Commercial Crime

Cryptoassets – Recent Developments in Global Regulatory and Legal Challenges

According to a recent Bloomberg report, as of 22 September 2020, cryptoassets are the world's top -performing asset class so far this year.

The rapid growth of the cryptocurrency ecosystem has meant that financial regulators around the world have had to address numerous and difficult challenges in an attempt to arrive at a consistent, clear, and coherent guidance across jurisdictions. This is particularly important to ensure that cryptoassets and any related activities are treated similarly due to the borderless nature of cryptocurrency transactions. There is a clear need for regulatory bodies worldwide to take a stance on cryptocurrency regulation to drive mainstream adoption. Mainstream adoption would mean that institutions would begin investing in cryptocurrencies, which would put pressure on cryptocurrency companies to operate with sound corporate governance. Regulatory challenges have been identified at each stage of the decision-making process: assessing the scope of crypto-related activities, determining the regulatory perimeter, identifying potential risks and harms, and gauging the suitability of existing national laws and regulations.

Here is a list I have identified of the most salient reasons why regulators and legislators have encountered difficulties in regulating cryptocurrencies:

- A cryptocurrency is a digital token that exists within a specific ecosystem that consists of a peer-to-peer network, a consensus mechanism, and a public/private keys infrastructure. There is no central authority that governs the system, instead the rules governing the system, (e.g. defining what constitutes a valid transaction, specifying the total supply of digital tokens and their issuance), are enforced by all the network nodes/participants.

- They ensure pseudo-anonymity (in the case of bitcoin, and ether, for example) or complete anonymity (in the case of Monero, Zcash) of the transacting parties.

- Transactions are irreversible and cannot be unfolded and changed by enforcement authorities.

- Past transactions are immutable, so it is not possible to guarantee the right to be forgotten.

- Transactions are automatically validated by the protocol and they do not need any type of authorisation or regulatory validation.

- The blockchain is transnational and transactions occur across national borders.

- Cryptocurrencies have a fungible, financially volatile, and unclear nature, meaning that they are cross-sectional and overlap with the domain of multiple regulatory authorities.

The current global regulatory guidance and legislative initiatives on cryptoassets focuses on three key aspects: (1) the nature and form of cryptoassets, (2) the issuance of cryptoassets, and (3) intermediated activities in the life cycle of cryptoassets.

Furthermore, the regulatory guidance seems to be converging towards the three-category classification of a cryptoasset as: (1) a payment/ exchange token, (2) a utility token, and (3) a security token.

As I will explain later, this seems to be a rather broad categorisation which may become more refined over time, as legislators, regulators, and national courts encounter an increasingly diverse set of cryptoassets. The advent of 'stablecoins' is a case in point. 'Stablecoins' are fiat-backed digital currencies, which attempt to offer price stability by being pegged to a national currency reserve such as the U.S. dollar. The first of its kind is Tether, whose stablecoin promised to be backed by $1 each to maintain value stability.'Stablecoins' can also be issued by a bank, and thus they are called central bank digital currencies, ('CBDCs'), or by a private company, such as Facebook's Libra or Tether.

European and U.S. financial regulators have recently issued positive statements regarding the viability of 'stablecoins'. The President of the European Central Bank, Christine Lagarde, stated at the Parliamentary Assembly this week that the supranational bank is looking into the benefits and risks of a bloc-wide digital currency. Rather than as a replacement for cash, a digital euro

would 'complement' traditional fiat money and provide an alternative to 'private digital currencies' for EU citizens. This, she added, would 'ensure that sovereign money remains at the core of European payment systems'. It is of note that there have already been dissenting voices in respect of the use and choice of terminology, 'stablecoins', as it may be misleading, and it should be replaced by a choice of terminology which shifts the emphasis away from the issuer's promise (and therefore potential liability) of 'stability'.

This cautious European approach may come in light of the legal suits Tether is now facing in the U.S. Tether and the crypto exchange Bitfinex and its parent firm, iFinex, face a class action accusing them of deceptive, anti-competitive and market manipulation behaviour. The complaint at the centre of the legal suit is that over five years Tether issued $3billion-worth of unbacked stablecoins, USDT tokens, which Bitfinex then used to purchase cryptocurrencies on the open market to prop prices up during market downturns. Tether is also facing another ongoing case brought by the New York Attorney-General. Last week the New-York Supreme Court ruled that Bitfinex and Tether must comply with a Court Order in place, namely a documents production order detailing the crypto exchange's financial history and transactions with Tether, the stablecoin issuer, with which it shares corporate owners and key executives. There is also an injunction in place prohibiting Tether from loaning funds to Bitfinex. The respondents have yet to explain what happened to the first $600 million Tether loaned Bitfinex.

