ALLEN & OVERY

Solving the Crypto-Crossword

UK Developments in the Legal and Regulatory Treatment of Cryptoassets

Cryptoassets? What are they?

Over 11 years after Satoshi Nakamoto published his white paper "*Bitcoin: A Peer-to Peer Electronic Cash System*", regulators, judges, central banks, academics, crypto-enthusiasts and many others are still furiously debating this question. Indeed, you might think of 'crypto' as a pun: both advertently referring to the use of cryptography, and inadvertently referring to the cryptic nature of these assets which have proved notoriously difficult to classify. Throw in associated technologies and concepts such as distributed ledger technology (**DLT**), blockchain (a type of DLT) and smart contracts, and the world of crypto can be pretty difficult for the lay person to get their head around. This may be one reason that, although the era of cryptoassets and related technologies has long been predicted, it is yet to go fully mainstream.

So are we getting any closer to solving this crypto-crossword? Well, it is fair to say that we don't have all the answers yet but a few clues at least started to emerge in 2019. In particular, the publication of regulatory and other guidance is a start in laying down the legal and regulatory foundations on which the market confidence, necessary for wider take-up of cryptoassets, DLT and smart contracts, can be built. Most notable among these were:

- the Financial Conduct Authority's (**FCA**) Final Guidance on Cryptoassets (PS19/22); and
- the UK Jurisdiction Taskforce's (**UKJT**) Legal Statement on Cryptoassets and Smart Contracts (the **Legal Statement**).

This article summarises, from a UK perspective, the key points coming out of those developments and highlights some of the areas where greater clarity would be useful.

The Common Law Framework for Cryptoassets

In May 2019, the UK Jurisdiction Taskforce, which consists of certain members of the judiciary and other legal practitioners, began a consultation process ahead of the preparation of a legal statement on the status of cryptoassets and smart contracts under English private law. The purpose of the Legal Statement was to address the lack of certainty regarding the legal status of cryptoassets and smart contracts, with the ultimate aim being to ensure that English law and the jurisdiction of England and Wales are "*well positioned to provide the legal foundation for the development of these technologies*".[1]

Following input from various stakeholders, including A&O, the UKJT published the Legal Statement in November 2019. The Legal Statement does not have the force of law but is intended to provide "*market confidence, legal certainty and predictability*"[2] in respect of novel questions raised by cryptoassets. These include the proprietary status of cryptoassets, whether security can be granted over them, insolvency treatment, transferability, whether they constitute 'goods' under the relevant legislation, and the status of a distributed ledger as a register. Our summary of the key points from the Legal Statement can be found here.

What is a cryptoasset?

The UKJT noted that, owing to the variety of cryptoassets and the fast development of the technology, it would not be useful to attempt a precise definition of cryptoassets.

Nevertheless, the Legal Statement sets out a high level description of cryptoassets, as follows:

- Cryptoassets are represented digitally within a system.
- That system uses cryptographic techniques to enable a record/ledger of assets and dealings in those recorded assets. For example, the two data parameters which represent the cryptoasset are the public key and the private key. The public key contains information about the asset (e.g. ownership). The private key, which should only be known by its holder, permits the holder to deal with the asset. However, the Legal Statement is keen to stress that these data parameters "*should not be seen as constituting the cryptoasset but rather as being, respectively, the record of it and the key to dealing in it.*"[3]
- The system is an application of DLT. Dealings in assets are broadcast to a network of participants and, once confirmed as valid, added to a digital ledger. Rules governing dealings are established by the informal consensus of participants.
- The principal novel and characteristic features of cryptoassets are therefore intangibility, cryptographic authentication, use of DLT, decentralisation, and rule by consensus.

Are cryptoassets capable of being property?

The Legal Statement adopts a two-step approach in answering this question. First, it analyses whether cryptoassets, taking into account their novel and distinctive features, meet the requirements to qualify as property. Secondly, it considers whether cryptoassets might be disqualified from being property on the basis that they constitute information.

As a matter of English law, the necessary characteristics of property are: definability and identifiability, certainty, assignability, permanence and stability, exclusivity, and control.[4] [5] The Legal Statement concludes that the novel features of cryptoassets do not prevent them from being property. In fact, some of the novel features of cryptoassets actually enable them to meet the requirements of property. For example, the public key, which indicates, among other things, the ownership of the cryptoasset, helps to satisfy the requirement for definability and certainty.

