Freshfields Bruckhaus Deringer

FSbriefing

Cryptocustody – what you need to know

Introduction

It's been impossible to avoid talk of cryptocurrencies over the past year. The highly volatile price of the most well-known cryptocurrency, bitcoin, has been a news story in itself. Even among the broader population of cryptocurrencies – increasingly recharacterised as 'cryptoassets' in the regulatory discourse, reflecting most regulators' view that these are not strictly currencies – the popularity of similarly volatile tokens offered through initial coin offerings (ICOs) and security token offerings (STOs) has been keeping commentators, investors and regulators (not to mention lawyers) busy.

In the UK, the Financial Conduct Authority (FCA) has recently published a consultation containing draft guidance that will help firms determine whether cryptoassets fall within the FCA's regulatory perimeter. The consultation was published in response to industry calls for regulatory clarity in this area. Although the consultation does not focus on the custody of cryptoassets, it provides a high level walkthrough of the steps that market participants should take to understand whether particular cryptoassets comprise 'specified investments' and thus whether a market participant would need to be authorised to carry out the safekeeping and administration of those assets. The final guidance is expected this summer.

This is the second of two briefings on cryptoassets. For an introduction to cryptoassets and their regulatory and legal characterisation, please see the accompanying briefing – *Cryptoassets – what you need to know*. In particular, this briefing focuses on the application of the UK's rules.

The need for cryptocustody

Whether the prices of their cryptoassets are rising or falling, investors need their holdings to be kept secure. Cryptoassets are vulnerable to criminal activity just as 'real world' and financial assets are. It is, therefore, unsurprising that the burgeoning cryptoasset industry has taken a cue from the financial services sector and even established firms are now beginning to offer 'cryptocustody' solutions, by which a custodian takes control over cryptoassets on behalf of customers.

With the technological sophistication of cryptoassets comes greater complexity in the measures required to safeguard them. One only needs to look to high profile exchange hacks in recent years – Mount Gox, the DAO hack, Coincheck – to realise that cryptoassets present risks to consumers through cybercrime. Cyber threats, which often stem from failings on the part of exchanges and wallet providers to put in place appropriate systems and controls, can put consumers at risk of large losses. Cryptoassets are now viewed as high-value targets for theft. Both investors and service providers (including cryptocustodians and crypto-exchanges) are increasingly being targeted by cybercriminals, in particular to obtain the private keys which enable consumers to access and transfer their cryptoasset.

As a result, the cryptoasset industry has looked to mimic the infrastructure of the more established financial sector (which has also had to deal with being a magnet for criminal activity). Firms are beginning to offer 'cryptocustody' solutions, by which a custodian safeguards on behalf of its customers the private cryptographic key that allows control over cryptoassets. Perhaps most notably, Fidelity has announced the launch of a new entity called Fidelity Digital Assets which, among other things, offers an '*enterprise grade platform for storing, trading and servicing eligible digital assets*' (which we know to include bitcoin and ether as well as '*others*'), while also executing trades in digital assets.

This provision of custody, custody-like, and custody-adjacent services provides a potential touchpoint for cryptoassets with the regulated financial services sector, and may in some cases be the only time that cryptoassets are brought within the financial services regulatory perimeter. This puts additional focus on the activities of cryptocustodians. Below, we explore how existing client money rules, custody rules and the broader regulatory regime in the UK apply to the custody of cryptoassets.

The application of UK client money rules

UK client money rules, set out in part 7 of the FCA's Client Assets Sourcebook (CASS), require firms to take appropriate steps to protect their clients' money whenever they hold or control that client's money.

CASS 7 broadly applies to a firm that receives money from or holds money for, or on behalf of, a client in the course of, or in connection with, its:

- MiFID business; and/or
- designated investment business; and/or
- stocks and shares ISA business; and/or
- innovative finance ISA business; and/or
- lifetime ISA business.

In this context, therefore, the threshold question is whether cryptoassets can constitute money. From a legal 'standpoint', there is no single wholly satisfactory definition of what money is, and 'money' is defined (somewhat circularly) in the regulatory context as "*any form of money, including cheques and other payable orders*."

