structural reality of digital-asset enforcement: exchanges may be an appropriate enforcement target in principle, but liability relies exclusively on evidential detail and doctrinal accuracy.

***COPA v Wright*: Evidential Rigour and the Implications of Decentralisation**

While *D'Aloia* illustrates the evidential requirements of tracing digital assets, *COPA v Wright* demonstrates the judiciary's strict forensic scrutiny of digital records.

The *COPA v Wright* case concerned the authorship of the Bitcoin white paper. In order to determine if Dr Wright was the same person as Satoshi Nakamoto, the Court examined a large amount of digital material. Following Mellor J's examination of metadata, file histories, and document integrity, it was determined that some documents were fabricated. The rigorous approach to digital evidence is directly relevant to enforcement cases, in which parties must prove the authenticity of their electronic records (arguably to a higher degree than in conventional commercial/ financial disputes).

More generally, the technical background explored in *COPA v Wright* suggests that Bitcoin (and likely similar cryptoassets) operates as a decentralised, peer-to-peer system with no central authority capable of reversing transactions or altering the ledger. From an enforcement perspective, this has important implications. Given that the blockchain itself cannot comply with court orders, remedies will then be typically directed at actors who can comply, such as exchanges, custodians, wallet providers or other intermediaries, rather than at the ledger as an abstract system (which somewhat contradicts *D'Aloia's* limitations on who should be pursued).

Challenges in Tracing and Recovery

Accordingly, it appears that the difficulties associated with enforcing rights in digital assets are not a function of gaps in legal doctrine, but instead of the technological and evidential characteristics of blockchain systems. The recent decisions in *D'Aloia* and *COPA v Wright* illustrate four interconnected challenges that courts and practitioners must address.

1. Pseudonymity and the Structure of Blockchain Transactions

One challenge highlighted by the evidence structure in *D'Aloia* concerns how transactions are recorded on the blockchain. There were fourteen sequential "hops" by which USDT was allegedly transferred from the claimant, each described by an alphanumeric wallet address in the evidence. The judgment makes no comment on whether these addresses reveal the identities of their controllers; it simply records, as part of the factual narrative, that the wallet associated with 82e6 belonged to Ms Hlangpan, a Bitkub customer.

Furthermore, the judgment does not explain how Bitkub identified the customer behind the 82e6 wallet. However, the fact that the Court discusses Bitkub's KYC and AML procedures in relation to that account somewhat suggests that the identification was based on information held

by the exchange rather than anything visible on the blockchain. This is an inference from the structure of the evidence rather than an express finding of the Court.

However, the combination of these points illustrates the inherent difficulty of linking on-chain activities to real-world individuals: *D'Aloia's* blockchain record consisted solely of wallet addresses, and any link to human actors was only possible through information outside the ledger.

2. Speed of Movement and Rapid Dissipation

The second difficulty is the ease and speed with which digital assets can be transferred, exchanged, and withdrawn. In *D'Aloia*, once the USDT alleged to include the claimant's property reached the 82e6 wallet on 21 February 2022, the funds were swiftly swept into a Bitkub hot wallet, converted into Thai baht and withdrawn. By the time the claimant brought proceedings, none of his property was left within the exchange. Consequently, the time window in which effective action could have been taken was reduced by the rapidity with which value was transferred through digital systems.

3. Fragility and Manipulability of Digital Evidence

There is an inherent malleability to digital evidence. Documents may be altered, fabricated, or backdated in ways that may escape superficial scrutiny. A striking example can be found in *COPA v Wright*. Mellor J was required to analyse digital records purportedly predating the Bitcoin white paper and, through meticulous examination of metadata, file histories, and internal inconsistencies, concluded that several documents had been fabricated. It is evident from this case that courts are willing to subject digital materials to rigorous forensic analysis, and that parties cannot assume that electronic evidence will be accepted on its face.

4. Decentralisation and the Limits of Court Orders

Finally, the decentralised nature of blockchain systems restricts the scope of available remedies. This means that enforcement can realistically focus only on the practical "choke points" where digital assets interact with identifiable or regulated actors, such as exchanges, custodians, and service providers. Even though this might appear to be incompatible with *D'Aloia*, the judgment does not actually preclude claimants from targeting exchanges. Instead, it demonstrates that liability occurs only in cases where a claimant can demonstrate, with precision, that the exchange actually received the property, or where a properly pleaded knowing receipt claim (or possibly a claim in dishonest assistance) is made. Additionally, the case illustrates the importance of timing: once assets have been transferred to pooled wallets or withdrawn into fiat currency, the proprietary basis for a claim may be lost, necessitating immediate action before dissipation occurs.

