NORTON ROSE FULBRIGHT

Financial institutions
Energy
Infrastructure, mining and commodities
Transport
Technology and innovation
Life sciences and healthcare

Global Blockchain Business Council

Fintech Update

Norton Rose Fulbright LLP – May 6, 2020 - Private and confidential

PERS-#5325262-v1

EU, UK, US and other International Regulatory developments

FinTech		
EU	**The European Commission launches a consultation on a new "Digital Finance Strategy" for Europe/FinTech action plan**	The European Commission launches a consultation on a new "Digital Finance Strategy" for Europe/FinTech action plan. The consultation is anticipated to contribute to a new Digital Finance Strategy / FinTech action plan that presents a number of areas that public policy should focus on in the next five years. The new strategy will build on the work carried out during the previous FinTech action plan that has now been completed. Based upon this, the Digital Finance Strategy will take into consideration *"all the recent market and technological developments that are likely to impact the financial sector in the near future."* The Commission has identified the following four priority areas to aid the development of digital finance in the EU: 1. Ensuring that the EU financial services regulatory framework is fit for the digital age; 2. Enabling consumers and firms to reap the opportunities offered by the EU-wide Single Market for digital financial services; 3. Promoting a data-driven financial sector for the benefit of EU consumers and firms; and 4. Enhancing the digital operational resilience of the EU financial system. Responses to the consultation will inform upcoming work on the Digital Finance Strategy / FinTech action plan. The consultation period began on the 3 April 2020 and ends on the 26 June 2020. Date: 3 April 2020
EU	**The European Commission launches a consultation on a "Retail Payments Strategy" for the EU**	The European Commission launches a consultation on a "Retail Payments Strategy" for the EU. This strategy will be an important contribution to reinforcing the international role of the euro and encouraging economic autonomy. The Commission emphasised that that the size of the Single Market creates opportunities *"for payment businesses to scale-up beyond the domestic sphere, for pan-European payment solutions to emerge, and potentially for European-scale champions in payments to become competitive globally."* This would then simplify payments in euro between the EU and other jurisdictions and *"reduce EU dependency on global players, such as international card schemes, issuers of global "stablecoins" and other big techs."* The consultation is focused around four objectives: 1. Fast, convenient, safe, affordable and transparent payment instruments, with pan-European reach and "same as domestic"

		customer experience; 2. An innovative, competitive, and contestable European retail payments market; 3. Access to safe, efficient and interoperable retail payments systems and other support infrastructures; 4. Improved cross-border payments, including remittances, facilitating the international role of the euro. The outcome of the consultation will assist the Commission with preparing its Retail Payments Strategy, to be published in Q3 of 2020. The consultation period began on the 3 April 2020 and ends on the 26 June 2020. Date: 3 April 2020
EU	**The European Commission is calling for Digital Finance stakeholders to join an online roundtable on "Ensuring a technology-neutral and innovation-friendly regulatory framework"**	The European Commission is calling Digital Finance stakeholders across the EU to join an online roundtable on the topic of ensuring a technology-neutral and innovation-friendly regulatory framework. As part of the ongoing consultation on a forthcoming digital finance strategy, this webinar will discuss how to ensure that EU financial services legislation promotes innovation while safeguarding financial stability. To that end, the webinar will focus on three topics: • *Is the EU financial regulatory framework technology neutral? If not, what are the key problems?* • *How should EU financial services legislation evolve to address these problems?* • *How is digitalization affecting the supply of financial services?* • *How should EU financial services legislation handle new providers of financial services, such as technology companies?* • *How should it handle new risks?* Date: 6 May 2020
EU	**The European Commission is calling on all relevant stakeholders in the crypto-asset ecosystem to join an online roundtable on "Enabling an EU framework for markets in crypto-assets"**	The European Commission is calling on all relevant stakeholders in the crypto-asset ecosystem across the EU to join an online roundtable discussion. As part of the wider digitalisation agenda, the Commission is working to present a proposal on crypto-assets in Q3 2020, to ensure that Europe can make the most of the opportunities they create and address the new risks they may pose. The Commission has recently consulted on the topic and received lots of valuable input – this webinar presents an additional opportunity for the Commission to engage with all interested stakeholders. The webinar and discussion will revolve around the following high-level questions: • *What are the main issues that a potential crypto-asset framework should address?*

