International
Comparative
Legal Guides

Practical cross-border insights into litigation and dispute resolution work

Litigation & Dispute Resolution

2022

15th Edition

Contributing Editor:
Greg Lascelles
Covington & Burling LLP

CDR Commercial Dispute Resolution

ICLG.com

Expert Analysis Chapters

Q&A Chapters

Digital Edition Chapters

The English Courts' Approach to Disputes Involving Crypto-Assets


Greg Lascelles


Alan Kenny

Covington & Burling LLP

Introduction

In recent years, there has been a remarkable global increase in interest in crypto-assets[1] and related technologies from retail and professional investors, multinational companies, institutions, and governments. This is despite some perceived crypto-asset vulnerabilities, particularly relating to uncertain regulatory status, security and traceability weaknesses, price volatility, links to criminality, and environmental impact. Against this backdrop, it is not surprising that crypto-related disputes have started to find their way to the civil courts, and this trend is expected to increase in the coming years.

The English Courts have already shown real flexibility in reinterpreting caselaw and adapting procedural rules to make them suitable for the often unique demands of crypto-related disputes. Recent rulings have demonstrated an understanding that this is an area of increasing importance to the technology and financial services sectors, both of which are growth areas for the UK economy; and, further, that there is a need for market confidence, legal certainty and predictability in how the English Courts deal with crypto-related and other new technologies, if England and Wales is to remain an attractive forum for the resolution of disputes in this area.

This chapter discusses the most important points emerging from recent crypto-related rulings of the English Courts[2] and connected crypto-related initiatives, assessing their likely impact on the practical realities of litigating disputes in this area, including:

(i) the acceptance of crypto-assets as "property";
(ii) questions of jurisdiction and governing law for crypto-related disputes;
(iii) the types of crypto-related court orders that are obtainable;
(iv) procedural issues when applying for crypto-related court orders;
(v) causes of action available in crypto-related disputes; and
(vi) the Digital Dispute Resolution Rules (the "**DDR Rules**"): a new procedural framework utilising new technologies designed to facilitate the rapid resolution of crypto-related (and other digital) disputes via arbitration or expert determination.

Crypto-Assets as "Property"

In November 2019, the UK Jurisdiction Taskforce ("**UKJT**")[3] issued a non-binding legal statement that crypto-assets were property.[4] This was referred to and endorsed by the English Courts for the first time in January 2020,[5] building on earlier cases from 2018[6] and 2019[7] where crypto-assets had been treated as property without this status having been expressly determined. This approach has been followed in successive cases.[8]

This development is important because certain causes of action and interim orders can only be obtained in relation to property, for example, freezing orders.[9]

Jurisdiction and Governing Law

Complicated questions of jurisdiction and governing law can arise in crypto-related disputes for a variety of reasons, including because:

(i) parties transacting with crypto-assets may do so without designating the jurisdiction or governing law provisions to apply to any related disputes;
(ii) the identity of parties owning or dealing in crypto-assets may not be public;
(iii) crypto-assets are generally not located in one place but rather constituted on a distributed network or platform that can be spread out over multiple jurisdictions;
(iv) crypto-assets can pass between parties and different jurisdictions quickly and easily; and
(v) interim orders and final orders may need to be enforced in jurisdictions outside of England and Wales.

In December 2020, the English Courts decided that the jurisdiction and governing law applying to non-contractual crypto-related disputes is the law of the place where the crypto-assets are situated (the *lex situs*) and/or where the relevant damage and/or unjust enrichment occurred, depending on the nature of the claim being brought. Further, the English Courts decided that crypto-assets are situated in the place where the person or company who owns them has its place of residence or business.

Following this clarification, parties bringing crypto-related actions in England or Wales can be confident that the English Courts are likely to find jurisdiction to hear the actions and to apply English law to the proceedings, provided the applicants/claimants are domiciled in England or Wales, or can point to damage or actionable conduct that occurred in this jurisdiction. This clarification will also make it easier for parties to obtain permission to serve proceedings on parties located outside of the jurisdiction, as explained in Section 5 below.

