FinReg
Davis Polk Insights on Financial Regulation

Davis Polk Blockchain Bulletin: A Cryptocurrency and DLT Newsletter

By The Davis Polk Crypto Team on May 8, 2018

POSTED IN FINTECH

Market Insights

The Problem of Digital Asset Fungibility

There have long been discussions in the digital currency community that the ability to trace bitcoin could gradually erode its fungibility. Notable contributions to this discussion include a widely republished reddit **post** from 2013 that used the *Crawfurd v. The Royal Bank* case (discussed below) to argue against the creation of bitcoin tracking software. *Money and Banking* blogger JP Koning also made substantial contributions to this discussion in his 2016 **post** by using the history of banknotes to reveal a possible future for bitcoin. Given the increased scrutiny of digital currency networks by financial crime enforcement bodies across the world, as well as the substantial influx of market participants, fungibility issues are more likely than ever to move from theory to reality. In this article, we hope to bring these important ideas back into circulation and build on them given developments in this field.

Fungibility describes the quality of a good whose units are effectively interchangeable with any other unit of that good. Fungibility is a desirable quality in a variety of contexts, but it is especially important for any good that is to be used as a currency. This fungible nature of currency has long been recognized in law. For example, an eighteenth century Scottish case, ***Crawfurd v. The Royal Bank***, held that the holder of a banknote takes free of infirmities of title. The court noted that requiring notes to be returned to a victim of theft "would be to render the Notes absolutely useless, and consequently would in a great Measure deprive the Nation of the Benefit of the Banks, which could hardly subsist without the Circulation of their Notes."

Fungibility of a currency can be maintained in one of two ways: Either the units must be exactly identical to each other such that they cannot be feasibly traced or distinguished; or there must be a legal structure that restrains the reasons for distinguishing between units of a good or the legality of doing so (*e.g.*, by providing for a good-faith purchaser exception to the rule that a buyer of a stolen good cannot take good title, or by requiring banks to accept all valid banknotes at face value). The first approach seems simple, but in practice it can be quite difficult to maintain. Seemingly identical goods can be marked, and basic accounting methods such as last-in, first-out ("**LIFO**") or first-in, first-out ("**FIFO**") can provided a means for tracing currency. There are also benefits to tracing—serial numbers on paper money help monitor for illegal activity.

The second approach allows for goods to be traced without sacrificing fungibility, but is no less hard-won, as it requires government action and support of the good as a currency. The history of the U.S. financial system provides an excellent example of using government regulation to ensure currency fungibility. During the early to mid-19th century, banking regulations prevented note-issuing banks from forming out of state branches, but notes could still be widely circulated. Due to the expensive and risky process of handling these notes and shipping them back to the issuing bank for redemption, it was common for banks to discount non-local notes as a form of transaction fee. This practice led to the publication of "banknote lists" that would provide recommended discounts for bank notes from around the country. It took the establishment of the national banking system through the National Bank Acts of 1863 and 1864—which, among other things, required all national banks to accept each other's notes at par—to establish a fungible national currency.

How do bitcoin fare as currency under this analysis? While bitcoin are fungible at first glance, the fact that the ledger is public means that bitcoin can be traced. (Technically, only total bitcoin inputs and outputs are public, but individual bitcoin can be traced by imposing an accounting convention such as LIFO or FIFO—indeed, such a method is necessary for bitcoin holders to track their tax basis in bitcoin purchased at different times.) Traceability erodes fungibility because it allows prospective purchasers to discriminate against bitcoin based on the particular bitcoin's transaction history in light of any legal risks associated with holding "tainted" currency, and the legal framework protecting fungibility of fiat currency does not clearly apply to bitcoin. For example, a merchant considering accepting bitcoin as payment may worry about exposing itself to conversion tort liability if the bitcoin were previously stolen. The merchant also may worry about the possibility that a digital asset exchange would refuse to exchange the tainted bitcoin for fiat currency on anti-money laundering or economic sanctions grounds. The publication of bitcoin address "blacklists," such as the one currently being considered by **OFAC**, and by the development of **tools** that facilitate bitcoin tracking, may help law enforcement seeking to police money laundering and other illegal activity, but also may severely limit the utility of bitcoin as a currency.