		• *Beyond issuance, trading and safekeeping are there other activities or services offered in relation to crypto-assets that should be covered in a potential crypto-asset framework?* • *What are the obstacles to the scaling up of crypto-asset firms in the EU?* • *Do so-called 'global stablecoins' – a subset of crypto-assets – require a specific framework?* • *To the extent you have experience of crypto-assets falling in scope of existing EU financial services legislation (e.g. MiFID II), have you encountered any specific regulatory obstacles*? Date: 13 May 2020
EU	**The European Commission is calling Digital Finance stakeholders to join an online roundtable on "Enabling a digital operational resilience framework for financial services"**	The European Commission is calling Digital Finance stakeholders across the EU to join an online roundtable on the topic of enabling a digital operational resilience framework for financial services. Date: 20 May 2020
EU	**The European Commission is calling Digital Finance stakeholders to join an online roundtable on "Digital Sustainable Finance - how can digital finance support sustainability?"**	The European Commission is calling Digital Finance stakeholders across the EU to join an online roundtable on the topic of Digital Sustainable Finance - how can digital finance support sustainability? Date: 27 May 2020
GERMANY	**Guidelines on applications for authorisation for crypto custody business**	These guidelines provide undertakings intending to submit an application for authorisation for cryptocustody business within the meaning of section 1 (1a) sentence 2 no. 6 of the KWG with initial guidelines on the aspects, which BaFin considers to be particularly important for the authorisation process. Date: 1 April 2020

ITALY	**Italy simplifies online conclusion of contracts**	Amid emergency initiatives aimed at coping with the Covid-19 emergency, Italy has taken two steps aimed at easing the modalities for concluding contracts online, both of which are particularly significant for the financial services sector. It is worth reminding that banking and financial contracts under Italian law are valid only if entered in writing. Furthermore, (before these new measures) contracts entered into via electronic means could automatically be deemed as signed in writing only if signed via advanced electronic signature, qualified electronic signature or digital signature. Where other forms of electronic signature were used, the determination as being signed in writing would be subject to a case-by-case assessment of their security, integrity and immodifiability. In summary the two new steps are: 1. E-mail consent automatically deemed as written form for banking and financial contracts with retail clients Law Decree no. 23 of 8 April 2020 (so called "Liquidity Decree", containing mainly measures aimed at supporting liquidity for Italian businesses) simplified the modalities of taking out contracts for certain banking and financial services to retail clients by introducing equivalence between consent given via e-mail to written consent (provided certain requirements are met, including attaching a copy of an ID document). The new measure is apparently aimed only at certain services (i.e. banking services such as accounts, and financing in any form, including guarantees, consumer credit, payment services), and it is questionable whether such provisions may be interpreted in a broader way as applicable in respect of other type of contracts that need to be entered into in writing under Italian law (e.g. for framework agreements for investment services). These provisions are clearly marked as an emergency measure, and will therefore remain in force only during the emergency period connected to the current pandemic. 2. Public digital ID can be used to sign documents electronically On 23 March 2020, the Agency for Digital Italy, issued guidelines on signing documents through the so called Public Digital Identity System (Sistema Pubblico Identità Digitale or SPID), i.e. basically a single set of credentials, issued by a qualified provider after a formal identification, aimed at granting access to online services offered by any Italian governmental or public sector entity and/or by private providers who opted-in to avail themselves of this system and entered into an agreement with the Agency for Digital Italy to this end. Following the technical steps laid down by these guidelines, it will be possible to use the same credentials to sign electronically any document, including contracts, and such documents will be deemed as signed in writing. While at the moment SPID is scarcely used by private-sector operators, this innovation will introduce a new additional way to allow for online client onboarding and the conclusion of contracts, that is more widely