Practical Adaptations for Effective Enforcement

Based on the above analysis, it can be concluded that the principles of property, evidence, and equitable tracing are sufficiently flexible to be applied to digital assets. It is, therefore, the practical implementation that poses the most significant challenge.

1. Adaptations for the Courts

First of all, there needs to be a better understanding of what constitutes sufficient evidence when it comes to the tracing of digital assets. *D'Aloia* provides an example of how tracing can fail not

because the law's unable to accommodate digital assets, but because the methodology is inadequately explained or supported. In this context, courts can serve as a source of assistance by articulating, through guidance or Practice Directions, what constitutes an acceptable tracing methodology. For example, the requirement that expert analysis be reproducible, data sources be identified, and methodology be justified in accordance with the token architecture.

The scope of disclosure requested from intermediaries should also be subject to judicial adaptation. In digital asset cases, Norwich Pharmacal and Bankers Trust orders are often used to obtain information required to identify wrongdoers or trace assets. However, as *D'Aloia* illustrates, internal records such as sweep data, violations of withdrawal limits, and compliance team interactions can also be crucial for understanding how assets were moved and managed. Even though the judgment does not specify the form that such orders should take, it demonstrates that effective tracing may require materials that go beyond what is visible on the blockchain. These internal records can fill evidential gaps that on-chain analysis alone cannot resolve, and future procedural guidance, whether through the development of case law or the Civil Procedure Rules, could clarify the types of material that may appropriately be sought in such applications.

The third recommendation is for the courts to continue to develop procedural flexibility. For example, in the case of *D'Aloia*, authorising service through NFT was a logical step because the defendants interacted exclusively through blockchain addresses.

Lastly, there is the structural aspect to consider. There are often disputes surrounding digital assets that involve technical concepts, such as hashing, wallet clustering, metadata, and exchange architecture, that would require a certain level of judicial expertise. As with construction or competition disputes, a specialist list or designated judicial panel can assist in developing consistent jurisprudence, improving speed and enabling judges to identify evidential deficiencies early.

2. <u>Adaptations for Practitioners</u>

Practitioners will also need to make appropriate adjustments. The first requirement is the need for parallel tracing workstreams. It is imperative to conduct both on-chain and off-chain investigations simultaneously. Waiting until blockchain analysis is completed before contacting exchanges may result in lost opportunities to preserve assets. Requesting temporary holds or flags via preservation notices can buy practitioners crucial time before obtaining formal relief.

Secondly, practitioners should incorporate evidence from issuers whenever possible. In stablecoin cases, the issuer's internal records are often the most authoritative source of information. The absence of proof from Tether Ltd in *D'Aloia* was a significant gap. By engaging issuers at an early stage, the tracing analysis can be corroborated, and the risk of evidential collapse reduced.

Furthermore, interim relief should be drafted to account for the realities of digital movement. Where assets pass through multiple hops, orders should capture each relevant wallet, not merely the final destination. Ideally, a practitioner should be able to present a coherent narrative that explains how each wallet contributes to the overall flow. In addition, applications directed at exchanges should anticipate that assets may already have been swept into pooled wallets and request the specific records necessary to establish token movements.

Fourthly, practitioners should adopt structured practices to preserve digital evidence. Given the scrutiny applied in *COPA v Wright*, metadata should be preserved, hash values recorded at the earliest possible stage, and all digital materials should be subject to a chain of custody. Using these techniques reduces the likelihood that evidence will be rejected or downweighted.

Lastly, although many disputes already involve cross-border elements in their recovery and enforcement, practitioners should adopt an even more international perspective in dealing with digital assets. As digital assets are inherently cross-border in nature, mirror injunctions, disclosure applications, and preservation measures will often require coordination across multiple jurisdictions.

Conclusion

While the enforcement of digital assets is based on familiar legal principles, and practitioners and judges should not be afraid to deal with these disputes, their practical application relies on both adapting judicial processes and professional practice to the realities of blockchain technology.

By clarifying evidential standards, directing disclosure, enhancing procedural flexibility, and enhancing technical expertise, the courts will be better equipped to resolve disputes involving digital assets. Consequently, practitioners will be better positioned to act rapidly in developing the case against the "choke point" entities and bringing it to court before assets can no longer be found if they initiate early action (by reaching out to exchanges to establish temporary holds, etc.), integrate tracing strategies, preserve digital evidence carefully, and coordinate internationally.

If these adaptations are embraced, enforcement against digital assets can evolve into a natural extension of traditional remedies, capable of meeting the speed, volatility and complexity of modern digital markets while remaining grounded in the enduring principles of English law.