A possible future for bitcoin is one in which the old banknote lists return in 21st century form—bitcoin from a particular address would be graded based on its transaction history and relative distance from flagged transactions or blacklisted addresses. For example, as generally described by JP Koning, Grade A bitcoin would be "fresh" bitcoin, purchased directly from a miner and would trade at a premium. Grade D bitcoin, meanwhile, may have passed through a blacklisted address and trade at a significant discount. In between are bitcoin that are not closely associated with a blacklisted address or that have been "cleaned" by passing through a bitcoin mixing service that makes tracing more difficult. Such grading schemes could easily become enormously complex given that bitcoin easily moves across borders, and various jurisdictions could have overlapping or inconsistent blacklists, tort laws, AML/KYC requirements, and laws particular to digital assets. This type of regime could lead to a market where any large bitcoin transaction would require a bespoke appraisal. Further, because bitcoin do not go out of circulation, bitcoin will "age," becoming less valuable over time as each transaction makes it more likely that it will pass through a tainted address. All told, fungibility issues could easily become a substantial limiting factor on bitcoin's usefulness as a currency.

The potential solutions for the bitcoin fungibility conundrum track the two methods discussed above for ensuring currency fungibility. The first is a technical solution. Bitcoin could adopt privacy-enhancing features such as those used by Zcash or monero, effectively making it impossible to track bitcoin. Or, the market could simply switch to these more anonymous digital assets. This solution has the obvious drawback of making financial crime harder to detect and making it more difficult for financial institutions to comply with related anti-money laundering and sanctions laws.

The second possible solution is government action. This could take the form of government recognition of bitcoin as a currency and, thus, governed by a legal framework ensuring its fungibility. At present, this seems an unlikely outcome, especially given that such an action would require international cooperation to maintain fungibility across borders. A perhaps more likely version would be a policy of refraining from action that unnecessarily harms bitcoin fungibility, such as publishing blacklisted addresses. Such blacklists may be of relatively limited use for law enforcement purposes, as tech-savvy criminals can easily cycle their bitcoin through more anonymous currencies, while law-abiding bitcoin users could face a tremendous amount of difficulty if they come into contact with tainted coin.

Key Takeaways

- Fungibility is an important feature for a good to be useful as a currency.
- Bitcoin fungibility is in jeopardy due to the ability to trace bitcoin and unclear legal consequences of potentially tainted bitcoin.
- Without government action to facilitate or protect fungibility, worries about the value of aging bitcoin may push users toward adopting anonymization features or more anonymous digital assets.

Squaring Blockchain Technology with Europe's GDPR

In January 2018, at the Eleventh Annual International Conference on Computers, Privacy and Data Protection (the "**Conference**") in Brussels, one **panel** that made some headlines centered around blockchain technology in the context of data protection. The core inquiry of the panel was two-fold: (1) whether blockchain technology can facilitate data protection regulatory objectives and (2) whether the

same technology makes it more difficult to enforce data protection laws. Unsurprisingly, neither inquiry produces a clear-cut answer.

One the one hand, blockchain technology could potentially advance the "privacy-by-design-and-default" principle promulgated by the EU's General Data Protection Regulation ("**GDPR**"), which comes into force on May 25, 2018. But on the other hand, some of the technology's signature features (*i.e.*, immutability and irreversibility) raise concerns related to the dual principles of (1) data minimization and (2) the right to be forgotten, which underpin those same regulations. The inquiry is further muddied by the facts that (1) this discussion speculates about the compliance potential of a ***distributed* technology** in light of regulations that are designed with ***centralization*** in mind, and (2) not all blockchains are created equal—in fact, while they can be grouped into broad categories (for example, public vs. private), the analysis must always be done on a case-by-case basis.