		available to retail customers than digital signature, and that new users can even obtain remotely during lock-down. The guidelines implement a legislative amendment passed in the course of last year, independently from the current emergency, therefore this new modality will remain in place even after the emergency will be over. Date: 15 April 2020
FRANCE	**Banque de France invites applications to experiment with wholesale CBDC solutions**	The Banque de France is calling for applications to experiment with a central bank digital currency for interbank settlements. The aim is to discover the potentialities offered by this technology, and identify cases integrating Central Bank Digital Currencies in procedures for the clearing and settlement of tokenised financial assets. The results will be a key element of the Banque de France's contribution to a broader project conducted by the Eurosystem on the potential implementations of a CBDC. Date: 24 April 2020
THE NETHERLANDS	**Act implementing 5MLD expected to enter into force on 18 May 2020**	As set out in our earlier blog post, the Dutch Senate (*Eerste Kamer*) adopted the Act implementing the Fifth Anti-Money Laundering Directive (**5MLD**) (*Implementatiewet wijziging vierde anti-witwasrichtlijn*, the **Act**) on 21 April 2020. On 4 May 2020, the Dutch Central Bank (*De Nederlandsche Bank*, **DNB**) published a new edition of its newsletter for crypto service providers, which among other things provides that the Act is expected to enter into force on 18 May 2020. DNB urges crypto service providers to register themselves as soon as possible, noting that crypto services providers registering themselves prior to 18 May 2020 will be able to rely on the transition regime. If no draft application for registration is submitted to DNB before this date, the transition regime will not be available and crypto service providers will need to cease certain activities. If a crypto service provider continues to carry out certain regulated activities without being subject to the transition regime, this may have an effect on the assessment of such provider's application and DNB may take enforcement action. In the newsletter DNB also provides some more clarity around the following. (1) Supervisory costs: DNB previously indicated that the total expected costs for supervising crypto service providers are EUR 1,700,000. This amount will be charged to the crypto service providers and will consist of (1) costs for one-off actions, namely the registration and assessments of (co-)policymakers and (2) a basic amount for ongoing supervision. DNB previously already provided information on the expected costs for one-off actions. In the crypto news letter DNB has now indicated that because crypto supervision is new, a basic amount will be charged to the parties that will be supervised in 2020 for ongoing supervision (crypto service providers will receive an invoice in the second half of 2020). The basic amount will be determined by the Dutch

		Minister of Finance (the **Minister**) by no later than 1 June 2020. When determining the basic amount, an estimate is made of the number of parties that will be supervised in 2020. Because the actual number of market entrants is uncertain and to avoid charging unnecessarily high costs, the Minister considers it reasonable to take into account a large number of new market entrants. As a result, the amount to be paid for ongoing supervision in 2020 will in any case be less than EUR 20,000. (2) Points for attention in setting up good governance: DNB notes that in its supervision it will look closely at the crypto service provider's governance. In this regard DNB gives a number of points for attention: (1) for transparency purposes the management of the company should comprise one or more natural persons (not legal persons); (2) when setting up a company and the various roles in your organization, sufficient account must be taken of potential conflicts of interest. DNB notes that healthy governance has sufficient checks and balances in place to prevent all roles within an organization from actually being in one or a few hands (for example, in the case of a structure with a director-major shareholder, DNB expects that there will be sufficient countervailing power within the organisation between the business and compliance); and (3) DNB notes that a compliance function must be independent, which generally means in practice that, for example, a family relationship or shareholder cannot fulfill this function. DNB has a crypto service providers section on its website which, among other things, provides detailed information on the registration process, screenings, success factors of applications. It is expected that this section of DNB's website will continue to be updated in the coming weeks and months. Date: 4 May 2020
UK	**FCA delays strong customer authentication**	On 30 April 2020, the FCA published a new web page setting out a statement regarding strong customer authentication and coronavirus. The statement provides that the FCA is giving industry an additional 6 months to implement strong customer authentication (SCA) for e-commerce. This will minimise potential disruption to consumers and merchants. The new timeline of 14 September 2021 replaces the 14 March 2021 date. Firms are required to take all necessary steps to comply with the revised detailed phased implementation plan and critical path to avoid the risk of enforcement action. The FCA adds that it expects UK Finance, as coordinator for the industry, to discuss the detailed phased implementation plan and critical path with all stakeholders and agree it with the FCA as soon as possible. In the meantime, firms should continue with the necessary preparatory activities such as robust end-to-end testing. The FCA warns that after 14 September 2021, any firm that fails to comply with the requirements for SCA will be subject to full FCA supervisory and enforcement action. Date: 30 April 2020

USA	**NYDFS Requires COVID-19 Plans by April 9**

On March 10, 2020, the New York Department of Financial Services (NYDFS) issued guidance to all of its regulated institutions engaged in virtual currency business activity, requiring them to have plans for preparedness to manage the possible operational and financial risks posed by the COVID-19 pandemic. NYDFS requires the plans to be submitted by Thursday, April 9, 2020.

NYDFS does not have a one-size-fits-all set of requirements, but instead requires that the plan be "sufficiently flexible to effectively address a range of possible effects that could result from an outbreak of COVID-19, and reflect the institution's size, complexity and activities." The regulated institution's board of directors is responsible for ensuring that the plan is in effect, with sufficient resources allocated to its implementation. Senior management are the ones to ensure that specific policies, procedures and processes are in place and effectively communicated to employees.