From a legal and regulatory point of view, it is critical therefore to understand how the creation, transaction, and use of cryptoassets/tokens is linked to the underlying digital infrastructure, the blockchain.

Significantly, traditional assets recorded on a distributed ledger technology (DLT) infrastructure (i.e. tokenisation) should be distinguished from new and natively-digital cryptoassets with unique characteristics, such as bitcoin or ether. The fundamentally new characteristic of a native coin such as bitcoin or ether is the incentive role that it plays in maintaining the infrastructure. This type of cryptocurrencies belongs to the protocol layer and do not have a central party issuing them. They are exchange/payment tokens and are unregulated.

Another type of token can be created on top of the original, native coin and can serve the purpose of running specific decentralized financial, ('DeFi') applications, or D'apps on the Ethereum infrastructure. These are, in turn, assets, either with financial instruments such as securities, or with commodities such as utility tokens. Actors operating at different layers of the infrastructure are likely to be treated differently from a regulatory and legal perspective.

It would be indeed hard to use a blanket approach to regulation. A legal and regulatory classification of a cryptoasset should be based on an in-depth assessment of several factors: rights attached, access, and economic function of the token. For example, if a token derives its value from the financial performance of some enterprise, then it is a financial asset or security. If the value comes from its use, like enabling participation in a community, then it is a utility token, and it is unregulated.

However there is still a certain degree of confusion regarding the position of when utility tokens meet the definition of e-money. According to the FCA guidance: *"E-money tokens are tokens that meet the definition of electronic money in the EMRs. That is: electronically stored monetary value that represents a claim on the issuer; issued on receipt of funds for the purpose of making payment transactions; accepted by a person other than the issuer; not excluded by regulation 3 of the EMRs".* The response from the public to this guidance was that it was unhelpful, categorizing e-money tokens within the utility tokens. This is because utility tokens are largely unregulated, and the combination of regulated and unregulated token types within one overarching category is confusing.

Many jurisdictions, including the UK, agree on regulating tokens according to this distinction. This, for example, means that those entities who transact and distribute tokens as currencies should be classified as a 'money transmitter', and therefore, subject to regulation and licensing in order to ensure compliance with anti- money laundering, and with combatting financing of terrorism regulations. The majority of cryptoasset-related activities carried out by intermediaries show strong similarities to existing financial activities found in traditional markets (e.g. storage, exchange and trading), and therefore are regulated as such. In other words, the points of contact between the cryptoworld and the real world deriving from the conversion of cryptocurrencies into fiat currencies has been the focus of attention of regulators and law enforcement.

For these reasons, all leading national and international authorities have focused their attention on those elements of the cryptocurrency ecosystem that allow the conversion of cryptocurrencies into fiat currencies, and their sale, exchange, purchase, storage/ custody and issuing. Three entities fall under this definition: 1 Crypto-exchanges, 2 Wallet providers, 3 Issuers and administrators.

The regulation of exchanges and wallet providers

Exchanges are of particular relevance. The Financial Action Task Force, ('FATF'), the international financial watchdog, has made it clear to regulators that they needed to cooperate to make measures such as the 'Travel Rule' more effective worldwide. FATF is set to meet in October to discuss how to improve global cooperation and how to develop measures for a stronger global framework for cryptocurrencies regulation. The main goal is for national authorities to coordinate and share information on virtual asset service providers, ('VASPs'). A VASP is a term used to describe crypto-exchanges and peer-to-peer services as well as wallet providers and custodians. It can also include any business that trades or transacts in digital assets.

Here are some of the main reasons why I am of the view that it makes sense for regulators to focus on exchanges:

1. Exchanges are legally recognized companies that are managed by centralized governance. They have managers, funders, owners, and shareholders, and the regulators and law enforcement can identify specific legal persons having formal authority, organizational responsibilities, and potentially legal liabilities. The Bitfinex case is a good example.
2. Centralized Exchanges (CEX) represent the only element of the ecosystem where a conversion between a cryptocurrency and a fiat currency can happen, thus representing the real point of interconnection between the cyberworld of cryptocurrencies and the real world of legally recognized fiat money.
3. This has become a particularly important aspect in the burgeoning crypto-litigation and investigation (blockchain forensics) in relation to matters such as identifying and tracing

fraudulent funds, and obtaining interlocutory remedies such as proprietary and freezing injunctions, document production orders, and asset preservation orders for complainants and victims of cyber fraud whose stolen cryptocurrencies are stored in a wallet with an account linked to a particular exchange. The following cases have made legal history in cyber litigation in the UK:

AA-v-Persons Unknown [2020] 4 WLR 35 (a proprietary injunction was granted to a cyber insurer in respect of bitcoin BTC paid as ransom to unknown hackers who transferred the funds to a wallet and accounts held with the crypto-exchange Bitfinex and its parent company iFinex. The Court acknowledged for the first time the legal status of bitcoin as property).