Crypto-Related Court Orders

Orders obtainable

In crypto-related disputes, the English Courts have shown flexibility in issuing a wide variety of different orders in different circumstances, as further explained below. The starting point is that generally an order will only be granted where there is a serious issue to be tried in the underlying claim, the balance of

convenience is in favour of granting the order,[10] and it is just and convenient in the circumstances to do so. There are also specific tests that must be satisfied for specific types of order.

(a) Freezing orders/injunctions

These restrain parties from disposing of or dealing with their own assets (often up to a specified value) for a limited period, typically until judgment can be obtained or enforced. The English Courts are willing to order domestic freezing orders in respect of assets located within England and Wales and worldwide freezing orders in respect of assets outside of the jurisdiction, in both cases where these are ancillary to a substantive claim that is ongoing or will be brought. Various criteria must be satisfied, including proving a real risk that, without the order, the assets would be dissipated.[11]

In crypto-related disputes, freezing orders/injunctions have been ordered against, for example:

(i) a crypto-currency trading company and its directors where the applicant, an individual investor, had deposited significant quantities of crypto-currency with the company to test its trading platform, had become concerned with the company's operations and made enquiries, and then received no credible response;[12]

(ii) companies providing electronic "wallets" holding crypto-currency, and exchanges involved in related transactions, where the applicant, an insurance company, had identified specific wallets (via the assistance of specialist blockchain tracers[13]) as those to which its insured had paid a crypto-currency ransom to hackers who had installed malware on their IT systems;[14] and

(iii) unknown fraudsters, where they had obtained access to the electronic wallet of the applicant and sold the applicant's crypto-currency to anonymous third-party buyers at a significant undervalue, retaining these sale proceeds.[15]

The courts have refused to maintain freezing orders in relation to crypto-assets belonging to the defendant where damages have been deemed an adequate remedy for the underlying claim, and the defendant has been deemed to have sufficient assets within the jurisdiction (or a jurisdiction where enforcement would be unproblematic) to satisfy the claim. In such instances[16] a key consideration was the price volatility of the assets (Bitcoin), which meant that if the defendant had been prevented from selling the assets, they could have faced very significant losses. A secondary consideration was the claimant's admission that they would have difficulty in satisfying any cross-undertaking as to damages[17] if the respondent suffered loss as a result of being prevented from selling the crypto-assets.

(b) Proprietary orders/injunctions

These restrain a respondent from dealing with assets over which the applicant asserts title. These will often be available – and have been ordered – alongside or in *lieu* of freezing injunctions, in circumstances the same as – or similar to – those outlined in Section 4.A.(a) above. Proprietary injunctions are viewed by the courts as a less draconian remedy than the "nuclear" option of a freezing order, and therefore are more readily granted.

For example, in a case[18] where the applicant had responded to a phishing email and transferred 100 Bitcoin to the alleged fraudster's electronic wallet, who in turn transferred 80 Bitcoin to a third-party wallet, the court was willing to grant a proprietary injunction over the 80 Bitcoin, but not a freezing order. This was on the basis that the court accepted there was a serious issue to be tried based on a proprietary claim, but did not consider the facts showed a sufficiently real risk of dissipation of assets.

The courts are generally less willing to discharge proprietary injunctions than freezing orders, due to the fact that if the assets to which the applicant/claimant asserts title are dissipated, their claim becomes nugatory.

(c) Disclosure orders

These seek disclosure of information or documents and can be sought from a defendant or third parties.

In the case of disclosure sought from a defendant, this will normally be pursuant to the normal processes in CPR 31 and Practice Directions 31A and B.

In the case of disclosure sought from third parties, this can be pursued through the process in CPR 31.17, where: (i) the documents sought are likely to support the case of the claimant or adversely affect the case of one of the other parties to the proceedings; and (ii) disclosure is necessary in order to dispose fairly of the claim or to save costs.