Explaining Blockchain in Data Protection Jargon. As a preliminary matter, let's explain why blockchain technology would even fall within the purview of data protection regulations. Since GDPR is currently considered the gold standard in this realm, we will look to it for key metrics of analysis. Under the GDPR, data protection rules apply only if an entity processes identified or identifiable personal data—that is, data relating to a living natural person. Article 29 Working Party explained in its **Opinion 05/2014 (WP 2016)** that **anonymized data** (*i.e.*, that which irreversibly prevents identification) is not subject to data protection rules—**not pseudonymized data**. In a public blockchain environment, every transaction carried out by a particular user is *linked* to the same encrypted public key. In blockchains where the public key is published, however, the same unreadable hash links the transactions to a particular user, and IP addresses or other metadata could make the user identifiable, thus putting these blockchains within the scope of GDPR. On the other hand, a blockchain such as Hyperledger, one implementation of which is designed to track products or materials in a supply chain, would not fall within the regulatory scope because there is no concern related to personal data.

Self-Sovereign Identity as the Ultimate Solution for Privacy-by-Design? One central tenet of the GDPR is the principle of privacy-by-design, whereby systems are set up to promote privacy and data protection compliance objectives from the start. Blockchain technology was designed, in this sense, to ensure data integrity by being resistant against data corruption. It was also designed to be breach-proof, by

moving from a centralized database model with a single point of failure to a distributed scheme. As one Conference panelist noted, blockchain technology also enables new forms of information-sharing whereby parties to a transaction do not need to reveal any more information about themselves than is absolutely necessary for that particular transaction. For instance, in the context of credential management, individuals can disclose personal data to a trusted authority who would be responsible for issuing attestations of particular attributes (*e.g.*, citizenship, age, address), **without the need** to have the underlying personal data being transferred every time. This could help comply with or take a particular transaction outside the scope of GDPR's strict cross-border data transfer rules (see **GDPR Chapter V and recitals 6, 48, 101-103, 107, 110-115**). As for other opportunities, another panelist noted that blockchain technology presents unique possibilities for GDPR compliance in the areas of (1) notarization of consent, (2) notification of usage of personal data, and (3) real-time information-sharing between a data controller and data processors. Taking this one step further, yet another panelist envisions a future where **self-sovereign identity** enabled by blockchain technology is the only way to be GDPR-compliant.

Can We Forget Immutable Data? The very potential of blockchain technology for ensuring data integrity—by being immutable and non-selective in its preservation—also poses challenges for compliance with key data protection principles. By capturing every transaction and making it publicly visible, the technology inevitably runs afoul of the principle of data minimization enshrined in GDPR Article 5. Because the information cannot be removed once it is recorded, blockchain technology also conflicts with the storage limitation principle. Moreover, Article 17 of the GDPR recognizes a right to be forgotten, or a right to erasure, as some call it. Under this principle, an individual is empowered to request the removal of personal data if it is no longer necessary in light of the original purpose for collection and processing, the data subject withdraws consent, and certain other requirements are met. At the end of the day, whether blockchain technology fundamentally conflicts with the right to be forgotten depends on what "erasure" means, and whether irreversible encryption, revocation of access rights (in smart contracts contexts), or other similar mechanisms could suffice.

Can Distributed Technology Thrive in the Age of Centralized Regulatory Scheme? As Deloitte recently **observed**, in light of the pressure to prepare for GDPR compliance, stakeholders have increasingly engaged in research to make

blockchain mechanisms editable, and prototypes have already been developed in response to the needs of large financial institutions. The irony is apparent, at least with the current proposed prototypes: to maintain the immutability premise of the technology all while complying with data protection rules requires the authority to alter information on the chain to be conferred to a "trusted administrator." In other words, short of having to rely on the consent of a majority of the nodes on the chain to create a new fork, in order for the distributed ledger to comply with the GDPR, the technology has to be reconfigured with a centralized patch. Does this mean that the GDPR is not as technology-neutral or agnostic as some might claim? Designed with notions of a centralized data governance model (*i.e.*, cloud computing and data controller) and with ill-fitting applications for blockchain technology, query whether aspects of the GDPR have already become **outdated** before the Regulation enters into force on May 25, 2018.