Robertson-v-Persons Unknown (unreported) 15 July 2019 (an asset preservation order was granted to a victim of a cyber fraud who was induced to transfer BTC to a person unknown, who then transferred most of the BTC to a further person who held the BTC in a wallet with an exchange. The victim obtained an asset preservation order in respect of the BTC held in the wallet together with a Bankers Trust, a Norwich Pharmacal disclosure order against the exchange).

Vorotyntseva- Money-4 Limited, trading as Nebeus.com [2018] EWHC 2596 (a freezing injunction was granted to prohibit the dissipation of cryptoassets, and the order was specifically made against the directors as well as the crypto-exchange).

4. Being centralized market places/platforms, they are not characterized by peer-to-peer exchanges and can be relatively easily identified, monitored, and regulated, when it comes to AML and CFT regulations, unlike de-centralized exchanges (DEX).
5. Exchanges and wallet providers have customers using them, accessing them, and subscribing to their services. Therefore, they can potentially request the identities of their customers and provide a comprehensive list of their customers' portfolio to regulators to counteract anonymity, so they can be KYC compliant.

6. Exchanges operate through clearly identifiable servers that are geographically located in a specific country and can be targeted and potentially shut down (of note, not only by regulators, but also by hackers).

As previously outlined, the use of cryptocurrencies that remain completely within the cyber world is not considered an object of regulation in most jurisdictions. Legally, bitcoin and ether are not securities; they are crytpocurrencies, or exchange/payment tokens, and as such they are unregulated. The essential characteristic of these cryptocurrencies is the lack of a central authority issuing or administering the currency.

The regulation of ICOs

Unlike native cryptoassets, cryptotokens released through a token sale also known as an initial coin offering, ('ICO') do have issuers, organisers and central administrators of a project who sell digital tokens to members of the public to finance the development of new technological services and platforms. After an initial sale, cryptocurrency exchanges scatter across the globe lists of tokens for trading and facilitating an active secondary market, in which wild price fluctuations are common. The spectacular growth of ICOs has caused some to argue that these sales are just new tools for fraudsters and ponzi schemes, making ICOs one of the main targets for regulators across the globe.

The majority of tokens released through an ICO tend to be treated as securities by nearly all jurisdictions. As such, these tokens are treated as investment contracts into underlying assets. The value of the underlying asset depends on the value generated by third parties in their direct management of the asset. In the U.S. the Securities Exchange Act 1934 and the Securities Act 1933 have introduced a test to determine whether a financial transaction is an investment contract, this is known as the Howey test. The test determines that a transaction represents an investment contract if *'a person invests money in a common enterprise and is led to expect profits solely from the efforts of a promoter or a third party."*

ICOs in which tokens are issued in the form of securities are called STOs. For this reason, a variety of legislations treat all asset tokens issued over a blockchain as "cryptosecurities", or security tokens.

According to the FCA guidance security tokens provide rights and obligations akin to specified investments, as for example a share or a debt instrument: *"For our taxonomy, we specifically refer to security tokens as only those that reach the definition of specified investments under the RAO. The category has been slightly amended to specifically exclude e-money from this definition."* Such tokens are regulated as specified investments under the Regulated Activities Order 2001 (RAO), as financial instruments under the Markets in Financial Instruments Directive (MiFiD).

The consensus that is emerging among regulators worldwide is that a token is a cryptosecurity when the following three conditions are met:

1. The token adheres to the tests employed to define securities.

2. The token is issued and distributed before the underlying service is fully developed and operational; there is no way to use the token directly.

3. The token is not sold straight to the buyer in order to be directly used; it is sold to intermediaries or third parties, such as custodians.

If any one of these three conditions holds, then the token issuance through an ICO can be regarded as creation and distribution of securities to the public through an STO. These three objectives ensure that the nature of the token is established by regulatory authorities beforehand, and that its use and value can be predicted and better understood, and thus protecting potential investors and consumers.

The Swiss Financial Market Supervisory Authority (FINMA) has been similarly influential in the emergence of token classification frameworks. FINMA was the first regulatory body to put forth a classification of cryptoassets in November 2017, which has since been considered by regulators from other jurisdictions. As of this month the Swiss have announced a complete overhaul of

their national laws to make for new crypto laws and a comprehensive legal framework - the Blockchain Act.