However, it is more common in crypto-related disputes for third-party disclosure to be sought and granted pursuant to the courts' equitable jurisdiction, in the form of "Norwich Pharmacal Orders" ("**NPOs**"). These are available where information and/or documents are sought in order to: (i) identify a wrongdoer; (ii) enable an applicant to plead its case against a wrongdoer; (iii) trace assets; and/or (iv) bring proprietary claims. In crypto-related disputes they are most commonly sought against exchanges, where an applicant has identified a crypto-wallet involved in a fraud but needs the assistance of the exchange to identify the registered user.[19] Disclosure orders (and other orders, in appropriate circumstances) can also be sought against crypto-currency/token minters.[20] Such orders are likely to be most appropriate where the crypto-currency/token in question is being held in a private wallet (and therefore disclosure cannot be provided by an exchange) and the minters in question have retained relevant rights over the crypto-currency/token.[21]

There are numerous requirements for obtaining an NPO, including that: (i) the respondent is likely to have relevant documents or information; (ii) there is a good arguable case that there has been wrongdoing with which the respondent is involved; and (iii) the order is necessary in the interests of justice and is not sought for an improper purpose. It is not necessary that the applicant has a definite intention to commence proceedings against the alleged wrongdoer.

More rarely, a party may seek a "Bankers Trust Order" ("**BTO**") relating to a third party (normally a bank). These seek confidential information, such as correspondence and banking records, in narrower circumstances, typically where: (i) the applicant seeks to trace assets that belonged to them and of which there is strong evidence that they have been fraudulently deprived; and (ii) a delay may result in dissipation of the assets before an action for recovery comes to trial. BTOs have been granted in crypto-related disputes, for example, against exchanges to procure information to assist in identifying fraudsters who obtained access to an applicant's electronic wallet and sold their crypto-currency to anonymous third-party buyers at a significant undervalue.[22]

In practice, applicants will often seek NPOs, BTOs and other disclosure orders in respect of the same documents or information, at the same time, to maximise their prospects of an order being granted.[23]

(d) Search orders

These allow a claimant's representatives, without notice, to enter a defendant's residential or business premises to search for, copy, remove and/or detain information, materials, or documents (hard copy and electronic). In exceptional circumstances, a search order may be made against a third party.

As these are amongst the most draconian remedies at the courts' disposal, they are strictly regulated. They will only be granted where the applicant can show: (i) an extremely strong *prima facie* case; (ii) clear evidence that the respondent has in its possession incriminating documents or other material; (iii) a real possibility that the incriminating material might be destroyed before any application could be brought on notice (i.e. an application for a

less draconian remedy, such as a delivery-up or preservation of documents order); and (iv) that the claimant/applicant would suffer serious damage if the order is not granted.

We are not aware of any crypto-related cases to date where a search order has been sought; however, it is easy to foresee circumstances where this may be beneficial, for example, where misappropriated crypto-assets (or related private keys) are in "cold storage".[24]

Procedural issues

(a) Private hearings

The general rule is that a hearing is to be held in public unless the court decides that it must be held in private in order to satisfy one of the seven requirements of CPR 39.2(3). Those most likely to apply to cyber-related disputes are where: (i) publicity would defeat the object of the hearing; (ii) it involves confidential information (including information relating to personal financial matters) and publicity would damage that confidentiality; (iii) it is a hearing of an application without notice (e.g. almost all freezing and search order applications); and (iv) the court for any other reason considers a private hearing necessary to secure the proper administration of justice.

The English Courts have allowed several hearings in crypto-related disputes to be held in private, citing all of these requirements as satisfied. For example, in a claim brought by insurers against unknown hackers who had obtained crypto-currency from their insured by ransom,[25] the court ordered a private hearing because, *inter alia*, a public hearing could: (i) potentially tip off the unknown fraudsters to dissipate the crypto-currency (the court noting that it is quick and easy to do so with virtual currencies); and (ii) risk further revenge or copycat attacks on the insurer and/or insured (the court also protecting against this risk by allowing the insurer and insured to remain anonymised).