However, it is clear that most regulators do not currently see bitcoin as money, even though it is the most widely used and most liquid of cryptoassets. Indeed, the UK's Cryptoassets Taskforce (the Taskforce, consisting of HM Treasury, the FCA and the Bank of England (BoE)), in its final report, confirms that:

'*While cryptoassets can be used as a means of exchange, they are not considered to be a currency or money, … They are too volatile to be a good store of value, they are not widely-accepted as means of exchange, and they are not used as a unit of account*.'

Further, the FCA's recent consultation paper indicates that cryptocurrencies should not be considered to be a currency or money, as both the BoE and the G20 Finance Ministers and Central Bank Governors have previously set out.

It seems unlikely, therefore, that firms will be required to treat cryptoassets as client money, at least for the time being. This may change if and when the UK regulators are convinced that a particular cryptoasset is used widely enough as a store of value, a means of exchange and a unit of account.

> Cryptoassets… are not considered to be a currency or money
>
> *Cryptoassets Taskforce*

Stablecoins are cryptoassets which are pegged to real world currencies or commodities usually by way of algorithmic pegging (involving the buying and selling of underlying instruments as directed by an algorithm in order to expand or contract the supply of the stablecoin) or by use of asset reserves (similar to the gold standard).

In and of themselves, stablecoins may be no different to other cryptoassets. They use the same technologies, are issued by the same sorts of market players, and ultimately can present the same risks to investors (in that losing possession or control of a private key would deprive an

investor of any ability to use the asset).However, if their proponents are to be believed, stablecoins can avoid the extreme price volatility that has characterised cryptoassets over recent years, and could be used by market participants in ways that start to make stablecoins look more 'money-like'. It will ultimately be for regulators and central banks to decide when a particular cryptoasset should be classed as money.

We also note that in relation to stablecoins, the FCA's consultation paper indicates that any token that is pegged to a currency, like USD or GBP, and is used for the payment of goods or services on a network could potentially meet the definition of e-money.

The application of UK custody rules

The starting point is that, consistent with the regulatory concept of technological neutrality, the regulatory status of an asset should not be affected by the use of technology.

How should the UK custody rules, set out in CASS 6, apply to services provided by cryptocustodians? The Taskforce makes it clear in its final report that:

'*The regulatory status of an asset or activity should not be affected by the use of DLT [Distributed Ledger Technology] and the process of tokenisation, provided that doing so does not change the financial risk characteristics of the asset or the legal title to the underlying asset.*'

If a cryptoasset would be regulated if it were in non-digital form, then using DLT should not change its regulatory status

Therefore, we can expect that if a cryptoasset would be regulated if it were in non-digital form, then representing it as a token using a DLT platform should not change its regulatory status. However, it is possible that operational differences between cryptoassets and non-cryptoassets may change the way in which regulation applies. For example, there could be differences in the way that systems and controls requirements would apply.

Technological neutrality is the principle that regulation should neither impose nor discriminate in favour of the use of a particular type of technology. The principle is defined in EU law (under recital 18 of the Framework Directive 2002/212) as follows:

'*The requirement for Member States to ensure that national regulatory authorities take the utmost account of the desirability of making regulation technologically neutral, that is to say that it neither imposes nor discriminates in favour of the use of a particular type of technology, does not preclude the taking of proportionate steps to promote certain specific services where this is justified, for example digital television as a means for increasing spectrum efficiency*.'

CASS 6 builds on the requirement on firms (set out in Principle 10 of the FCA's Principles for Businesses) to take appropriate steps to protect the clients' safe custody assets for which it is responsible. In short, a firm will be subject to CASS 6 when it:

- holds 'financial' instruments belonging to a client in the course of its MiFID business; and
- is safeguarding (ie holding) and administering certain specified investments, in the course of business that is not MiFID business.

This, therefore, gives rise to two threshold questions in the context of cryptoassets:

- Is a cryptoasset a financial instrument (or, in the UK, a specified investment)?
- What does it mean to 'hold' a cryptoasset?

Are cryptoassets financial instruments?