While this guidance is aimed at those regulated entities engaged in virtual currency activity, other regulated entities also could use the guidance as part of their own pandemic preparedness planning.

The plan must cover nine subjects, as further described in the guidance:

1. Preventative measures to mitigate the risk of operational disruption, including identifying the impact on your customers, and counterparts;
2. Strategy to address the impact of the outbreak in stages, so that your efforts can be appropriately scaled, consistent with the effects of a particular stage of the outbreak;
3. Assessment of all of your facilities, systems, policies and procedures necessary to continue critical operations and services if your employees are unavailable for longer periods or are working off-site, including the effectiveness and security of remote access;
4. An assessment of potential increased risk of cyber-attacks and fraud due to an outbreak;
5. Employee protection strategies, including employee awareness and steps that employees can take to reduce the likelihood of contracting COVID-19;
6. Assessment of preparedness of your critical third-party service providers and suppliers;
7. Development of an effective communication plan to reach customers, counterparties and the public, as well as to communicate with employees, and provide a way for questions to be raised and answered;
8. Testing the plan to ensure your policies, processes and procedures are effective; and
9. Governance and oversight of the plan, including identifying the critical members of your response team, to ensure ongoing review and updates to the plan, including the tracking of relevant

		information from government sources and your own monitoring program. The plan also must consider the financial risks to your business: • Assessment of the valuation of your assets and investments that may be, or have been, impacted by COVID-19; • Assessment of the overall impact of COVID-19 on your earnings, profits, capital, and liquidity of your institutions; and • Assessment of reasonable and prudent steps to assist those adversely impacted by COVID-19. As noted above, the NYDFS wants the plan to include an assessment of potential cyberattacks at the institution, noting it had special concerns with respect to hacking risks, given how dependent virtual currency businesses are on software and electronic accounts. NYDFS pointed out that bad actors are seeking to take advantage of the disruptions caused by the current coronavirus emergency, thus requiring that the plan include increased security measures to detect possible fraudulent activity. For example, the NYDFS cybersecurity regulations require implementation of multi-factor authentication. In addition, NYDFS expressed concerns about custody risks, "such as the possible need for special arrangements to move Virtual Currency from 'cold' to 'hot' wallets during times when employees may not all be working from their usual locations." Because people likely will be working from alternate locations, employers may wish to remind their employees to be extra vigilant: many employees may have forgotten passwords or other user credentials. Consider using multi-factor authentication or other out-of- band communications to reset credentials for legitimate users, and not for hackers trying to steal cryptocurrency. The same day, similar letters requiring the submission of preparedness plans also were issued to all NYDFS-regulated institutions covering operational and financial risks, and an additional letter was issued to NYDFS-regulated insurance entities. The NYDFS has a special webpage devoted to the pandemic. In addition, Norton Rose Fulbright has established a webpage focused on the COVID-19 pandemic, offering a wide variety of information and training resources Date: 2 April 2020
SOUTH AFRICA	**Dirty money and the rise of digital payments**	Exchanging bank notes and coins are increasingly seen as risky business, as noted by Thomson Reuters in an article on the rise of digital money transactions. The COVID-19 pandemic may speed up the global move towards digital-only payments. Apart from the more widespread use of payment apps, electronic funds transfers and cryptocurrencies, the idea of digital currencies is gaining currency. Countries including China, the USA, Sweden, Japan and Russia are considering the creation of digital currencies. How these currencies are regulated remains to be seen. China's approach seems to involve the government being able to