(b) Orders against "persons unknown"

Given the nature of crypto-related disputes, it will often not be possible at the outset for an applicant to identify the respondent against whom an order is sought. For example, in a case where fraudsters appropriated crypto-assets and sold them to third parties at an undervalue, the applicant sought a proprietary injunction, world-wide freezing order, and ancillary information disclosure against "*the individuals or companies who own or control the accounts into which the [crypto-assets] or the traceable proceeds thereof are to be found*". This category of persons would encompass not only the fraudsters who appropriated the crypto-assets, but also any recipients of the crypto-assets, whether knowing or unknowing and whether or not they received the assets at an undervalue. As such, the court required that the applicants differentiate between (i) the fraudsters, (ii) those who had received the assets other than at full price, and (iii) those who had received the assets at full price. The court was willing to grant the freezing, proprietary and disclosure orders against the fraudsters, but only the latter two orders against the other categories of persons, and only then subject to qualifications designed to restrict the scope of the proprietary relief available against unknowing (i.e. innocent) recipients.

This is consistent with the courts' general concern to minimise the potential for court orders to negatively impact innocent third parties, which requires orders generally to be drafted as narrowly as possible to give effect to their purpose. As such, to maximise the potential for orders against "persons unknown" to be granted, parties should:

(i) describe the characteristics of the "persons unknown" with sufficient certainty and with reference to the unlawful conduct in question, such that it is possible to identify who would fall inside and outside of scope;

(ii) only include people who have not been identified at the time the order is granted, but who are capable of being identified; and

(iii) seek permission for a method of service that can be shown to be reasonably expected to bring the proceedings to the attention of all the "persons unknown".

(c) Service relating to orders

Where an applicant applies for an order against a respondent, the applicant is required (unless the application is made without notice) to serve a copy of the application notice on the respondent. Similarly, they must serve a copy of any order granted on all parties subject to the order.

CPR 6 and Practice Direction 6A set out which methods and places of service are permitted, depending on the document – and location of the party – being served. In general, parties located outside of the jurisdiction should be served in accordance with the procedure set out in the 1965 Hague Convention[26] or any other applicable civil procedure convention or treaty. Some orders may not be served on parties outside of the jurisdiction.[27]

However, in crypto-related cases it will often be necessary to serve orders on parties very quickly and outside of the jurisdiction and, in the case of orders against persons unknown, potentially in an unknown jurisdiction. In such circumstances, where service by ordinary means would be impossible or take so long that it would defeat the purpose of the order, the courts have shown a willingness to allow for service by an alternative method and/or at an alternative place, for example, by email. Where permission to serve out is sought in such circumstances, it is advisable for applicants to produce evidence as to the delay that would likely result from having to effect service under the Hague Convention, or the reasons why such service is not possible.

(d) Practicalities of drafting crypto-related orders

Applicants should pay close attention to the drafting of crypto-related orders to ensure that they are effective, in practice, to achieve their ultimate objectives. They should provide as much specificity as possible. For example, the order should provide (as appropriate to its focus) any known information relating to relevant known: email accounts; usernames and passwords; drives and devices; internet histories; mobile applications; and cold-storage repositories.

This is particularly important in the case of freezing, search and disclosure orders, where the ultimate objective is to freeze or locate misappropriated crypto-assets, which will often only be possible by locating the private key(s) to the relevant crypto-wallet(s), which could be stored on any media. For example, in a recent Irish case,[28] the state seized digital wallets belonging to an incarcerated defendant understood to contain crypto-assets worth around £45 million, representing the proceeds of crime, but were unable to access the assets without the private keys (which it is understood were written down on pieces of paper stored in an aluminium fishing box that the defendant's landlord threw away whilst he was in custody).

Causes of Action for Crypto-Related Disputes

The specific cause(s) of action available to a claimant in a crypto-related dispute will depend on the specific facts and circumstances. However, given the English Courts' willingness to accept crypto-assets as property, it is to be expected that the full range of contractual, tortious and fraud-based claims are available.

To date, in interim hearings relating to crypto-assets (no crypto-related dispute having yet proceeded to trial), claimants have asserted – and the courts have been willing to accept for the purposes of granting interim remedies – that claims are possible:

(i) in restitution and/or on the basis of a constructive trust (for example, in a case where crypto-currency was paid to hackers as ransom and could be traced and identified[29]);
(ii) in deceit, unlawful means conspiracy, and for an equitable proprietary claim (for example, in a case where a party alleged it had been induced by fraudulent means to invest crypto-currency in a sham initial coin offering ("**ICO**"),[30] and the crypto-currency could be traced and identified); and
(iii) in unjust enrichment and in breach of confidence (for example, in a case where crypto-assets were stolen via the theft of a private key and then sold to alleged knowing third parties at an undervalue[31]).