The way that different types of cryptoasset are categorised under the regulatory regime stems from the taxonomy set out by the Taskforce, which divided cryptoassets into three types: exchange tokens (essentially, cryptocurrencies), security tokens (which give rights in or entitlements to other assets) and utility tokens (which give rights in or entitlements to a

product or service). More recently, the FCA adopted the Taskforce's taxonomy in its latest consultation paper. See our accompanying briefing for further information. Broadly speaking, under the Taskforce's taxonomy:

- exchange tokens and utility tokens are unlikely to be financial instruments (unless they share the characteristics of a security token); but
- security tokens will always constitute a financial instrument or a specified investment. This is due to the fact that they are defined as security tokens by virtue of being specified investments under the Regulated Activities Order.

However, the Taskforce report identifies that the complexity and opacity of many cryptoassets means it is difficult to determine whether or not a particular asset will qualify as a security token. For example, although it is not explicitly stated in the Taskforce report, it seems possible that non-native tokens could be treated differently to native tokens, as they share certain similarities to depositary receipts (as set out in further detail in our accompanying briefing).

Whether and what regulation applies to a particular cryptoasset can ultimately only be decided on a case-by-case basis. The FCA's draft guidance on cryptoassets aims to help firms conduct this analysis for themselves, but acknowledges that the analysis is likely to be highly nuanced. The FCA, therefore, encourages firms to seek expert advice if they are unsure whether the products they offer or interact with fall within the regulatory perimeter.

In addition, the FCA commented in its risk warning on so-called ICOs last year that although many ICOs will fall outside the regulated space, depending on how they are structured, some cryptoasset offerings marketed as ICOs may involve specified investments (in which case they would be termed more appropriately as STOs) and firms involved in an ICO may be conducting regulated activities.

Control of the private key is often the only way to spend cryptoassets and may be considered to be the same as 'holding' that asset

What does it mean to 'hold' a cryptoasset?

In order to fall within the CASS rules, it must be ascertained that a firm 'holds' a qualifying cryptoasset. There are conceptual difficulties relating to the idea that one can 'hold' an asset that exists purely in digital form. However, in practice, investors in cryptoassets can do everything associated with holding an asset – most importantly, sending the cryptoassets in their 'wallet' (ie an address held within the DLT system) to another person – by using the private key for that cryptoasset. Cryptoassets are, therefore, only as secure as the private key that controls them. If the private key is lost, the cryptoassets may become completely and irreversibly inaccessible. Similarly, if a cybercriminal gains control of the private key, they will have total control over the underlying assets.

Having control of the private key which allows a cryptoasset to be moved between digital wallets and transferred to other persons is often the only way that the cryptoasset can be controlled, and may, therefore, be considered by a pragmatic regulator to be the same as 'holding' that asset. Indeed, the European Securities and Markets Authority (ESMA), in recent advice, has stated its preliminary view '*that having control of private keys on behalf of clients could be the equivalent to custody/safekeeping services, and the existing requirements should apply to the providers of those services.*' It is uncertain how legislators and regulators will reconcile 'multi-signature keys' – which require more than one digital signature to authorise a transaction – with existing concepts of 'holding', possession and ownership.

Another way of characterising a firm's ability to control cryptoassets using a client's private key, is as a mandate under CASS 8. A mandate is anything that gives a firm the ability to control assets that are held by another person. This would not involve the cryptocustodian 'holding' cryptoassets, and would engage a less detailed regime for cryptocustodians. However, in the context of cryptoassets existing on decentralised systems, it may not always be clear that there is another 'person' who the firm can instruct to deal with the client's assets. The FCA will need to provide clarity one way or another as to whether firms can characterise their cryptocustody activities in this way.

Controlling bitcoin, without a private key

The difficulty of exercising any control over a cryptoasset without having the private key is most apparent in a decentralised DLT system such as the bitcoin blockchain. bitcoins are not held in any physical location that could be seized, nor in any single 'digital' location that could be hacked, rather they are represented on a distributed ledger (the blockchain).