		monitor payments, thus hampering money laundering schemes. However the risks of cyber-attacks and privacy concerns are significant. A digital currency could be based on a blockchain system and if governments issue a digital wallet to all citizens, the payment of social grants and other relief may become easier. But in countries like South Africa where many are unbanked or have no access to the necessary technology, the move to digital-only payments recedes into the future. Our large informal sector often requires payment in physical money. Promisingly, our regulators launched the Intergovernmental Fintech Working Group (IFWG) Innovation Hub on 7 April 2020 to respond to changes in the financial sector driven by fintech. The IFWG seeks to promote responsible innovation in the sector. Support from our regulators for new financial technologies may help to speed up the rise of digital payments, even in South Africa. Date: 4 May 2020
NEW ZEALAND	**Cryptocurrencies are property capable of being held on trust, New Zealand High Court holds**	In *Ruscoe v Cryptopia Ltd (in Liquidation)* [2020] NZHC 728 the New Zealand High Court held that cryptocurrencies, as digital assets, are a form of property that are capable of being held on trust. The decision is important: • as one of only a few currently in the common law world to address expressly the question, in a fully reasoned judgment, as to whether digital assets such as cryptocurrencies constitute property and can be the subject of a trust; and • because it also addresses the difference between "pure information", on the one hand, and "digital assets", on the other, in terms of characterisation as property (this is an issue of significance in areas going beyond the realm of cryptocurrencies and Distributed Ledger Technology – for example, in relation to ownership of machine-generated data created by Artificial Intelligence and the Internet of Things). This briefing outlines the Court's findings on these issues before considering the wider implications of the judgment. **How did the dispute arise?** Cryptopia was a cryptocurrency exchange that enabled account holders to trade pairs of cryptocurrencies among themselves. It maintained a database listing the account holders and their digital assets held on the exchange (in the form of digital "wallets" or accounts). Cryptopia charged fees for trades, deposits, and withdrawals made by account holders. The account holdings within digital wallets were protected by encryption, with Cryptopia exclusively holding the private keys to the digital wallets (account holders did not have access to the private keys). Despite such protection, in 2019 Cryptopia's servers were hacked and approximately NZ$30 million of cryptocurrency from account holder

wallets was stolen, using the private keys.

Cryptopia's shareholders placed the company into liquidation and the liquidators applied to the Court for guidance on two questions relating to the categorisation and distribution of assets in the liquidation:

- Is cryptocurrency "property" for the purposes of section 2 of New Zealand's *Companies Act 1993*, capable of forming the subject matter of a trust?
- Was the cryptocurrency in fact held on trust by Cryptopia for the account holders?

Essentially the dispute was a contest between the account holders and the unsecured creditors (and potentially the shareholders) as to whom was entitled to distribution of the remaining assets of the business.

Were cryptocurrencies property?

The account holders argued that cryptocurrencies must be seen as a form of intangible personal property *both* at common law and within the definition in section 2 of New Zealand's *Companies Act 1993* (the relevant statutory provision in terms of the pool of assets available for distribution on liquidation).

Section 2 of New Zealand's Companies Act 1993 defines "property" as:

"[P]roperty of every kind whether tangible or intangible, real or personal, corporeal or incorporeal, and includes rights, interests, and claims of every kind in relation to property however they arise."

The Court held that all of the various cryptocurrencies at issue were "property" within the definition in section 2 of New Zealand's *Companies Act 1993* "and also probably more generally" (i.e. at common law).

This briefing does not consider the Court's reasoning in relation to the *Companies Act* definition of property, but focuses on the reasons the Court gave for its conclusion on the position at common law. Specifically, in reaching such conclusion, the Court relied on Lord Wilberforce's opinion in the House of Lords in the English case of *National Provincial Bank Ltd v Ainsworth* [1965] AC 1175 (HL) at 1247–1248, where he said:

"Before a right or an interest can be admitted into the category of property, or of a right affecting property, it must be definable, identifiable by third parties, capable in its nature of assumption by third parties, and have some degree of permanence or stability."

The Court in *Ruscoe* was *"satisfied the criteria for Lord Wilberforce's definition of 'property' were clearly met in this case."* This was because:

- **Identifiable subject-matter:** the Court considered that this requirement was met because "computer-readable strings of characters recorded on networks of computers established for the purpose of recording those strings … are sufficiently distinct to be capable of then being allocated uniquely to an account

holder on that particular network. For the cryptocurrencies involved here, the allocation is made by what is called a public key – the data allocated to one public key will not be confused with another. This is the case even though the identical data is held on every computer attached to the network";

- **Identifiable by third parties:** the Court was also "satisfied here that cryptoassets clearly meet this criterion. On this aspect, it has long been recognised by property lawyers that the power of an owner to exclude others from an asset provides a more important indicator of ownership than the power actively to use or benefit from that asset." On the facts of the current case, "the degree of control necessary for ownership (namely the power to exclude others) is achieved for cryptocurrencies by the computer software allocating to each public key a second set of data made available only to the holder of the account (the private key), and requiring the combination of the two sets of data in order to record a transfer of the cryptocurrency attached to the public key from one account to another";
- **Capable of assumption by third parties:** the Court held that this criterion was met too – cryptocurrencies had the two characteristics of property relevant to this criterion. That is, that property is: (1) "by its nature to be concerned with legal rights that affect strangers to bilateral transactions"; and (2) "normally, but not always, an asset recognised by the law as an item of property will be something which is potentially desirable to third parties such that they would want themselves to obtain ownership of it"; and
- **Some degree of permanence or stability:** the Court held that this criterion was also satisfied. Referring to the fact that, on a blockchain, a cryptocurrency is transferred by the digital destruction of an existing asset in the hands of the transferor and by the creation of a new one in the hands of the transferee, the Court noted that there "will be situations where the short life of an asset is the result of the deliberate process of transferring the value inherent in the asset so that one asset becomes replaced by another. [C]ryptocurrencies work in this manner but it is also true that bank payments use a similar process which is simply native to the type of property in question. This is not inimical to the asset's status as property."