Where a claimant is seeking to bring such a claim against a defendant located (or in the case of persons unknown, potentially located) outside of the jurisdiction, it will need to obtain permission from the court to do so, which requires the claimant to show that: (i) the claim gives rise to a serious issue to be tried on the merits; (ii) the claimant has a good and arguable case that the claim falls within one of the 21 procedural gateways identified in Practice Direction 6B (the "**PD 6B Gateways**"); and (iii) in all the circumstances, England and Wales is clearly and distinctly the appropriate forum in which to bring the claim (the *forum conveniens*).

Several of the PD 6B Gateways rely, ultimately, on the claim relating to assets located in the jurisdiction. As such, obtaining permission has been made easier by the English Courts' decision that crypto-assets are situated in the place where the person or company who owns them has its place of residence or business, as further explained in Section 3 above.

The Digital Dispute Resolution Rules

Separate to the developments in English caselaw discussed above, the English judiciary has also been involved in the development of an entirely new procedural framework, the DDR Rules, which is likely to play an increasing role in the future in the resolution of disputes in this area.

The DDR Rules are designed to facilitate – by arbitration or expert determination conducted under English law – the rapid resolution of digital disputes. They contain several novel features that are specifically tailored to such disputes and which are likely to be attractive to some parties dealing in crypto-assets. It is beyond the scope of this chapter to discuss these features in detail, but they include:

(i) a streamlined process designed to take far less time than litigation;
(ii) compatibility with new technologies, including allowing electronic or encoded incorporation of the DDR Rules directly within digital assets, and allowing for "automatic dispute resolution";[32]
(iii) access to arbitrators/experts with the specific expertise required for crypto-related disputes;
(iv) party anonymity; and
(v) enhanced default powers and enforcement mechanisms for tribunals, including relating to digital assets and potentially allowing for the implementation of decisions directly "on-chain".

Conclusion

The steps taken by the English Courts to date show that they are willing and able to respond consistently and flexibly to the new challenges presented by crypto-assets and connected emerging technologies. In particular, they emphasise a willingness (absent express provisions providing otherwise) to find jurisdiction to hear crypto-related disputes and apply English law to such disputes, where there is a nexus to England and Wales. Where jurisdiction is found, claimants are likely to be able to obtain permission to serve proceedings on parties outside of the jurisdiction and have recourse to a full range of causes of action and remedies. Further, the courts are willing to grant a wide variety of interim remedies, particularly where an applicant alleges that they have been the victim of fraud. In doing so, the courts are providing welcome assistance in establishing English law and jurisdiction as ideally suited to govern crypto-related contracts and disputes, as well as helping to provide a foundation for the responsible future utilisation of such technologies.

Finally, new alternatives are emerging to traditional dispute resolution options. These come in the form of both "automatic dispute resolution" options built into smart contracts, but also in the form of emerging decentralised arbitration protocols.[33] The latter are designed to allow disputes to be resolved entirely online, with all of their processes integrated on the blockchain, and often tailored specifically for crypto-related disputes. It will be interesting to see over time the extent to which these new alternatives find favour for crypto-related disputes over more traditional court and arbitration options.