The bitcoin blockchain is designed so as to prevent control by any central participant – it would require a group collectively representing more than 50 per cent of the network's total computing power, to be able to exercise any element of control over a bitcoin without holding the corresponding private key. This is known as a '51 per cent attack'

A 51 per cent attacker would likely only be able to prevent new transactions being entered into using another participant's private key. The incentive for a 51 per cent attack is to enable the attacker to 'double spend' the coins they already hold (meaning that innocent participants could receive funds which are later invalidated), and it is important to note that even a 51 per cent attack does not enable the attacker to spend any bitcoins for which they do not have the private key.

Consequences of acting as a custodian if regulated

The CASS rules set out detailed requirements for those providing custody services, comprising the safeguarding and administration of clients' assets. It is, therefore, important to understand how the CASS rules apply to cryptoassets, and what it means to safeguard and administer cryptoassets.

Cryptocustodians typically focus their efforts on ensuring the private key cannot fall into the wrong hands

Adequate arrangements to safeguard

Requirement

Custodians can be required to take a huge variety of steps to ensure the adequate safeguarding of the assets they hold, and the regulatory requirements under CASS 6 are broadly drafted:

- CASS 6.2.1 requires firms to make adequate arrangements so as to safeguard clients' ownership rights, especially in the event of the firm's insolvency, and to prevent the use of safe custody assets belonging to a client on the firm's own account except with the client's express consent.
- CASS 6.2.2 requires firms to introduce adequate organisational arrangements to minimise the risk of the loss or diminution of clients' safe custody assets, or the rights in connection with those safe custody assets, as a result of the misuse of the safe custody assets, fraud, poor administration, inadequate record-keeping or negligence.

Application to cryptoassets

Because the enjoyment of a cryptoasset is closely tied to the security of the private key, cryptocustodians typically focus their efforts on arrangements to ensure the private key cannot fall into the wrong hands. The safekeeping of private keys is normally done in one of two ways, either of which could be considered adequate under the regulatory regime. However, it will be for firms to decide which method is more appropriate:

- *hot storage*, which essentially means keeping the private key in a place that is connected to the internet. A private key held in hot storage can be easily moved from one account to another as transactions can be instantly digitally signed and cryptoassets sent between users. The downside is that hot storage is less secure from cyberattacks. Hot storage is, therefore, likely to be used by (and offered to) those regularly trading cryptoassets; and
- *cold storage*, which refers to keeping private keys on a device that is offline (ie not connected to the internet). Moving assets in and out of cold storage can be time consuming, although private keys held in cold storage are theoretically less vulnerable to cyberattacks (but may be susceptible to destruction or theft through other means, depending on how they are held). This type of storage is likely to be more appropriate for less frequent traders of cryptoassets.

In relation to these cryptoassets, the concern as to the diminution of clients' assets relates less to insolvency, and more to the potential for a cyberattack. Backups are, therefore, an essential part of cryptocustody, and some firms have even resorted to creating physical backups made of paper (and in some cases, steel) to decrease their vulnerability to attack. A key consideration for firms contemplating this will be whether they can get comfortable that they will have in place adequate record keeping and administrative processes in relation to those physical assets.

Certain cryptoassets, in particular non-native tokens, are arguably less inextricably linked to the private key that controls their usage (see our accompanying briefing for further discussion of the legal characterisation of non-native tokens). This gives rise to an important question – should the custody of native tokens (where the private key is the only possible evidence of entitlement and transfer of an asset) be treated the same way as for non-native tokens (where there may be a competing way of demonstrating entitlement to the underlying asset)? The answer to this question will be for legislators to decide. One potential model for non-native tokens could be the model used for depositary receipts: the depositary (and issuer of the receipts), rather than the receipt holder or their custodian, is registered as title holder to the underlying shares. This process effectively immobilises the underlying shares so that the rights of the receipt holders are not undermined by the transfer of those shares.

Legal title

Requirement

The difficulty in determining who owned which assets following the collapse of Lehman Brothers has placed an emphasis on proper separation of firm and client assets in post-crisis regulatory reform. Under CASS 6.2.3 firms must effect registration or recording of legal title to a client's safe custody asset in the name of:

a) the client (or in certain cases the client's client);

b) a nominee company, an affiliate, an investment exchange or a sub-custodian;

c) any other third party if neither of the above routes is possible, the client has been notified and the asset is subject to law or market practice outside the UK; and

d) the firm, if none of the above routes is possible, the client has been notified and the asset is subject to law or market practice outside the UK.