1 UKJT Consultation paper, *The status of cryptoassets, DLT and smart contracts under English private law*, May 2019, p. 4
2 Foreword to the Legal Statement by Sir Geoffrey Vos, Chancellor of the High Court (p. 3)
3 Legal Statement, paragraph 60
4 *National Provincial Bank v Ainsworth* [1965] AC 1175
5 *Fairstar Heavy Transport NV v Adkins* [2013] EWCA Civ 886

In relation to the second step there was an argument that, since information has not historically been treated as property under English law, cryptoassets might be disqualified from being property. However, the UKJT did not consider that this argument held up on analysis. In particular, the principal objection to information being property is that it can easily be duplicated. Once it has been duplicated and disseminated, multiple people can use the information simultaneously without any discernable loss of utility, making it difficult to exercise practical control over information or to determine who the owner is at any one time. By contrast, a cryptoasset by its very nature is exclusive in that only the owner of the corresponding private key can effect a transfer of the asset, and the process of authentication in relation to such transfers means that duplication and double spending is impossible.

The Legal Statement concludes that cryptoassets are not disqualified from being property on the ground that they constitute information. This conclusion is consistent with two High Court decisions[6], issued earlier in 2019, that treated crypto-currencies as property for the purposes of an asset preservation order and a freezing order respectively. More recently, the Legal Statement's analysis of the proprietary status of cryptoassets received High Court endorsement in *AA v Persons Unknown* [2019] EWHC 3556 (Comm), which concerned an application for an interim proprietary injunction by a Canadian insurance company that paid a ransom in bitcoin after it had been hacked. While these are all interlocutory decisions, they are revealing of an apparent developing consensus that cryptoassets are capable of being property.

A new category of intangible property?

Traditionally, English law has distinguished between two types of property: choses in possession and choses in action. This categorisation matters for two reasons in particular. First, there is authority[7] (albeit in an *obiter dictum*[8]) that English law only recognises as property things which fall in either of the two categories. Secondly, depending on the category an asset falls into, certain types of security may or may not be available in relation to that asset.

The Legal Statement concludes that cryptoassets are not choses in possession because they cannot be physically possessed.

In relation to choses in action the position is muddied by the fact that it has two possible meanings; (i) a wide meaning – any asset that is not a chose in possession: or (ii) a narrow interpretation – a right that can be claimed by action. Many cryptoassets (such as exchange tokens like bitcoin) will not fall within the latter, narrower interpretation of choses in action, although they could logically fall within the former. Instead of characterising cryptoassets as choses in action in the wider sense, which would be "*neither necessary nor useful*"[9], the Legal Statement suggests that they be analysed as a novel category of intangible property as had been found in previous cases concerning EU carbon emission allowances[10] and milk quotas[11].

Analysis of transfer – creation of a new cryptoasset?

One aspect of the Legal Statement which might prove controversial is the analysis on how an asset is transferred.

The Legal Statement analyses the transfer of a cryptoasset as involving the creation of a new asset in the hands of the transferee rather than the transfer of the same asset: "*the transferor typically brings into existence a new cryptoasset, with a new pair of data parameters: a new or modified public parameter and a new private key*".[12] The original cryptoasset remains in the network, under the control of the transferor, but becomes inert (i.e. no one will accept it because the ledger shows that it has been spent) after the creation of the new asset.

---

6 *Robertson v Persons Unknown, unreported*, CL-2019-000444 and *Elena Vorotyntseva v Money-4 Limited t/a Nebeus.Com, Sergey Romanovskiy, Konstantin Zaripov* [2018] EWHC 2596 (Ch)

7 *Colonial Bank v Whinney* (1885) 30 Ch D 261 (CA), 285

8 I.e. a comment "in passing" in a judgment that gives helpful guidance as to the likely legal position but is not binding as legal precedent because it is not an essential part of the decision in the case in question.

