IFRS (#)

Accounting for crypto-assets

EY

Building a better working world

Contents

1

Introduction

Crypto-assets experienced a breakout year in 2017. Cryptocurrencies, such as bitcoin and ether, have seen their prices surge as the public's awareness has increased, and financial market participants have thus increasingly turned their attention to the phenomenon. Simultaneously, a wave of new crypto-asset issuance has been sweeping the start-up fundraising world, sparking the interest of regulators in the process.

Accountants have thus far been notable by their relative absence from that narrative. Perhaps, most notable is the fact that the Australian Accounting Standards Board (AASB) has submitted a discussion paper on "digital currencies" to the International Accounting Standards Board (IASB), and the Accounting Standards Board of Japan (ASBJ) has issued an exposure draft for public comment on accounting for "virtual currencies".[1] In addition, the IASB discussed certain features of transactions involving digital currencies during its meeting in January 2018, and will discuss in future whether to commence a research project in this area.[1]

This also highlights the lack of a standardized crypto-asset taxonomy, which makes it difficult to determine the applicability of standard setters' published perspectives. Furthermore, due to the diversity and pace of innovation associated with crypto-assets, the facts and circumstances of each individual case will differ, making it difficult to draw general conclusions on the accounting treatment.

Despite the market's increasingly urgent need for accounting guidance, there have been no formal pronouncements on this topic to date.

In this report, we aim to first briefly introduce cryptocurrencies and other types of crypto-assets. Then, we discuss some of the recent activities by accounting standard setters in relation to crypto-assets.

This structure highlights the fact that dealing with crypto-assets requires a detailed understanding of the technical intricacies of distributed ledger technology (often referred to as blockchain) on one hand, and relevant accounting concepts on the other.

However, we do not aim to specifically address the merits and potential of the underlying blockchain technology here. For that, we would recommend consulting the recent EY-sponsored **Global blockchain benchmarking study**.
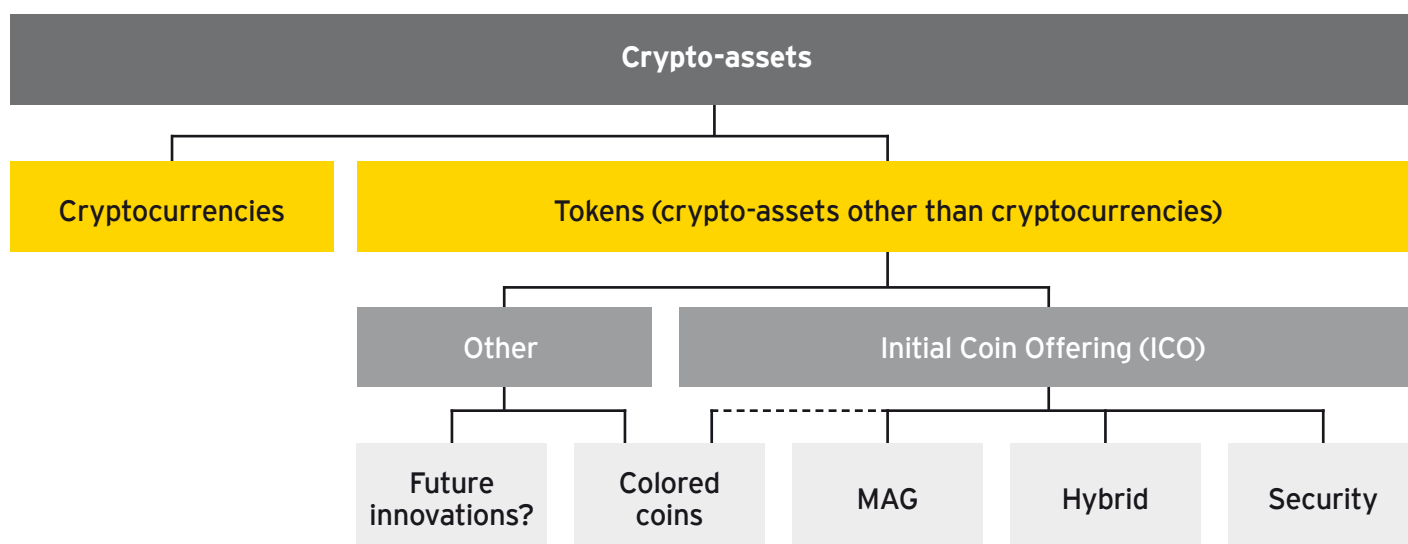
2

What are crypto-assets?