If using option c) or d), the firm must also have taken reasonable steps to determine that there is no other feasible or better option.

> "Another area of doubt [for cryptoassets] is in property law
>
> Lord Hodge
> *Justice of the Supreme Court of the UK*

Application to cryptoassets

It is difficult to come up with hard and fast legal rules as to what constitutes legal title to a cryptoasset, and how it may be transferred. The analysis that applies to one cryptoasset may not be appropriate for another.

It is not yet clear whether the current approach in relation to dematerialised securities (regarding custodians as holding legal title to the securities on behalf of clients) is capable of being extended to cryptoassets, or if a cryptocustodian should be considered to hold possession only. As a practical matter, given this uncertainty, cryptocustodians should consider whether, whatever steps they take to safeguard their client's asset (in most cases, taking control of the private key), those steps should be taken in the name of the client or a nominee company in the first instance, and only in the name of a third party or the firm itself if there are no better alternatives.

Depositing cryptoassets with third parties

Requirement

The multitude of different cryptoasset exchanges that exist in countries around the world means that a cryptocustodian could seek to appoint a sub-custodian to provide custody services with respect to cryptoassets traded in a particular market or jurisdiction where the

cryptocustodian does not have an operation. Under CASS 6.3, when a firm makes the selection, appointment and conducts the periodic review of the appointment of a sub-custodian, it must take into account:

- the expertise and market reputation of the third party; and
- any legal requirements related to the holding of those safe custody assets that could adversely affect clients' rights.

CASS 6.3.4 restricts firms from depositing safe custody assets held on behalf of a client with a third party in a third country which does not regulate the holding and safekeeping of safe custody assets for the account of another person unless:

- the nature of the safe custody assets or of the investment services connected with those safe custody assets requires them to be deposited with a third party in that third country; or
- the safe custody assets are held on behalf of a professional client and the client requests the firm in writing to deposit them with a third party in that third country.

Application to cryptoassets

These requirements create particular difficulties for cryptocustodians as cryptoassets are subject to differing legal, regulatory and licencing regimes around the world, and exist in a legal grey area in many jurisdictions. Custodians will, therefore, have to carefully consider, and seek legal advice on, whether they can provide services in markets which do not regulate cryptoassets in the same way as other financial instruments, even if using a sub-custodian in those jurisdictions.

Administration

Requirement

The administration services provided by a custodian typically include:

- settling transactions in assets;
- cash processing associated with the client's assets;
- collecting and dealing with dividends and other income associated with the assets; and
- carrying out corporate actions such as proxy voting.

A cryptocustodian's administration activities could be significantly different to those of a traditional custodian

Where a custodian holds legal title to custody assets such as shares, the default position is that the custodian, not its client, will receive the benefit of dividends and voting rights. Under English trust law the general position is that, in the absence of a client agreement to the contrary, the custodian will be obliged to enable the relevant rights to be exercised by or on behalf of the client. Because of this, a custodian's duties in relation to administrative activities are typically limited by way of custody agreements with clients.

Application to cryptoassets

The administrative services a cryptocustodian is required to provide will depend on the nature of the cryptoassets and the custody agreements in place with clients. The capabilities of cryptoasset technology mean that a cryptocustodian's administration activities could be significantly different to those of a traditional custodian. In particular, a trend in cryptoassets has been to automate dividends and dividend-like payments through the use of smart contracts, and to utilise the cryptoasset's technological platform to enable direct voting by investors.

It is conceivable that a cryptocustodian's clients would be able to vote and receive dividends without the custodian having to intermediate the process. In this respect it is relevant to note that the FCA highlighted in its 2017 discussion paper on DLT that corporate actions are an area where cryptoassets may have an advantage over other assets, and that the technology '*may augment or replace the existing process in soliciting a proxy vote for exercise of shareholder rights*'. It is possible, therefore, that the FCA would expect a cryptocustodian to safeguard the '*transparent and fully verifiable*' electronic voting and dividend payment processes that '*work*

to empower investors [in cryptoassets]'. However, this is an area that will require further guidance from the regulators.