9 Legal Statement, paragraph 86(a)

10 *Armstrong v Winnington* [2012] EWHC 10, [2013] Ch 156

11 *Dairy Swift v Dairywise Farms Ltd* [2000] 1 WLR 1177

12 Legal Statement, paragraph 45

An analogy is drawn with a bank payment where funds are not actually transferred but rather one chose in action (in the form of a debt owed by the transferor's bank to the transferor) is cancelled and another corresponding chose in action is created (in the form of a new debt owed by the recipient's bank to the recipient). However, it is not entirely convincing, not least because (as the Legal Statement recognises) the premise of many cryptoassets is that they do not bestow a claim against anyone but merely record an asset recognised by the relevant network.

Further, this analysis sits rather uneasily with the conclusion elsewhere in the Legal Statement that the data parameters (i.e. the public and private keys) "*represent*" the cryptoasset but are not the cryptoasset itself.[13] If they are not themselves the cryptoasset, then what is being destroyed/made inert and what is being created? This point is explored further below. There may also be tax implications which flow from this "destruction-creation" analysis.[14]

It is therefore possible that an English court might take a different view as to the nature of cryptoassets and how they might be transferred. One possible alternative analysis is set out below.

Alternative transfer analysis – Could bitcoin be imaginary?

In a lecture given to the Insolvency Lawyers' Association on 17 October 2019[15], Mr Justice Zacaroli also came down firmly in favour of cryptoassets being property. However, in doing so he drew a clear distinction between a bitcoin itself and the public and the private key that represent/record the bitcoin: "*the fact that the private key is necessary in order to transact bitcoin does not make it the thing that is the bitcoin*". As noted above, this distinction – i.e. that information about the asset (i.e. the public/private key) is distinct from the asset itself (i.e. the bitcoin) – appears to be endorsed by the Legal Statement itself. However, the conclusion drawn is different.

Mr Justice Zacaroli observes that in his view "*bitcoin is an entirely imaginary thing*" and it is that imaginary thing "*that is the subject matter of the transfer*". On this logic, a change in the information about the asset upon transfer does not necessarily entail a creation of a new asset. Rather, the new block on the blockchain records the fact that the cryptoasset (i.e. the same cryptoasset) has moved. By contrast (and as noted above), although the Legal Statement recognises that the asset is only "*represented*"[16] by the public/private key data parameters (rather than being embodied by those parameters), it appears to shy away from this conclusion in its analysis about transfer.

Although the suggestion that a bitcoin (for instance) is imaginary might instinctively conjure up worrying thoughts of the "Emperor's New Clothes", in fact it is similar to the position with fiat currency. Many fiat currencies are no longer backed by a right to anything per se, but rather have value because (i) participants in that currency system, and the world at large, agree they have value and (ii) that value is contained in the unique ability of the owner of the asset to effect a transfer of value to a third party recipient within the accepted rules of the applicable system.[17]

Consider, for instance, the simple case of a pound coin. It has little or no intrinsic value itself but all accept that I will transfer one pound's worth of value if I give my pound coin to a shopkeeper. So too with crypto-currencies. Once the private key holder effects a transfer of one bitcoin to a third party by recording on the blockchain a new entry against the recipient's public key (and following the process of authentication), the transferor is indisputably one bitcoin down and the recipient transferee is undoubtedly one bitcoin up.

There is therefore no conceptual problem in some[18] cryptoassets being imaginary (in the sense that attributable value rests on consensus building among a network of participants and the broader economy). The financial system is based on the concept of trust and belief that although the tokens (i.e. notes and coins) that represent fiat currency have no intrinsic

13 Legal Statement, paragraph 60

14 See for instance "Disposals of cryptoassets, tax & the UKJT Legal Statement" by Leigh Sagar: https://www.scl.org/articles/10801-disposals-of-cryptoassets-tax-the-ukjt-legal-statement

15 Contained in South Square Digest (November 2019), pp. 53-59

16 Legal Statement, paragraph 60

17 Of course one important additional feature of fiat currencies, not possessed by crypto-currencies, is that they are backed by legislation confirming that they are legal tender. See for instance in the UK – the Coinage Act 1971 in respect of coins and the Currency and Bank Notes Act 1954 in respect of banknotes.