Endnotes

1. The term "crypto-asset" is used to describe a wide variety of different types of assets existing within different systems, from notional payment tokens such as bitcoin to digital representations of real-world tangible objects, and as such is difficult to define. However, generally, a crypto-asset is an intangible digital asset that uses cryptographic authentication techniques for security, and is normally part of a decentralised system ruled by consensus and using distributed ledger/blockchain technology (i.e. where transactions relating to the crypto-assets are recorded on a ledger that is not centralised but rather maintained across several computers linked in a peer-to-peer network). A more comprehensive definition is provided in the UKJT's "*Legal statement on cryptoassets and smart contracts*", accessible here: https://35z8e83m1ih83drye280o9d1-wpengine.netdna-ssl.com/wp-content/uploads/2019/11/6.6056_JO_Cryptocurrencies_Statement_FINAL_WEB_111119-1.pdf.
2. All the decisions referred to in this chapter relate to interim applications and, therefore, are not technically definitive judicial authority (which only arises from final judgments); however, they will be persuasive in future cases and demonstrate a clear direction of travel.
3. The UKJT (one of the six taskforces of the LawTech Delivery Panel) is a group of senior individuals from the judiciary, commercial legal sector, financial services regulation, and business, supported by the UK Government, with the objective to "*demonstrate that English law and the jurisdiction of England and Wales together provide a state-of-the-art foundation for the development of distributed ledger technology, smart contracts and associated technologies*", including crypto-assets.
4. The statement also expressed the view that smart contracts were valid contracts under English law.
5. *AA v Persons Unknown* [2019] EWHC 3556 (Comm).
6. *Vorotyntseva v Money-4 Ltd (t/a Nebeus.com)* [2018] EWHC 2596 (Ch).
7. *Robertson v Persons Unknown*, unreported, CL-2019-000444.
8. For example, *Toma & True v Murray* [2020] EWHC 2295 (Ch), and *ION Science Ltd v Persons Unknown and others* (2020), unreported (Comm).
9. Crypto-assets have also been found to constitute property/realisable property for the purposes of ss 74 and 83 of the Proceeds of Crime Act 2002 ("**POCA**"). Criminal inves-

tigators and prosecutors that suspect or prove that crypto-assets are the proceeds of crime have access to a range of potential orders under POCA and/or other applicable legislation, such as the Criminal Finances Act 2017, the details of which are beyond the scope of this chapter.

10. I.e., the court will consider the likely inconvenience or damage that would be suffered by the applicant if the injunction is not granted as against the likely inconvenience or cost to the respondent if it is granted. Where the applicant can show a *prima facie* case of wrongdoing, this will often go a long way towards tipping the balance in favour of granting the order.
11. I.e., that the respondent will move, dispose of, or otherwise deal with their assets, other than in the ordinary course of business, that would serve to make it more difficult for an existing or potential future judgment or award to be satisfied/enforced. Various other orders may be made in support of freezing orders, such as an order pursuant to CPR 25.1(g) directing a party to provide information about relevant property or assets which are or may be the subject of an application for a freezing order.
12. *Vorotyntseva v Money-4 Ltd.*
13. Blockchain tracing companies specialise in analysing transactions on blockchains, for example, to try to track the movement – and ultimate location – of crypto-assets that have been misappropriated.
14. *AA v Persons Unknown.*
15. *Fetch.ai Ltd v Persons Unknown* [2021] EWHC 2254.
16. *Toma & True v Murray.*
17. An undertaking provided by an applicant to the court to compensate the respondent if it is subsequently determined that the applicant was not entitled to the relief granted. In effect, this is the "price" paid by the applicant for the relief.
18. *Robertson v Persons Unknown.*
19. In many jurisdictions where exchanges are regulated, providers are required to retain "know your customer" information for anti-money laundering – or other – purposes, which can prove invaluable to a defrauded claimant.
20. See, for example, *Lubin Betancourt Reyes and Custodial Management Solutions Limited v Persons Unknown and others* [2021] EWHC 1938 (Comm).
21. The design and protocol of certain crypto-currencies/tokens allow minters to retain certain rights over them, including to potentially, *inter alia*: refuse registrations; block transactions; track and report circulation; suspend or terminate the administration of services related to the currency/token or connected addresses or wallets; and revoke currency/tokens.
22. *Fetch.ai Ltd v Persons Unknown.*
23. Albeit this approach is not without risk, as it is likely to increase the applicant's costs liability to the respondent in the event that no order is granted.
24. "Cold storage" is a term used to describe the process of storing crypto-assets in an offline "cold" wallet, as opposed to a "hot wallet" connected to the internet. A private key providing access to a cold wallet is typically made up of a set of alphanumerical characters and can therefore be stored on any number of devices, such as a USB, CD hard drive, or piece of paper.
25. *AA v Persons Unknown.*
26. The Hague Convention on the Service Abroad of Judicial and Extrajudicial Documents in Civil or Commercial Matters.
27. Generally, the courts are not willing to grant permission for NPOs to be served on parties outside of the jurisdiction, although they have exercised their discretion to grant permission in a handful of cases, including in relation to crypto-assets – see *Lubin Betancourt Reyes and Custodial Management Solutions Limited v Persons Unknown and others.* The courts seem recently to have confirmed, against a backdrop of conflicting authorities, that they are willing to grant permission for BTOs to be served on parties outside of the jurisdiction, in appropriate circumstances, including in relation to crypto-assets – see *Fetch.ai Ltd v Persons Unknown.*
28. *DPP v Collins*, unreported (February 2020).
29. *AA v Persons Unknown.*
30. *ION Science Ltd v Persons Unknown.* An ICO is, in essence, a means of raising funding for a new crypto-currency venture, and is similar in some respects to an initial public offering (or "**IPO**") of shares in a newly public company.
31. *Fetch.ai Ltd v Persons Unknown.*
32. Meaning a process associated with a digital asset that is intended to resolve a dispute by the automatic selection of a person, panel or AI agent whose vote or decision is implemented directly within the digital asset system (including by operating, modifying, cancelling, creating or transferring digital assets).
33. For example, Kleros, Jur and Aragon Network.