The Court was therefore satisfied that cryptocurrencies met the standard criteria outlined by Lord Wilberforce so as to be considered a species of "property":

"They are a type of intangible property as a result of the combination of three interdependent features. They obtain their definition as a result of the public key recording the unit of currency. The control and stability necessary to ownership and for creating a market in the coins are provided by the other two features – the private key attached to the corresponding public key and the generation of a fresh private key upon a transfer of the relevant coin."

Pure information versus digital assets

The liquidators in *Ruscoe* had argued that information is not generally recognised as a form of "property" and cryptocurrencies might be said to be a form of information. Referring to English authorities on the point,[1] such argument - the Court explained - was based on the view that neither the common law nor equity recognised property in "information", and cryptocurrencies are said to be merely digitally recorded information.

The Court took the view that, whether or not this was the definitive position at common law, cryptocurrencies were not, in any event, pure information:

- the Court noted that "the whole purpose behind cryptocurrencies is to create an item of tradeable value not simply to record or to impart in confidence knowledge or information"; and
- pure information can be infinitely duplicated. This, the Court said, was not true of cryptocurrencies, "where every public key recording the data constituting the coin is unique on the system where it is recorded. It is also protected by the associated private key from being transferred without consent."

Moreover, referring to a number of New Zealand authorities dealing with computer data and electronic information,[2] the Court said that the New Zealand courts "have accepted that the orthodox position that information is not 'property' does not attach to cases involving digital assets. [D]igital files were seen as 'property' by distinguishing them from 'pure information'."

While it is still too early to say so definitively, it is possible that, in having to consider: (1) where new technologies lie within the orthodox legal categorisations of property; and (2) the reality that electronic data has enormous value in commercial dealings, courts in the common law world may increasingly feel compelled to begin to draw distinctions such as those made in *Ruscoe*. There a distinction was drawn between digital files / digital assets (property) and pure information (not property). Perhaps we may soon see that kind of judicial pragmatism in other jurisdictions too.

For example, the English Court of Appeal in *Fairstar Heavy Transport NV v Adkins & Anor* [2013] EWCA Civ 886 said as early as 2013 that it "would be unwise … for this court to endorse the proposition that there can never be property in information without knowing more about the nature of the information in dispute and the circumstances in which a property right was being asserted. Some kinds of information, such as non-patentable know-how, are more akin to property in their specificity and exclusivity than, say, personal information about private life."[3]

Was there a trust?

Having found that the cryptocurrencies were property, it followed, the Court in *Ruscoe* said, that they are capable of forming the subject matter of a trust.

Did such a trust in favour of account holders arise on the facts? The Court held that the three elements required to give rise to a trust were

met:

- **Certainty of subject matter:** This element was satisfied because the subject matter of the various trusts (being the cryptocurrencies) was clearly recorded in Cryptopia's database.
- **Certainty of objects:** The Court found that there was no uncertainty as to whom the beneficiaries of the relevant trusts were. They were those account holders with positive balances for the respective currencies in Cryptopia's database.
- **Certainty of intention:** An intention of the settlor to create a trust had been established, the Court found, because Cryptopia had manifested its intent through its conduct in creating the exchange without allocating to account holders public and private keys for the digital assets it commenced to hold for them. The database that Cryptopia created showed that the company was a custodian and trustee of the digital assets.

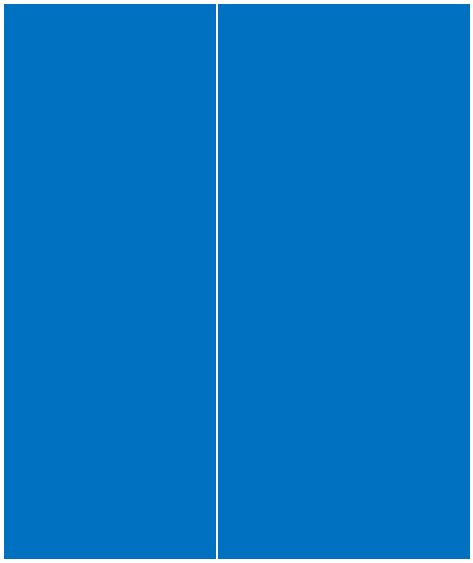
What are the wider implications of the judgment?