Crypto-assets are digital assets recorded on a distributed ledger. They derive their name from the cryptographic security mechanisms used within public, permission-less distributed ledgers. In many cases, they pose a challenge to established beliefs about money, economic relationships and investing, thereby also raising questions about their appropriate financial reporting.

Cryptocurrencies, such as bitcoin and ether, constitute the earliest and best-known examples of crypto-assets, but the space continues to grow and evolve, producing new types of assets that are commonly called tokens.

In such a fast-moving environment, it is difficult to create any lasting taxonomy of crypto-assets. For the purposes of our analysis, we deliberately have shown below a distinction between cryptocurrencies and non-cryptocurrency tokens. We do so in full acknowledgment of the fact that all crypto-assets may commonly be referred to as "tokens" and a hard boundary between our two categories may at times be difficult to draw. We elaborate further on these definitions in the relevant sections below.

Crypto-assets					

Crypto-assets

Cryptocurrencies — **Tokens (crypto-assets other than cryptocurrencies)**

Under Tokens:
- **Other**
  - **Future innovations?**
  - **Colored coins**
- **Initial Coin Offering (ICO)**
  - **MAG**
  - **Hybrid**
  - **Security**

2.1. Cryptocurrencies

The word "cryptocurrencies" is often used as a blanket term for all crypto-assets. However, we use it specifically to mean those crypto-assets that are meant to constitute a peer-to-peer alternative to government-issued fiat currency; a general-purpose medium of exchange independent of any central bank. These were the first types of crypto-assets to emerge, rising to prominence with the launch of Bitcoin in 2009.

2.1.1. Bitcoin

Bitcoin was one of the first cryptocurrencies, fostered at the height of the global financial crisis by a libertarian community deeply distrustful of governments and central authorities. It has spawned many imitators, but remains the leading cryptocurrency by market capitalization.

In the Bitcoin blockchain, anyone can view the ledger which records ownership of bitcoins and transact upon it. Privacy is thus achieved only through pseudonymity, i.e., a lack of connection between the Bitcoin address and an identifiable legal or natural person.[2]

Crucially, anyone with sufficient computing power can participate in the validation of transactions by using one's computer to solve complex cryptographic equations. The equation solutions enable "blocks" of transactions to be added to the "chain" in return for newly "mined" bitcoins. There is no need for mutual trust or central authority (e.g., a bank) to enforce rules and maintain the "golden source" of transactions. Each computer maintains, or has access to, a full record of every transaction since the blockchain's inception. Whenever a transfer of bitcoins is made, this public record is used to verify availability of funds and the new transaction is encoded into the consensus ledger through the mining process described above. Therefore, the ledger is virtually immutable. There is almost no risk of fraud or manipulation in participant-to-participant transactions on the blockchain itself (though there may be when trading the asset, and there is also potential for market manipulation or theft of private keys, for example).

Bitcoin is specifically designed as a currency and payment system, but it is worth pointing out that in a public, permission-less distributed ledger, it is customary to offer a form of on-chain value to incentivize transaction validation.

In the Bitcoin blockchain, this incentive currently takes the form of not only transaction fees, but also newly-mined bitcoins. When every block is mined, the miner receives a predetermined amount of bitcoin, but the supply of bitcoins is actually finite by design. Once the last bitcoin is mined, the system will switch to an exclusively transaction fee-based incentive. This forms part of the allure of Bitcoin to the libertarian crypto community. Its finite, deflationary money supply can be likened to a digital gold standard.