The UK, on the other hand, has been lagging behind. The "UK Jurisdiction Taskforce"('UKJT') published its much-anticipated Legal Statement on the Status of Cryptoassets and Smart Contracts in November 2019 to coordinate the efforts of the financial regulator (the Financial Conduct Authority - FCA), the central bank (the Bank of England - BoE), and the Ministry of Finance (Her Majesty's Treasury). The expected benefits of coordination include information sharing, learning and the pooling of resources, in addition to potentially providing a higher degree of legal certainty and regulatory guidance for the industry and consumers.

Enforcement actions

A number of enforcement actions have been observed, in particular within jurisdictions with the highest levels of cryptoasset activities, such as the USA, Japan, South Korea, Switzerland and Israel. Most U.S. enforcement and legal actions have focused on ICOs. The U.S. regulator, Securities and Exchange Commission ('SEC') has been particularly active in enforcing securities regulation on ICOs of tokens deemed securities. To date there haven't been any UK cases.

A brief overview of the American cases is informative.
Lacking homogeneity across federal states, the status of tokens under U.S. securities laws is anything but clear. The test under which security status is assessed—the Howey test—has uncertain application to blockchain-based tokens, particularly those that entitle the holder to use a particular technological service.

U.S. federal courts have been asked to clarify whether a particular token is a security, for instance. One example is the class action against Ripple Labs in the USA, alleging that the XRP token was a security when offered to the public.
Another very interesting case is **SEC-v-Telegram**. Founded in 2013, by a group of Russian founders with the legal headquarters in UK, and the operational centre in Dubai, UAE, Telegram is a global cloud-based instant-messaging and Voice over Internet Protocol application (VoIP).

VoIP refers to the delivery of voice messages (e.g. phone calls) and multimedia (e.g. photos and videos) using the internet.

In December 2017, Telegram announced its plan to use an ICO to launch its own blockchain platform called the Telegram Open Network (TON), including a cryptocurrency called "gram". The TON infrastructure would be both decentralised and centralised, as some centralisation was necessary in order to scale quickly and effectively. One of the benefits of Telegram developing its own currency is the ability to offer an in-app payment system. This means that users could move funds privately (due to the encrypted nature of Telegram's messages) and across borders with minimal fees. Telegram set out to fundraise in two distinct stages. The first involved the sale of contractual rights to acquire 'grams' if and when they were successfully launched. The second stage would be to release the 'grams' themselves. This process is widely known as Simple Agreement for Future Tokens, ('SAFT'). According to U.S. securities laws and SEC, the contractual rights would be treated as securities, and those sales would have to be registered (if not exempt from registration).

Telegram argued that it had complied with the U.S. securities law by registering the contractual rights and the company was waiting to issue 'grams' until they were functional. At that point, Telegram argued, the 'grams' were not securities, so did not require registration.

The SEC contended that the entire plan amounted in law to a single scheme to distribute 'grams', which were not registered and were not exempt from registration. Because there was a single scheme, the original purchasers of the contractual rights would be 'underwriters' acting for Telegram, and thus the entire distribution would be tainted because the ultimate purchasers would not all qualify as accredited investors.

The federal district court of New York ruled in favour of the SEC. There is now a worldwide injunction in place prohibiting Telegram to sell 'grams'. The main points of interest which arise from this case are:

1. This ruling stands as a warning to any crypto-entrepreneur contemplating the SAFT process.

2. The regulatory arm of SEC is long, as it has successfully reached a company, a crypto-entrepreneur operating primarily overseas, (UK and UAE), and only 39 of the 171 initial purchasers were in the U.S.

3. This is the first legal ruling (binding on Telegram) which reinforces the broad stance taken by the American regulator in pursuing SAFT distributions, namely that a sale of contractual rights to acquire a cryptoasset when launched has to be integrated with the eventual sales or re-sales of the asset because the original purchasers are actually underwriters.

4. SEC brought this suit in the absence of any claimed fraud.

5. When it comes to crypto sales using the SAFT process, it does not matter what entrepreneurs call contractual rights. Telegram didn't call them SAFTs, but the SEC successfully argued they were.

The future of crypto-regulation and legal challenges

FCA regulatory guidance has thus far predominantly focused on the creation and distribution of pre-mined cryptoassets (e.g. ICOs), as well as cryptoasset exchanges and trading intermediaries, and this is the case with most jurisdictions. Significantly an important crypto-related activity, such as mining, the driving force behind bitcoin's blockchain, has remained unregulated. An exception is Russia's draft Federal Law on Digital Financial Assets, whereby miners are required to obtain a license based on their level of activity (dependent on energy consumption).