Greg Lascelles advises clients in high-stakes matters with significant financial or reputational risk. His broad-based practice covers complex international commercial litigation, arbitration, regulatory investigations and Parliament Select Committee hearings. He acts for major corporates, financial institutions, entrepreneurs and individuals, and his cases involve disputes relating to interpretation, M&A disputes, bonus and remuneration, Companies Act matters, shareholder disputes, data litigation, securities litigation and disputes involving serious issues of fraud. He has been involved in ground-breaking High Court and FCA disputes relating to market abuse and collective selling, as well as in the Supreme Court on the interpretation of standard contractual clauses. Greg's regulatory matters (including at the FCA, FRC, SFO and Insolvency Service) relate to market abuse and financial statement reporting. As well as regular advice to clients on contract drafting and risk avoidance, he has recently been advising on developments in FDI and national security legislation.

Covington & Burling LLP
22 Bishopsgate
London EC2N 4BQ
United Kingdom

Tel: +44 207 067 2000
Email: glascelles@cov.com
URL: www.cov.com

Alan Kenny focuses on high-value, complex, multiparty and multijurisdictional matters, advising companies, banks, institutions, and high-net-worth individuals on all stages of dispute avoidance and resolution. He has experience representing clients in: mediation; commercial litigation (before the English High Court and Court of Appeal); and international and trade association arbitration (both *ad hoc* and under a variety of rules). He acts for clients in a broad range of industries with particular experience in financial services, commodities, shipping, media, and technology.

Covington & Burling LLP
22 Bishopsgate
London EC2N 4BQ
United Kingdom

Tel: +44 207 067 2000
Email: akenny@cov.com
URL: www.cov.com

ICLG.com

Current titles in the ICLG series

Alternative Investment Funds
Anti-Money Laundering
Aviation Finance & Leasing
Aviation Law
Business Crime
Cartels & Leniency
Class & Group Actions
Competition Litigation
Construction & Engineering Law
Consumer Protection
Copyright
Corporate Governance
Corporate Immigration
Corporate Investigations
Corporate Tax
Cybersecurity
Data Protection
Derivatives
Designs
Digital Business
Digital Health
Drug & Medical Device Litigation
Employment & Labour Law
Enforcement of Foreign Judgments
Environment & Climate Change Law
Environmental, Social & Governance Law
Family Law
Fintech
Foreign Direct Investment Regimes
Franchise
Gambling
Insurance & Reinsurance
International Arbitration
Investor-State Arbitration
Lending & Secured Finance
Litigation & Dispute Resolution
Merger Control
Mergers & Acquisitions
Mining Law
Oil & Gas Regulation
Patents
Pharmaceutical Advertising
Private Client
Private Equity
Product Liability
Project Finance
Public Investment Funds
Public Procurement
Real Estate
Renewable Energy
Restructuring & Insolvency
Sanctions
Securitisation
Shipping Law
Technology Sourcing
Telecoms, Media & Internet
Trade Marks
Vertical Agreements and Dominant Firms

The International Comparative Legal Guides are published by: global legal group