Key Takeaways

- Blockchain technology's pseudonymization of personal data approach could bring it within the scope of data protection obligations under the GDPR and other similar regulations.
- The technology's immutable and distributed features present opportunities to advance the notion of privacy-by-design-and-by-default. These features could also be leveraged to circumvent the need to transfer personal data for purposes of authentication via a credential-granting mechanism, and make data protection rules inapplicable.
- The same features, however, could also create challenges for the right to be forgotten and data minimization principles under the GDPR.
- Stakeholders have identified a regulatory-compliant fix in centralizing the authority to edit information on certain blockchains. This and similar approaches could be perceived as threats to the core identity of the technology and begs the question of whether the GDPR and other similar data protection schemes are fundamentally incompatible with a decentralized technology like the blockchain.

Litigation

Nano/XRB Securities Class Action Lawsuit

Investors in the XRB, a cryptocurrency developed by the company Nano, have filed a **class action lawsuit** in federal court in the Eastern District of New York, alleging that Nano and its employees violated federal securities laws by failing to register its initial coin offering ("**ICO**") for XRB, which plaintiffs argue is a security, with the SEC. Plaintiffs also allege that Nano misled them about the safekeeping of their assets in an Italian cryptocurrency exchange called BitGrail and that, as a result, investors lost $170 million worth of XRB when the tokens "disappeared" from the exchange.

***Unregistered Securities Offering*.** One of the key allegations made in the Nano suit is that the XRB ICO constituted an unregistered offering of securities. While there is as of yet no definitive ruling about what types of digital asset tokens constitute securities under U.S. federal securities law, the SEC concluded in its July 2017 report pursuant to Section 21(a) of the Exchange Act analyzing digital tokens distributed by The DAO, and in its December 2017 order instituting cease-and-desist proceedings against Munchee Inc., that at least some distributions of digital tokens constitute illegal securities offerings. Subsequent enforcement actions brought by the SEC and statements by SEC officials have reinforced this position.

Consistent with the Commission's approach in the DAO report and Munchee case, the plaintiffs in the Nano suit apply the four-pronged *Howey* test, according to which an asset constitutes an "investment contract" and, thus a security, if it involves (1) an investment of money, (2) in a common enterprise, (3) with the expectation of profits, (4) to come solely from the efforts of others. Plaintiffs allege that they "invested funds and assets to stake and trade XRB," that they "were investing in a common enterprise with [Nano]," and that "the success of XRB . . . was entirely reliant on [Nano's] ability to maintain and expand the functionality of XRB."

While this is not the first lawsuit by ICO investors to allege that an ICO-gone-wrong was, in fact, an illegal offering of securities, we believe that there are likely many more such actions to come. It appears that private litigants are not waiting for more

detailed guidance from the SEC to determine whether ICO tokens pass the *Howey* test, and thus we are likely to see courts start to take up this issue.

***BitGrail Exchange*.** Plaintiffs in the Nano case also allege that Nano negligently misrepresented that "BitGrail had in place adequate security measures to properly safeguard BitGrail accountholders' assets." As a result, the plaintiffs claim, approximately $170 million worth of XRB was stolen from their BitGrail accounts due to a lack of security features in BitGrail's software.

This episode underscores a broader theme in the cryptocurrency space about the importance of wallet security, including for exchanges and other intermediaries that are not involved in issuing ICO tokens but facilitate customer trading or holding digital tokens. Given the immutable nature of distributed ledger transactions, it is extremely difficult for lost, hacked, or stolen funds to be returned to their rightful owners, and for that reason, lack of secure storage for digital asset tokens is likely to be a strong impetus for legal action going forward.