18 As noted above, there are many different types of cryptoasset and so it is unlikely that the analysis will be the same in every case.

value, they nevertheless represent the ability to transfer value. If it can work for fiat currencies, it is possible that it may work for crypto-currencies also.

The Legal Statement does not go that far (although it does accept that the commercial value of a cryptoasset is in the holder's unique ability to effect a transfer). However, it remains to be seen whether the Legal Statement's "destruction-creation" transfer analysis will stand the test of time, including when applied to existing legislation and regulation.

Other outstanding questions and uncertainties

The Legal Statement does not purport to provide final answers to the long list of potential questions raised in relation to cryptoassets. For example:

- Ownership: the determination and vesting of ownership of cryptoassets remains a grey area. The starting point would be to look for the person who has acquired knowledge and control of the private key. However, this may not always lead to a clear answer as more than one person might acquire knowledge/control of the private key.
- Governing law: another open question is the determination of the law governing proprietary aspects of dealings in cryptoassets. Traditionally, it has been the location of the asset that determines the governing law. The decentralised nature of cryptoassets presents a challenge to the traditional approach as participants in the distributed ledger can be located across jurisdictions. The Legal Statement makes various suggestions as to potentially relevant factors and alternative rules to determine the governing law but ultimately concludes that legislative intervention and international cooperation will be required to address this uncertainty.

Smart Contracts

The Legal Statement also addresses the English law status of smart contracts.

Distinctive features of smart contracts

As the Legal Statement notes, it is difficult to give a precise definition of smart contracts. However, their distinctive feature is that they are performed, at least in part, "*automatically and without the need for, and in some cases without the possibility of, human intervention*".[19]

This automation, both in terms of entering into contracts and performance under contracts, is achieved through computer code. That code can form part of the contract (i.e. provisions are written in code) or, alternatively, software can simply be an implementing mechanism for a natural language contract.[20]

Another key feature identified by the statement is that smart contracts are often (but not always) embedded in networked systems that execute and enforce performance of legal obligations using the same techniques (cryptographic authentication, distributed ledgers, decentralisation, consensus) as cryptoassets.

How will English law be applied to smart contracts?

Encouragingly, if not unexpectedly, the Legal Statement concludes that the ordinary rules of contract law apply to smart contracts and smart contracts are capable of satisfying the English law requirements for formation of a contract. It notes, however, that evidence extrinsic to the smart contract may sometimes need to be considered in determining whether an agreement has been reached and whether the parties intended to create legal relations, for instance where a smart contract is written entirely in computer code.

In terms of contractual interpretation, the ordinary rules will apply to smart contracts, including those that are written wholly or partly in computer code. In most cases, the code will be clear such that ambiguity will not arise as to its meaning. In cases when the code is unclear, then the judge will look at the contract as a whole, and admissible extrinsic

[19] Legal Statement, paragraph 135
[20] *Ibid.*

evidence, in determining what the parties objectively intended the contract to mean. This may require expert evidence as to the meaning of the code.

Other interesting takeaways from the Legal Statement include:

- A smart contract between anonymous or pseudonymous parties will still be a valid contract under English law.
- Statutory signature requirements are highly likely to be capable of being met by using a private key.
- Statutory 'in writing' requirements will be met in the case of source code (i.e. code that is written using a human-readable programming language). The treatment of object code (i.e. the output after software processes source code in order to create an executable program) is more uncertain and it will be necessary to determine the extent to which it is readable.

Some outstanding questions and uncertainties

The key message of the Legal Statement in relation to smart contracts is that "*English law is well able to deal with technological developments and it has an impressive track record of doing so*".[21] This may well be the case, but uncertainties regarding the legal treatment of smart contracts will remain until disputes involving smart contracts come before the courts. Further, just because English Law is capable of dealing with and analysing contracts drafted wholly or partly in code, does not automatically mean that is necessarily a good idea for parties to use computer code to govern their contractual obligations.

One cautionary tale comes from the case of *B2C2 Ltd v Quoine Pte Ltd* [2019] SGHC(I) 03, which came before the Singapore International Commercial Court in 2019. The case has been prominent because it offers support for the characterisation of crypto-currencies as property and the Legal Statement specifically refers to it for this reason. Another interesting aspect of the case is its consideration of the application of traditional common law principles – in this case the doctrine of unilateral mistake – in the context of a smart contract[22] entered into by two computer programs.