Record keeping

Requirement

The requirements in CASS 6.6.2 R to CASS 6.6.4 R provide that a firm must keep internal records and accounts of clients' safe custody assets. Therefore, any records falling under those requirements should be maintained by the firm, and should be separate to any records the firm may have obtained from any third parties, such as those with whom it may have deposited, or through whom it may have registered legal title to, clients' safe custody assets.

Application to cryptoassets

The immutability of certain DLT transactions (including those on the bitcoin blockchain) raises a question of how to deal with a self-executed transfer that is later found to be in breach of law or has to be unwound. Such a transfer may have to be effected manually by requiring an equal and opposite transaction, rather than a true unwind. This feature may well be compatible with the fact that, following the implementation of the revised Markets in Financial Instruments Directive (MiFID 2), the custody rules now specifically refer to the need for the firm's records and accounts to be capable of being used as an audit trail. It is possible that the DLT system itself would form part of the audit trail, although it is unlikely to be sufficient on its own.

Consequences of acting as a custodian if not regulated

Even where the relevant cryptoassets are not directly subject to regulation, the regulatory regime may still bite on cryptocustodians.

The potential for customer harm means that even unregulated activities are likely to be monitored closely by regulators

Immature market structures and operational risk issues associated with cryptoasset exchanges, and trading platforms, as well as the fact that these institutions are often targets for cybercrime, may increase the risks faced by cryptocustodians and their customers. These issues could delay or deny consumers easy access to their invested funds or to secondary market trading in cryptoassets. This is particularly the case for less widely used cryptoassets (where there is no guarantee of liquidity in the secondary market, and where market structures may be even less mature). The potential for customer harm means that even unregulated activities are likely to be monitored closely by regulators.

Cryptocustodians offering custody of both regulated and unregulated assets will, therefore, need to take heightened precautions in relation to the unregulated areas of their business. This reflects in part concerns around a potential cross-over impact – ie, if the firm's systems involved in usual regulated custody activities are compromised because of unregulated cryptoasset activity, this could amount to a regulatory breach of systems and controls requirements.

Anti-money laundering

ESMA has stated that it believes that all cryptoassets and related activities should be subject to anti-money laundering provisions. This position has been reiterated by the European Banking Authority (as part of its report and advice on cryptoassets) and other regulators, and in the UK the FCA has put a significant emphasis on financial crime risks relating to cryptoassets.

The fifth Anti-Money Laundering Directive (MLD 5) expands the requirement for know your customer checks to 'custodian wallet providers' (namely, '*an entity that provides services to safeguard private cryptographic keys on behalf of its customers, to hold, store and transfer virtual currencies*.') and requires those providers to register with regulatory authorities. It is not yet clear to what extent MLD 5 will apply to cryptoassets other than exchange tokens, as it relies on a definition of 'virtual currency' that is based on the cryptoassets being used as a medium of exchange (ie a '*digital representation of value that…is accepted by natural or legal persons as a means of exchange and which can be transferred, stored and traded*

electronically'). In the UK, HM Treasury has stated that it intends to go beyond MLD 5 requirements and will seek industry views on including crypto-to-crypto exchanges, cryptoasset ATMs, wallet providers and non-UK firms (when providing services to UK consumers) within the scope of UK anti-money laundering rules.

General rules applying to financial services firms

It should be noted that a number of financial services regulations are expressed to apply even to the unregulated areas of a regulated firm's business.

FCA rules

The Taskforce report highlights that three of the FCA's Principles for Businesses apply to the unregulated activity undertaken by regulated firms – specifically, those relating to:

- the adequacy of a firm's financial resources;
- the adequacy of a firm's systems and controls; and
- the duty to deal with the FCA in an open and cooperative way.

Further, in some circumstances, the requirement for a firm to observe proper standards of market conduct applies to some unregulated activities, eg, where the unregulated activity is carried on in connection with certain regulated business. In addition, the FCA has indicated that the unregulated activities of a firm may be relevant to whether that firm continues to meet the threshold condition on suitability which requires that the firm must be fit and proper.