In spite of that principle, it is important to note that Bitcoin is dynamic rather than static. The reference implementation code is open source, i.e., it is managed and updated by volunteers who must achieve consensus among nodes for a change to be adopted. The Bitcoin community has continuously advocated for more widespread adoption, and has even made changes to the Bitcoin blockchain to that end. Over the course of 2017, this created philosophical divisions in the community over the future direction of the technology, pitting adherence to founding principles against increased acceptance by the mainstream.

One such division led to the August 2017 "hard fork" (i.e., backward-incompatible system upgrade) that created two competing versions of the Bitcoin blockchain: one adopted by the majority of users, which is bitcoin (BTC), and a new offshoot labeled Bitcoin Cash (BCH). This highlights the decentralized, consensus-driven nature of the technology.

2.1.2. Ether

Ethereum went live in July 2015, having been funded by a crowd sale not dissimilar to some of today's initial coin offerings (ICOs). It is a decentralized platform similar to an operating system like those found in smartphones; anyone can build applications on top of the platform to perform various tasks. This distinguishes Ethereum from Bitcoin. Bitcoin was designed specifically to be limited to simple logic – as a peer-to-peer electronic cash system. Ethereum supports programming code for any type of decentralized application; its capability is wider. The platform runs smart contracts – computer protocols that enforce or negotiate contracts through code.

Despite its primary function as an enabler of decentralized applications, Ethereum, like any public permission-less blockchain, requires a form of on-chain value to incentivize transaction validation, or in other words pay the machines that execute the operations that build and maintain the ledger. This payment comes in the form of a cryptocurrency called ether.

Ethereum currently functions using a proof-of-work system, much like Bitcoin. In the near future (2018), it is expected to gradually move to a new proof-of-stake consensus algorithm[3] called Casper.

The public Ethereum platform relies on the consensus of its participants in the same way as Bitcoin does, and this has proved equally problematic. There have been multiple hard forks in the Ethereum ledger – in 2014, 2015 and 2016. For a further discussion of hard forks, refer to the "Special situations" section below.

The last fork received widespread news coverage, as it caused a deep divide in the Ethereum community over the decision to return US$50m in stolen Ether to investors in The Distributed Autonomous Organization (the DAO).[4]

The case of the DAO has been useful in furthering the broader public debate on ICOs (discussed within the "Tokens" section on the next page), as it prompted an investigation by the U.S. Securities and Exchange Commission (SEC) into whether ICO tokens (such as those held by investors in the DAO) constitute securities. The SEC released its Report of Investigation in July 2017 stating that the DAO tokens were securities and should thus have been subject to securities laws and regulations.[6]

Proof of work[3]

In a proof-of-work system, network participants compete to be the fastest to solve the cryptographic puzzles required to add a new block to the blockchain. When the puzzle is solved, the machine involved proves that it completed the work, and is rewarded in any given system with a token of value.

Proof of stake[3]

In a proof-of-stake system, a validator must prove ownership of a certain amount of coins in order to participate in transaction validation. The validator's probability of validating the next block is equal to its share of all coins in existence. Transaction fees earned by the validator are paid by the transacting parties.

2.1.3. Other cryptocurrencies

Bitcoin and Ether represent two of the most widely used cryptocurrencies, but many alternatives exist. Examples from the top 10 cryptocurrencies by market capitalization at the time of writing are:

► Bitcoin Cash

► Ripple (XRP)

► Litecoin

These highlight the myriad design choices available within the umbrella of distributed ledger technology – choices that imply trade-offs in terms of functionality, transaction speed, energy consumption, security and trust (or centralization).