The account holders in *Ruscoe* had argued that any finding by the Court that cryptocurrencies were not property would have unsatisfactory implications for the law, including in particular insolvency law, succession law, the law of restitution, and commercial law more generally.

Property is the foundation of many transactions. In the absence of legislation, under common law cryptocurrencies cannot become the subject matter of a trust or a proprietary right of security unless they are recognised as property. "The same is true of a secured creditor or trust beneficiary enforcing their claim in property to the unsecured creditors of an insolvent coin-holder. The development of a viable cryptocurrencies derivative market may sometimes require that the primary assets from which secondary claims are constructed are capable of legal recognition as property."[4]

Similarly, the UK Jurisdiction Taskforce's *Legal Statement on Cryptoassets and Smart Contracts*[5] (cited with approval in *Ruscoe*) observed that "it is important to understand whether the many statutory and common law rules applicable to property apply also to crypto-assets and, if so, how. Of particular significance are the rules concerning succession on death, the vesting of property on personal bankruptcy, the rights of liquidators in corporate insolvency, and tracing in cases of fraud, theft or breach of trust. It would, to say the least, be highly unsatisfactory if rules of that kind had no application to crypto-assets."

Perhaps influenced by such policy considerations, we may soon see more common law decisions following the kind of reasoning in *Ruscoe* in relation to cryptocurrencies and property, and maybe even in relation to other kinds of digital assets more broadly. Whether other jurisdictions take a similar path to this decision remains to be seen. The Court of Appeal of Singapore – the nation's highest court – has expressly not decided whether cryptocurrencies are a type of property, and in England and Wales there is High Court authority to say that cryptocurrencies are property.[6]



Of more significance, longer term though, is the distinction made in the case between pure information and digital files/digital assets in the light of the ascendancy of the importance of data in the commercial arena.

The protection of data has long been problematic for commerce and industry. Intellectual property rights provide very limited protection for machine-generated data, such as that produced from Artificial Intelligence and the Internet of Things (with limited scope for copyright and database rights, and reliance typically having to be placed on the weaker rights of confidentiality/trade secrets law or contractual rights). The possibility that some forms of data may constitute property could have profound implications for the protection and commercialisation of commercial and industrial data.

Date: 5 May 2020

International developments

G20

G20 and the BIS Innovation Hub invite global innovators to find solutions to the most pressing financial regulatory & supervisory challenges

On 29 April 2020, the Saudi G20Presidency and the Bank for International Settlements (BIS) Innovation Hub launched the G20 TechSprint Initiative to highlight the potential for new technologies to resolve regulatory compliance (RegTech) and supervision (SupTech) challenges. The BIS Innovation Hub, through its Singapore Centre, and the Saudi G20 Presidency have published high-priority RegTech/SupTech operational problems and invite private firms to develop innovative technological solutions. The problem statements identify challenges in regulatory reporting, analytics, and monitoring and supervision, and have been developed from submissions received from Financial Stability Board member jurisdictions.

Date: 29 April 2020

Financial Stability Board (FSB)

1. FSB consults on regulatory, supervisory and oversight recommendations for "global stablecoin" arrangements

On 14 April 2020, the Financial Stability Board (FSB) published a consultation paper proposing 10 high-level recommendations that are addressed to national authorities to advance consistent and effective regulation and supervision of global stablecoin (GSC) arrangements. The consultation paper also highlights key international regulatory standards from the Basel Committee, FATF, CPMI and IOSCO that could apply to GSCs.

The recommendations focus on financial regulatory and supervisory issues relating to privately-issued GSCs predominately intended for retail use. Wider issues such as monetary policy, monetary sovereignty, currency substitution, data privacy, competition, and taxation issues are beyond scope.

The proposed recommendations are motivated by GSCs predominantly intended for retail purposes that may pose financial stability risks, but could also apply to stablecoins or other crypto-assets that pose similar risks. The recommendations seek to address the particular governance challenges of a GSC arrangement. They call for regulation, supervision and oversight that are proportionate to the risks, and stress the need for flexible, efficient, inclusive and multi-sectoral cross-border cooperation, coordination and information sharing arrangements that take into account the evolution of GSC arrangements and the risks they may pose over time.