***Rescue Fork*.** Perhaps the most interesting feature of the Nano lawsuit is that plaintiffs are seeking "an order requiring Nano to 'rescue fork' the allegedly missing XRB into a new cryptocurrency in a manner that would fairly compensate [plaintiffs] for each missing XRB and would eliminate all of the 'missing' XRB." Such a "rescue fork" would require the Nano developers to rewrite the code for XRB, in order to create new tokens that would be distributed to the investors who lost their funds stored on BitGrail. Plaintiffs allege, however, that creating this new token would run against the Nano developers' own financial interest because they own a large percentage of the extant XRB tokens, which would lose value as a result of the fork.

This is the first time that plaintiffs in a class action suit have requested this type of relief, and it raises a couple of interesting questions. First, it is not immediately clear what the consequences of a court order requiring developers to implement a rescue fork would be. Would the new forked currency entirely replace XRB, so that all extant XRB would have to be burned? Or would it supplement "classic" XRB and instead replace only the missing BitGrail tokens? How would the value of the new token be calculated or its value manipulated to properly compensate plaintiffs? Additionally, it is also not clear whether, for tokens trading on public blockchains, the community would accept a court-ordered fork, or whether it would continue to value the original copy of the blockchain over the rescue version. One of the core features

of distributed technologies such as cryptocurrencies is that they are not easily amenable to control by centralized authority. The very concept of the rescue fork represents an interesting and untested challenge to that model.

Key Takeaways

- The Nano lawsuit represents a continuing trend of litigation asserting that ICOs are illegal, unregistered securities offerings under federal securities law.
- The allegations regarding the missing tokens from BitGrail wallets underscore the need for wallet security, including to protect against legal action.
- The concept of the "rescue fork" sought by plaintiffs in this case represents an interesting and untested approach to relief in crypto-litigation.

Regulatory Developments

SEC Reconsidering Bitcoin Futures-Backed ETFs

On March 23, 2018, the SEC issued an **order** instituting proceedings to determine whether it will approve a proposal by NYSE Arca to list two ProShares-sponsored bitcoin futures-backed exchange-traded funds ("**ETFs**"). On April 5, 2018, the SEC published a **second order** instituting proceedings relating to a rule change proposal by Cboe BZX Exchange, Inc. that would allow for the listing of two GraniteShares-sponsored ETFs that invest in Bitcoin futures contracts.

The Cboe Order and NYSE Arca Order ask for comments on many of the same issues. The Orders institute a new period of review for such products, and they request comment from the public, focusing on twelve areas of interest. These areas include concerns relating to (1) such ETFs' investment practices, (2) the underlying spot and futures markets for bitcoin, and (3) how such markets may in turn affect ETFs that invest in Bitcoin futures. For example, the SEC requests comments on the ETFs' valuation policies (*e.g.*, how would such policies account for the possibility of a **hard fork**), including how such policies relate to the underlying bitcoin spot markets, their potential for manipulation and what, if any, effect these factors could have on the ETFs' net asset value. In addition, the SEC asks for comments on

liquidity issues (*e.g.*, whether the futures contracts' relatively high margin requirements present issues for the Bitcoin futures ETFs to meet redemption requests).

The Orders seem to represent a restart of the SEC's review process for bitcoin-related investment products. The original NYSE Arca rule change proposal for the two Proshares bitcoin ETFs was filed in December 2017. In January 2018, the SEC extended its review of that proposal. And, also in January 2018, the SEC's Division of Investment Management published a **letter** in which SEC Staff (1) outlined several concerns[1] that sponsors would be expected to address before the SEC would consider granting approval for funds holding "substantial amounts" of cryptocurrencies or "cryptocurrency-related products" and (2) requested that proposed Bitcoin futures-backed ETFs withdraw their applications. With the Order, it now has instituted formal review proceedings and is seeking public comment.