Some cryptoasset infrastructure providers, maintainers, and operators (e.g. developers, miners, and node operators) have received little to no attention in regulatory frameworks thus far, or have not been clearly exempted from existing regulations.

Likewise, the role of developers has been largely ignored to date. Some blockchain protocols and systems have become highly centralised, i.e. a small number of core developers may hold the power to change the protocol. There have been suggestions to consider expanding fiduciary duties to protocol developers with highly centralised governance rights, although these proposed measures have been met with resistance from the technical fraternity.

Node operators arguably may be liable for unlawful uses of a DLT system. Under the EU's General Data Protection Regulation (GDPR), node operators could face liability as so-called "data controllers" because they actively run the software and have a say in protocol upgrades. However, the EU Blockchain Observatory suggested otherwise, recommending that developers — as well as node operators on public, permissionless blockchains — should probably not be held liable under the GDPR. [cf. The EU Forum and Observatory on Blockchain (2018) Blockchain and the GDPR].

Liability of infrastructure providers and operators may need to be assessed differently depending on the layer of the DLT system on which they operate and the role they fulfil. For example, there is a strong argument for regulators to treat developers of a particular DLT-based application differently from developers of the underlying DLT protocol. Likewise, those involved in issuing a particular cryptoasset contract may be treated differently by regulators than those producing records (e.g. mining blocks). Those involved in developing public, permissionless protocols could be subjected to different liability standards than those developing private, permissioned protocols.

Whilst ICOs have been on most regulators' radar, other mechanisms of token distribution, such as forks have received very little or no attention. A set of questions would need to be answered by regulators in order to understand where and what regulatory intervention is needed for these other distinct distribution mechanisms. One unanswered question is who, if anyone, should be considered responsible for the token issuance in case of a fork. In the event of a fork, network participants and service providers (e.g. miners, node operators, developers, exchanges, wallets, etc.) ultimately decide which side of the fork to support. For instance, in the case of a 'hard fork', custodial service providers may be assigned the responsibility of selecting the appropriate chain on behalf of their clients, and credit newly created tokens accordingly. Forks create a substantial

opportunity for "wealth-tunnelling" (i.e. the use of rights within a system to transfer wealth from one group to another in a legally questionable manner) and things akin to minority shareholder oppression. For example, forks could be created by majority holders to change governance and profit rights of minority holders. If minority holders refuse to run the newly forked chain, they may be left with worthless cryptoassets.

Furthermore, there is the rise of decentralised exchanges, (DEXs) which pose new concerns for regulators given their decentralised nature. While most regulatory responses have only focused on centralised or peer-to-peer exchanges, it remains unclear whether DEXs are included and, if so, how regulatory requirements can be enforced for this type of exchange. Some steps to address this regulatory challenge could be to gauge the level of decentralisation of these exchanges, clarify the applicability and enforcement of AML/CFT and assess whether practices (e.g. collecting transfer fees) may automatically bring them under existing regulation.

Regulators will eventually need to decide which of these activities should comply with existing regulations, be subjected to bespoke regulation, or remain unregulated. This will require some fine-tuning and the main challenge is to ensure the technology operates in a fair and secure environment but at the same time ensuring innovation and creativity of the cryptoasset ecosystem.

By Flavia Kenyon
36 Commercial Crime

Flavia holds an impressive and varied portfolio of national and international financial crime cases. She has developed a strong profile in government advisory and ambassadorial work,

recently advising the Romanian Embassy on issues of state immunity and commercial property. Her advisory work also extends to non-governmental organizations and she is currently advising Transparency International on an international case of bribery of public officials in the oil and gas industry.

Flavia also advises start-ups, SMEs, and individuals on cyber fraud litigation and regulatory issues emerging from new technologies, such as blockchain, crypto-currencies, and deepfakes.
Flavia is frequently instructed to defend in complex, multi-handed fraud trials with an international dimension. She has defended in insolvency prosecutions, money laundering, cyber fraud, fraudulent dealing, international conspiracies to defraud financial institutions, and to making articles to use in fraud, ponzi schemes, and fraud by misrepresentation.
Flavia is the author of numerous legal articles on the subject and of a monthly blog, "36 Cyber Bites".
Flavia was born in Romania, educated at Oxford University and called to the Bar in 2005. Flavia is the first British criminal barrister of Romanian origin to be called to the UK Bar in modern times.
Flavia is listed as a leading individual in both Chambers and Partners and The Legal 500.

For further guidance, please contact the 36 Commercial Crime and Regulation team by calling +44 (0)20 7421 8051 or emailing clerks@36commercial.co.uk