The doctrine of unilateral mistake under English law renders a contract void where one party has made a mistake as to a sufficiently important or fundamental term when entering into it and the other party knew of that mistake at the time of entering into the contract but remained silent. There are subtle differences between the Singaporean law doctrine and the English law doctrine, but these are not relevant for present purposes.

In *B2C2 v Quoine*, the claimant used software to trade on a crypto-currency platform. The defendant owned the platform and used its own software to facilitate trades on the platform. A defect in the defendant's software resulted in trades being entered into between the claimant and other parties (the **Smart Contracts**) at 250 times the market exchange rate for bitcoin and Ethereum in favour of the claimant. The defendant, as operator of the platform, reversed the trades the following day and the claimant sued it for breach of the platform contract between them.

The key question for the court was whose knowledge was relevant for the purposes of determining whether the unilateral mistake operated to render the Smart Contracts void. The relevant mistake was the mistaken belief of the other parties under the Smart Contracts that trades would never be transacted on the platform that deviated so substantially from actual market prices. In relation to knowledge of this mistake, as the contracts had been entered into by software, there was no human involvement and therefore no human knowledge at the time of entering into the Smart Contracts. The computer programs did not rely on artificial intelligence as they only did what they had been programmed to do. Therefore, the 'knowledge of the programs', to the extent this is possible to determine, was irrelevant in this case.

The court held that the knowledge and intention of the programmer of the claimant's software should be considered at the time the program was written. While it was relevant that the programmer had included values which were 250 times off market value when programming the software, these values were inserted to protect the claimant's position rather than to take advantage of other parties trading on the defendant's platform. Therefore, the court held that the

[21] Legal Statement, paragraph 20
[22] Although not one stored on a distributed ledger.

programmer did not have knowledge of the other parties' mistaken belief and as such the Smart Contracts were not void for unilateral mistake.

B2C2 v Quoine shows that while ordinary contractual principles will apply to smart contracts, the novel features of such contracts (such as the role of software or entities such as programmers) raise some challenging questions and will therefore require further refinement of these principles. For example, if *B2C2 v Quoine* had involved an ordinary contract concluded by humans which had been 250 times off market, that contract would probably have been rendered void. Is it really desirable that the Smart Contracts with the same excessive terms (the only difference being that they were concluded by software) were upheld?

Implications: are smart contracts the smart option?

This apparently perverse outcome not only suggests that traditional contractual principles may need some refinement in the context of computer-made contracts, and smart contracts more widely, it also should sound a note of caution against rushing headlong into a widespread adoption of contracts where key contractual principles are governed by computer code. The job of a good contract lawyer is to draft easily understandable, contractual documents that are unambiguous in their terms but contain enough flexibility to cater as far as possible for unforeseen issues that might crop up in the parties' relationship. The job of the court in contractual disputes is to give effect to the parties' bargain by discerning the objective intention of the parties from the words used set against the relevant factual background at the time the agreement was made. Both of these tasks are likely to be much more challenging if parties move significantly away from ordinary language contracts in favour of contracts written in computer code, with attendant increases in commercial risks for contracting parties.

In particular, given the scope for disputes to arise over plain language contracts drafted by highly skilled lawyers, the introduction of computer code is likely to increase these risks exponentially. For instance, even "human readable" computer code is difficult for the lay person to understand. This is likely to make it challenging not only for a court to find the objective intention of the parties (indeed, the code would likely need to be deciphered by experts before it could be interpreted by the presiding judge) but also for the parties to have had a meeting of minds in the first place. Another practical difficulty is that computer code is also often full of gaps, bugs and glitches, which can lead to outcomes that may sometimes be upheld in the courts even where they are commercially perverse (as we saw in the *B2C2* case).