The deadline for comments on the consultation paper is 15 July 2020. The FSB intends to issue a final report in October 2020.

Date: 14 April 2020

2. FSB consults on toolkit of effective practices for cyber incident response and recovery

On 20 April 2020, the Financial Stability Board (FSB) published a consultation report on Effective Practices for Cyber Incident Response and Recovery.

In its consultation report the FSB sets out a toolkit of effective practices that aims to assist organisations in their cyber incident response and recovery activities. The toolkit lists 46 effective practices, structured across seven components:

1. Governance – frames how cyber incident and recovery is organised and managed.
2. Preparation – to establish and maintain capabilities to respond to cyber incidents, and to restore critical functions, processes, activities, systems and data affected by cyber incidents to normal operations.
3. Analysis – to ensure effective response and recovery activities, including forensic analysis, and to determine the severity, impact and root cause of the cyber incident to drive appropriate response and recovery activities.
4. Mitigation – to prevent the aggravation of the situation and eradicates cyber threats in a timely manner to alleviate their impact on business operations and services.
5. Restoration – to repair and restore systems or assets affected by a cyber incident to safely resume business-as-usual delivery of impacted services.
6. Improvement – to establish processes to improve response and recovery capabilities through lessons learnt from past cyber incidents and from proactive tools, such as tabletop exercises, tests and drills.
7. Coordination and communication – to coordinate with stakeholders to maintain good cyber situational awareness and enhances the cyber resilience of the ecosystem.

The effective practices are meant to serve as a toolkit of options rather than applied in a one-size-fits-all manner, as not all practices are applicable to every organisation or in every cyber incident. The toolkit does not constitute standards for organisations or their supervisors and is not a prescriptive recommendation for any particular approach.

The deadline for comments on the consultation report is 20 July 2020. The final toolkit, taking on board the feedback from the consultation, will be sent to the October G20 Finance Ministers and Central Bank Governors meeting and published.

Date: 20 April 2020

Bank for International Settlements (BIS)

BIS report on how fintech can promote financial inclusion - opportunities and challenges

BIS released the following press release:

Financial technology can spur financial inclusion by facilitating payments, but the opportunities come with challenges, according to a new report by the Committee on Payments and Market Infrastructures (CPMI) and the World Bank.

The report, Payment aspects of financial inclusion in the fintech era, connects fintech innovation with financial inclusion, providing a framework for incorporating and leveraging technological opportunities

to promote access and use of transaction accounts, while also addressing potential challenges.

"Technological innovation has made major inroads into financial services, which has implications for payments and their key role for financial inclusion. While fintech can support improved access to safe transaction accounts and encourage their frequent use, it is not a panacea and there are risks that need to be managed", according to Sir Jon Cunliffe, Chair of the Committee on Payments and Market Infrastructures and Deputy Governor for Financial Stability of the Bank of England.

Fintech can contribute to improved design of transaction accounts and payment products, make them ubiquitously accessible with enhanced user experience and awareness. It can make services more efficient and lower market entry barriers. Still, these benefits bring risks, in terms of operational and cyber resilience, protection of customer funds, data protection and privacy, digital exclusion and market concentration. If not adequately managed, these risks could undermine financial inclusion.

"Incorporating fintech into the PAFI framework will help firms and policymakers extend payments services to the poor, the first step for expanding access to other important services, such as credit and insurance," said Ceyla Pazarbasioglu, Vice President for Equitable Growth, Finance and Institutions (EFI), World Bank Group.

The report builds on the guidance on Payment aspects of financial inclusion (PAFI), issued by the CPMI and the World Bank in 2016. This study outlined seven guiding principles for public and private sector stakeholders and recommended key actions for countries seeking to implement these principles. This was done in a technology-neutral and holistic way and remains relevant in the fintech era.

The new report shows that fintech can be used to underpin access and usage of transaction accounts. Yet it is not without challenges, and if risks are not properly managed, they can undermine financial inclusion. Payment aspects of financial inclusion in the fintech era sets out key actions, helping the relevant stakeholders to strike the right balance between increasing efficiency and ensuring safety.

Date: 14 April 2020

International Organisation of Securities Commissions (IOSCO)

There has been no reported activity.

Committee on Payments and Market Infrastructures (CPMI)

There has been no reported activity.

Basel Committee on Banking Supervision (Basel Committee)

There has been no reported activity.

Financial Action Task Force (FATF)

There has been no reported activity.

World Economic Forum

There has been no reported activity.