Key Takeaways

- The SEC is considering the approval of rule changes submitted by NYSE Arca and Cboe BXZ Exchange that would permit them to list ETFs backed by Bitcoin futures contracts, after a January 2018 request that all proposed Bitcoin futures-backed ETFs withdraw their applications.
- The SEC is requesting comments from the public that focus on twelve areas of interest, including concerns relating to (1) such ETFs' investment practices, (2) the underlying spot and futures markets for bitcoin and (3) how such markets may in turn affect ETFs that invest in Bitcoin futures.

SEC Files Suit Against AriseBank

On January 25, 2018, the SEC filed a **complaint** in the U.S. District Court for the Northern District of Texas Dallas Division charging AriseBank (a/k/a AriseBank Ltd. and AriseBank Foundation, LLC) with violating Sections 5(a), 5(c) and 17(a)(2) of the Securities Act of 1933, Section 10(b) of the Securities Exchange Act of 1934 and Rule 10b-5 under the Exchange Act. The Complaint also charges the AriseBank's co-founder and chief executive officer and its other co-founder and chief operating officer with aiding and abetting those violations. On February 2, 2018, the SEC filed an amended complaint adding additional allegations against the

defendants. The SEC obtained an emergency temporary restraining order and asset freeze against AriseBank and court order freezing the assets of the defendants and appointing a receiver over AriseBank before the company closed on its initial coin offering ("**ICO**").

As alleged in the complaint, AriseBank began raising money through an ICO of its digital currency, AriseCoin, as early as November 2017. The complaint explains that in conjunction with its ICO, defendants first issued an abridged whitepaper signed by the CEO in October 2017 and then distributed one or more longer versions, signed by the CEO and COO in November and December 2017. The complaint states that prospective investors could purchase AriseCoin with various virtual currencies and U.S. dollars on AriseBank's website.

The SEC alleges that AriseBank marketed the AriseCoin ICO as the largest ICO ever launched and claimed in a press release issued on January 18, 2018 that it had raised $600 million. The complaint states that, in its marketing materials, AriseBank claimed to have developed an algorithmic trading application that would automatically make trades in various cryptocurrencies in each customer's account, thus generating daily profits. A portion of these profits, according to AriseBank, would be paid to AriseCoin holders in a different, expiring cryptocurrency called eACO, which would be minted daily based on the collective gains of AriseBank customers. AriseBank's marketing materials described how eACO holders would then be incentivized to spend the cryptocurrency before it expired, thus driving the overall circulation of AriseCoin in the market and further increasing its value.

The SEC charged the defendants with violations of the registration and antifraud provisions of the federal securities laws. Additionally, the SEC alleged that the defendants violated Section 10(b) of the Exchange Act and Rule 10b-5 for making untrue statements of a material fact and omitting to state a material fact necessary to make such statements not misleading. For example, the complaint alleges that AriseBank falsely claimed to have acquired a 100-year-old FDIC-insured bank and could offer its customers FDIC-insured accounts and transactions; that AriseBank falsely claimed to offer an AriseBank-branded VISA card that allowed customers to spend any of 700 cryptocurrencies on goods and services; that AriseBank failed to disclose the criminal background of its CEO in the public biographies section of its website, including the fact that he was charged with felony theft and tampering with government records and remains on probation for those charges; and that

AriseBank fabricated a relationship with Kelvin Spencer, whom it held out to potential investors as its President.

While the alleged conduct in this case appears to be extreme, the case serves as an important reminder for ICO issuers and intermediaries involved in these markets that the SEC will look to all aspects of, and communications made in connection with, an ICO in determining whether to bring charges under federal securities laws. Market participants will be well-served to carefully vet information included in white papers, provided to potential investors otherwise, and posted on websites to ensure accuracy and consistency.

Key Takeaways

- The SEC obtained an emergency temporary restraining order, asset freeze and other expedited relief to halt an ICO claiming to have raised approximately $600 million from investors.
- This enforcement action serves as a reminder to market participants to carefully vet information disseminated in connection with an ICO that may be a securities offering.

Regulatory Developments Around the World

Below is a snapshot of recent blockchain and crypto-related news from around the world.