This is not to say that, in certain contexts, there cannot be compelling reasons why the benefits of smart contracts (such as the time and cost efficiencies from automation) justify their use. Similarly, it may be that incremental improvements in coding and/or developments in the law make the adoption of smart contracts more viable. Indeed, there is much excellent work already underway from industry bodies, such as ISDA, who have been looking into the feasibility and utility of using computer code to automate certain (but by no means all) elements of financial contracts, with a view to producing market standard documentation for "smart derivatives".[23]

However, it is likely that, for the moment at least, smart contracts may not be the smart option for most parties most of the time[24]. Even where automation and/or efficiency are being prioritised, it will often make sense to agree the legally binding terms in ordinary language contracts, even if the way that they are implemented is via automated systems that operationally rely on computer code to execute the steps (e.g. payments) required under the contracts. Moreover, prudent parties seeking to use computers to automate the fulfilment of contractual obligations may wish to state specifically in their contracts that, in the event of a conflict, the ordinary language terms will prevail. They may also seek to allocate expressly the risks that may arise from computer malfunction or other related glitches.

The *B2C2* case also hints at a wider potential problem that may result as technology develops further. In *B2C2* the computers were broadly executing a strategy designed and programmed by a human. The level of automation in this case is in many ways nothing new. However, with the advent of artificial intelligence/machine learning we may reach a stage where contracts are not only automatically executed by computers, but the strategy behind them is also going to be

[23] https://www.isda.org/2019/10/16/isda-smart-contracts/
[24] In the sense of smart contracts where binding legal obligations are written in code.

computer generated. In *B2C2*, the judge considered that the relevant state of mind was that of the programmer at the time the computer program was coded. How far will that be still be applicable as the technology gets ever more sophisticated and the detachment between the actions of humans and the formation of contracts gets ever wider? It may be that new legal theory and appropriate laws will need to be developed to cope with this brave new world.

The Regulatory Framework for Cryptoassets

While the primary legal issue has been the status of cryptoassets as property, the primary question in the regulatory sphere has been whether cryptoassets fall within established regulatory categories such as specified investments, including e-money. This is particularly important because whether or not a particular cryptoasset falls within the FCA's regulatory perimeter ("*the boundary that separates regulated and unregulated financial services activities*"[25]) will determine the extent to which issuers of, and dealers in, such assets, and market participants more widely, will need to comply with the FCA's regulatory requirements.

The legal and regulatory frameworks are distinct but the approach taken in relation to one framework may well influence the other. For example, the fact that a particular cryptoasset is treated as e-money might be taken into account by a court when determining whether that cryptoasset meets the legal criteria of money.

UK statutes and regulations that might apply to cryptoassets include, for example:

- The Financial Services and Markets Act 2000 (**FSMA**)
  - The general prohibition at section 19 states that only authorised or exempt persons may carry out regulated activities in the United Kingdom.
  - 'Regulated activities' are defined in section 22 and include the carrying out of a specified activity by way of business in relation to a specified investment.
  - The full list of specified investments is contained in Part III of The Financial Services and Markets Act 2000 (Regulated Activities) Order 2001 (**RAO**).
- The Electronic Money Regulations 2011 (**EMRs**)
  - Regulation 63 contains a prohibition on issuing e-money (or purporting to do so) in the UK without the correct authorisation(s), unless an exemption applies.
  - E-money is defined in regulation 2 (Interpretation) as "electronically (including magnetically) stored monetary value as represented by a claim on the electronic money issuer which (a) is issued on receipt of funds for the purpose of making payment transactions; (b) is accepted by a person other than the electronic money issuer; and (c) is not excluded by regulation 3".
- The Payment Services Regulations 2017 (**PSRs**)
  - Regulation 138 contains a prohibition on providing payment services (or purporting to do so) in the UK unless appropriately authorised or exempt.
  - There is a range of payment services listed in schedule 1 to the PSRs. It is conceivable, depending on the nature of the cryptoasset and the system within which it circulates, that certain participants in that system could be deemed to be performing payment services.
- The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 as amended by the Money Laundering and Terrorist Financing (Amendment) Regulations 2019 (the **MLRs**).

Against this background, the UK Cryptoasset Taskforce (which consists of HM Treasury, the FCA and the Bank of England) published its final report in October 2018, which set out the UK's policy and regulatory approach to

[25] Paragraph 2 of the Perimeter Guidance at Appendix 1 to PS19/22

cryptoassets and DLT and included, among other things, a commitment to provide clarity on the regulatory perimeter in respect of cryptoassets.