Additionally, the UK's Senior Managers and Certification Regime allows regulators to hold senior management in regulated firms to account for the unregulated activities for which they are responsible and the FCA's systems and controls provisions cover, amongst other things, organisational requirements, risk control, record keeping, and employee requirements. The FCA has a history of taking action against regulated firms for breaches in systems and controls relating to unregulated activities (in particular, unregulated financial services-related activities such as spot FX).

Risks relating to cryptoassets should be considered fully by the board and highest levels of executive management

PRA rules

Similarly, in its *Dear CEO* letter on cryptoassets, the Prudential Regulation Authority (PRA) emphasised the relevance of the PRA's Fundamental Rules to:

- act in a prudent manner;
- have effective risk strategies and risk management systems; and
- deal with regulators in an open and co-operative way.

In addition, the PRA stated its expectation that risks relating to cryptoassets should be considered fully by the board and highest levels of executive management. In particular, an individual approved by the PRA to perform an appropriate Senior Management Function should have responsibility for reviewing and signing off on the risk assessment framework for any planned business direct exposure to cryptoassets and '*to entities heavily exposed to cryptoassets*'. By reiterating this requirement in writing, as well as requirements relating to remuneration, the PRA hopes to encourage firms not to engage in excessive risk-taking even in unregulated instruments. The PRA also encouraged firms to ensure that they have access to appropriate, relevant expertise to assess any risks stemming from their exposure to these assets.

Potential future rules applying to cryptoassets

ESMA has stated its belief that '*greater clarity around the types of services/activities that may qualify as custody/safekeeping services/activities under EU financial services rules in a DLT framework is needed*'. In the UK, although last year's *Dear CEO* letter on cryptoassets from the PRA was aimed at firms investing in cryptoassets as principal, rather than holding as custodian, it holds some clues as to the likely future direction of the PRA's supervisory activity in this area:

- the letter relates to all cryptoassets, rather than just those that fall within the regulatory perimeter;
- the letter focuses almost entirely on avoiding excessive risk taking, and, therefore, suggests that the PRA's concerns centre around the unpredictable nature of cryptoassets' pricing and low liquidity, rather than any particular concern that cryptoassets are a fundamentally different type of financial instrument (albeit that they are potentially more vulnerable to cybercrime than other 'real world' assets); and
- the letter emphasises the areas of existing regulation that apply to cryptoassets.

It is possible, therefore, that the PRA has decided that it is better to incorporate cryptoasset activity into the existing regulatory regime rather than design a new framework of regulation specifically for cryptoassets. The former would be easier and not without precedent in the fintech sphere (operating a peer-to-peer lending platform was brought into the existing regime by being added as a regulated activity).

For further information and up to date commentary on cryptoassets and other fintech topics, please see the Freshfields Digital blog (digital.freshfields.com). If you have any questions relating to cryptoassets or any other topics mentioned in this briefing, please contact:

Michael Raffan
Partner, UK
T +44 20 7832 7102
E michael.raffan@freshfields.com

Gunnar Schuster
Partner, Germany
T +49 69 27 30 82 64
E gunnar.schuster@freshfields.com

Mark Kalderon
Partner, UK
T +44 20 7832 7106
E mark.kalderon@freshfields.com

Alexander Glos
Partner, Germany
T +49 69 27 30 85 05
E alexander.glos@freshfields.com

James Smethurst
Partner, UK
T +44 20 7832 7478
E james.smethurst@freshfields.com

Markus Benzing
Partner, Germany
T +49 69 27 30 81 29
E markus.benzing@freshfields.com

David Rouch
Partner, UK
T +44 20 7832 7520
E david.rouch@freshfields.com

Claire Harrop
Senior Associate, UK
T +44 20 7427 3259
E claire.harrop@freshfields.com

Emma Rachmaninov
Partner, UK
T +44 20 7785 5386
E emma.rachmaninov@freshfields.com

John Risness
Associate, UK
T +44 20 7785 2669
E john.risness@freshfields.com

freshfields.com