European Union

Twenty-two European countries—including the United Kingdom, France, Germany, Norway, Spain and the Netherlands—signed a declaration on April 10, 2018 establishing the European Blockchain Partnership. According to the **European Commission**, the decentralized and collaborative nature of blockchain is conducive to fostering the digital Single Market. The aims of the partnership include avoiding fragmented approaches across EU member states, ensuring interoperability and wider deployment of blockchain-based services across the EU and ensuring that blockchain-based services are in full compliance with EU laws.

India

The Reserve Bank of India ("**RBI**") **stated** on April 5, 2018 that entities under its regulation "may not deal with or provide services to any individual or business entities dealing with or settling [virtual currencies]." RBI issued a **circular** the next day clarifying that services facilitating an entity in dealing or settling virtual currencies include:

- maintaining accounts;
- registering;
- trading;
- settling;
- giving loans against virtual tokens;
- accepting virtual tokens as collateral;
- opening accounts of exchanges dealing with virtual currencies; and
- transferring or receiving money in accounts relating to the purchase or sale of virtual currencies.

Entities already dealing in virtual currencies or providing the above services will have to stop engaging in such activities within three months from the date of the circular (April 6, 2018).

Japan

The Center for Rule-making Strategies in Japan, a government-funded research group, issued **proposed guidelines** for the legalization of initial coin offerings ("**ICOs**"). The proposed guidelines include identifying investors to prevent money laundering, establishing protections for shareholders and debt holders, restricting unfair trade practices (such as insider trading) and ramping up cybersecurity efforts.

Mexico

Mexico's national digital strategy coordinator Yolanda Martinez **announced at a tech conference** that the Mexican government has been working on a project to

track bids for public contracts using blockchain. The blockchain would store records of bidding processes, allowing for audits after the fact. Martinez touted the project as a means of reducing public corruption and increasing transparency in the public tender process.

United Kingdom

The Financial Conduct Authority ("**FCA**") released a **statement** on April 6, 2018, warning that firms offering cryptocurrency derivatives require authorization from the FCA. The FCA stated, "it is likely that dealing in, arranging transactions in, advising on or providing other services that amount to regulated activities in relation to derivatives that reference other cryptocurrencies or tokens issued through an [ICO], will require authorization by the FCA." The FCA noted that cryptocurrency derivatives include cryptocurrency futures, cryptocurrency contracts for differences and cryptocurrency options. The regulator further warned firms offering cryptocurrency derivatives that they must comply with all rules in the FCA's Handbook and any relevant provisions in applicable EU regulations.

Taiwan

Taiwan's Ministry of Finance **announced** on April 10, 2018 that it will push for the application of existing AML rules to cryptocurrencies. The Ministry's announcement follows numerous meetings with financial regulators and law enforcement agencies, including its central bank and the Financial Supervisory Commission, as well as with domestic cryptocurrency exchanges. The ministry will propose a draft ruling to Taiwan's executive branch as a next step.

If you have any questions regarding the matters covered in this publication, please contact any of the lawyers listed below or your regular Davis Polk contact.

Avi Gesser	**+1 212 450 4181**	**avi.gesser@davispolk.com**
Jai R. Massari	**+1 202 962 7062**	**jai.massari@davispolk.com**
Byron B. Rooney	**+1 212 450 4658**	**byron.rooney@davispolk.com**
Zachary J. Zweihorn	**+1 202 962 7136**	**zachary.zweihorn@davispolk.com**
Trevor I. Kiviat	**+1 212 450 3448**	**trevor.kiviat@davispolk.com**
Jennifer Lin Ricci	**+1 212 450 4823**	**jennifer.ricci@davispolk.com**
Chad Richman	**+1 212 450 3420**	**chad.richman@davispolk.com**
Zachary B. Shapiro	**+1 212 450 3451**	**zachary.shapiro@davispolk.com**
Mengyi Xu	**+1 212 450 3559**	**mengyi.xu@davispolk.com**