As a response to that commitment, the FCA released its Guidance on Cryptoassets Consultation Paper (CP 19/3) in January 2019 that set out its proposed position on the regulation of cryptoassets.

Following feedback, in July 2019, the FCA released PS19/22, which contained its Final Guidance on Cryptoassets. The focus of the Final Guidance is on FSMA and the EMRs. In outlining the interaction between cryptoassets and the regulation, the Final Guidance (which refers to cryptoassets as tokens) draws a distinction between unregulated tokens and regulated tokens, as follows:

Unregulated tokens

Unregulated tokens "*do not provide rights or obligations akin to specified investments*".[26] These include "exchange tokens" and "utility tokens". Exchange tokens (e.g. a crypto-currency such as bitcoin) are those tokens that are intended and designed to be used as a means of exchange. Utility tokens are similar to pre-payment vouchers and provide holders with access to a service or product (e.g. a token that grants the holder early access to a new product to be released by a company). According to the Final Guidance, exchange and utility tokens usually fall outside the regulatory perimeter. However, it is important to note that an FCA authorised firm dealing with unregulated cryptoassets might still need to comply with other FCA rules such as the Principles for Business. Given the nascent nature of unregulated tokens and the untested and developing regulatory landscape, consideration should be given to using a separate and unregulated entity to issue unregulated tokens, so as to achieve effective segregation from any regulated business undertaken by the same group of companies. In this context, parties should also be aware that HM Treasury is currently giving active consideration as to whether an extension to the regulatory perimeter is appropriate to cover certain cryptoassets that are currently unregulated.

Regulated tokens

Regulated tokens are regulated by the FCA, including under FSMA or the EMRs. The Final Guidance sets out two broad categories of regulated tokens: security tokens and e-money tokens. Security tokens are "*those tokens that provide rights and obligations akin to specified investments as set out in the RAO excluding e-money*".[27] The most relevant specified investments for cryptoassets are identified as shares, debt instruments, warrants, units in collective investment schemes, and rights and interests in investments. Santander's world-first end-to-end blockchain bond, the issuance of which A&O advised on[28], is an example of a cryptoasset that would be treated as a debt instrument. Separately, e-money tokens are tokens that meet the definition of e-money under the EMRs (i.e. as noted above, a representation of fiat currency on an electronic device which is usable to pay third parties).

Persons carrying out activities in respect of regulated tokens should therefore consider whether they are operating within the regulatory perimeter and, if they are, which permissions they require from the FCA. In the cryptoasset context, relevant market participants who should be aware of the regulatory perimeter include exchanges and trading platforms, payments providers, custodians/wallet providers and advisers, brokers and other intermediaries, and token issuers.

Some outstanding questions and uncertainties

The Final Guidance recognises that cryptoassets can be structured in many different ways and this may present difficulties for categorisation. This concern is particularly acute in the context of 'stablecoins': a collective term for cryptoassets which are subject to methods of value stabilisation such as being backed in whole or in part by fiat currency or some other financial asset.

---

26 Paragraph 34 of the Perimeter Guidance at Appendix 1 to PS19/22

27 Paragraph 64 of the Perimeter Guidance at Appendix 1 to PS19/22

28 *A&O advises Santander on the first end-to-end blockchain bond issue* (12 September 2019) (https://www.allenovery.com/en-gb/global/news-and-insights/news/allen-and-overy-advises-santander-on-the-first-end-to-end-blockchain-bond-issue)

Factors such as rights granted by the coin or the underlying assets that back the coin will provide an indication as to whether it might be categorised as a security token or e-money. However, the Final Guidance recognises that ultimately the categorisation of stablecoins can "*only be determined on a case-by-case basis*".[29] Given the volatility in pure exchange tokens, like bitcoin, many commentators have assumed that stablecoins would perhaps be more likely to make a meaningful breakthrough as potential alternatives to fiat currency. However, this anticipated growth has been stymied to a certain extent by the inherently "international" nature of DLT which can give rise to the need to comply with laws and regulations across multiple jurisdictions, including the financial crime controls noted below.

A related point highlighted by the Final Guidance is that a particular cryptoasset may move between categories over time. Although the structure of and rights granted by a token will usually be determinable at the outset, it will also be necessary to be mindful of how a token is used in practice; as practice changes, so might the nature and appropriate categorisation of the token. Firms operating in this space need to be alert to this risk and keep these factors in mind as they might require permissions in relation to tokens which were previously unregulated.

The Final Guidance primarily focuses on FSMA and the EMRs. It does not consider whether the FCA's regulatory perimeter should be extended but rather looks at the question of which cryptoassets fall within the existing regulatory perimeter. HM Treasury is due to consult on the extension of the regulatory perimeter to capture unregulated cryptoassets. One example of the extension of regulation to cover cryptoasset-related activities is the implementation of the EU's Fifth Anti-Money Laundering Directive. Amendments to the MLRs were published on 20 December 2019 and came into force on 10 January 2020. Importantly, cryptoasset exchange providers and custodian wallet providers now fall within the scope of the MLRs and are therefore subject to registration, disclosure, customer due diligence, internal controls, record-keeping, and reporting requirements. An overview of the amendments to the MLRs can be found here.

The FCA is just one of many regulators determining the interaction of cryptoassets with their regulatory perimeters. A harmonised international framework for cryptoassets regulation would be beneficial from the regulators' perspective as it would reduce the risk of regulatory arbitrage and also from the perspective of firms that operate in multiple jurisdictions. At present, regulators appear to be taking divergent approaches. For example, in contrast to the FCA's approach of applying the existing regulatory perimeter to cryptoassets, France[30] has created a bespoke framework for 'digital assets'. The European Commission's consultation document, published on 19 December 2019, is a promising development in that it seeks, among other things, to address the classification of cryptoassets at an EU level. Bodies such as the European Commission as well as the Global Financial Innovation Network, International Organisation of Securities Commissions, and European Supervisory Authorities will be crucial in encouraging regulators to approach cryptoassets in a consistent way.

Conclusion

So are we any closer to solving the crypto-crossword? Perhaps, but there are many clues that won't be identified (let alone solved) until there is a significant increase in the number of disputes involving cryptoassets and smart contracts that come before the courts.

As we have explored in this article, some of the key current themes in cryptoassets and smart contracts are:

- The proprietary nature of cryptoassets is still to be fully worked through, even putting to one side the possible variation between different types of cryptoassets. For instance is bitcoin merely imaginary (as suggested by Mr Justice Zacaroli) or will there be some data that actually is your bitcoin? As we have discussed, the answer to this central question will have significant implications for transfers of cryptoassets and parties' respective rights, for instance if cryptoassets are sold, stolen, or are the subject of trust or security arrangements.
- In the field of smart contracts, it is still relatively early days. While a degree of comfort can be derived from the Legal Statement's (unsurprising) conclusion that English contract law can be applied to smart contracts, this isn't the same

[29] Paragraph 52 of the Perimeter Guidance at Appendix 1 to PS19/22

[30] French law paves the way for the digital assets services providers regulation (29 November 2019) (https://www.allenovery.com/en-gb/global/news-and-insights/publications/french-law-paves-the-way-for-the-digital-assets-services-providers-regulation)

thing as saying it's necessarily a good idea in every case. For instance there can be significant risks in contracts that use computer code partly or wholly for their contractual terms while, as the *B2C2 v Quoine* case shows, contracts automatically concluded by software run the risk of being binding even where the outcome is commercially perverse.

– As for the regulatory sphere, there is no doubt that regulators in the UK and elsewhere are becoming ever more focused on cryptoassets, although we are yet to see a harmonised approach across international regulators and supranational bodies. While increased regulatory scrutiny does create more potential pitfalls for market participants, it also has the potential to give cryptoassets the level of credibility required for major finance and tech powerhouses to have the confidence to invest in the development of cryptoassets in a serious way and hence for cryptoassets to become much more mainstream.

One thing is for certain: 2019 was the year that awareness of cryptoassets increased exponentially, not only among commercial parties, lawyers and regulators, but also in the public at large. We expect this trend to continue in 2020 and beyond.

Contact information

Oliver Rule +44 20 3088 2072
Counsel, London oliver.rule@allenovery.com

Mohamed Sacranie +44 20 3088 1741
Trainee, London mohamed.sacranie@allenovery.com