2.2. Tokens (crypto-assets other than cryptocurrencies)

We use "tokens" as an umbrella term for a wide variety of crypto-assets. In contrast to cryptocurrency, which is designed as a general-purpose medium of exchange across applications, tokens tend to be designed to support a more narrowly-defined, specific use case of distributed ledger technology. Although cryptocurrencies may also commonly be referred to as "tokens", we deliberately draw the above distinction here, defining the term tokens herein to mean non-cryptocurrency tokens providing something other than purely general-purpose value transfer.

The market's focus has recently been on tokens issued in ICOs, but one should note that other types of tokens exist. An ICO is the process by which some of them are brought to market, but tokens are not necessarily simply a capital-raising tool. We discuss some examples below while acknowledging that new types of tokens may yet be developed.

2.2.1. Ether

In the "Cryptocurrencies" section above, we noted that Ethereum's native cryptocurrency, ether, is necessary to incentivize transaction validation in the network and thereby acts as a medium of exchange similar to bitcoin. Yet, ether also fulfills the role of "crypto-fuel" to run smart contracts, i.e., it is an enabler of decentralized applications built on Ethereum.

This might invite the argument that ether has a specific application and should thus fall under "tokens" as opposed to "cryptocurrencies" within our taxonomy. However, we would emphasize the general-purpose nature of the Ethereum platform, and by extension ether, which contrasts with the more narrowly defined use cases seen among other tokens. This is underscored by the fact that ether is widely used as a means of payment for ICO tokens. It is strongly characterized by its role as a medium of exchange.

Therefore, although we acknowledge the technological distinction between bitcoin and ether, we deem it more appropriate to classify ether as a cryptocurrency for the purposes of an accounting discussion.

2.2.2. Initial Coin Offerings (ICOs)

The term "ICO" evokes the concept of an IPO, i.e., an initial public offering of a company's shares on a stock exchange.

An ICO involves the issuance of new coins recorded on a distributed ledger (virtually always Ethereum).[5] The public decides whether to purchase them on the basis of information set out in a "white paper" published by the issuing developer, among

other considerations. The white paper typically sets out the technical details of the tokens' functionality and explains the value proposition of the system they underpin.

However, the tokens issued in an ICO may or may not be securities, depending on the underlying economic relationships involved. It is crucial to understand that many ICO tokens do not fit the standard investing paradigm at all, which requires preparers of financial information to make unique and complex judgments in relation to their appropriate reporting.

ICOs' ambiguity and novelty also complicate the determination of how to approach them from a regulatory perspective, as many jurisdictions lack codified legislation or legal precedent upon which to base consistent rulings.

2.2.2.1. Securities on a blockchain

Perhaps, the most straightforward form of ICO is one where the tokens issued represent economic interests in the issuing business, such as ordinary shares. That is, the white paper will set out the token holder's right to receive distributions of profit from the activity carried out by the issuing organization (see Figure 1).

Such distributions might be discretionary or subject to a formulaic calculation. Voting rights may or may not be attached to the

tokens, as is the case even for traditional ordinary shares (Snap, Inc. being a recent example of an IPO of shares lacking voting rights). The investor ultimately has the choice of either holding the token to collect the cash flows from the issuer or selling it in the secondary market.

In such a scenario, the ICO is in substance an IPO of shares or debt, i.e., securities, as was recently highlighted by the SEC's ruling in relation to the DAO.[6] The innovation is thus "merely" technological, consisting of the immediate settlement and reconciliation-free record-keeping of transactions facilitated by the distributed ledger. There is likely to be little incremental ambiguity in relation to the appropriate accounting treatment, for both the issuer and the investor, as in the case of a more conventional investment. In essence, the concept is similar to crowdfunding, though perhaps one (thus far) targeting a more technologically literate audience.

An ICO represents an attractive source of financing for a start-up business, as it eschews the cost, time and perceived discomfort involved in obtaining finance through traditional means such as banks, venture capitalists or the stock market. This also benefits investors who can use ICO investments to gain exposure to early-stage investments without paying high management and performance fees to VC funds.

Figure 1: Securities on a blockchain
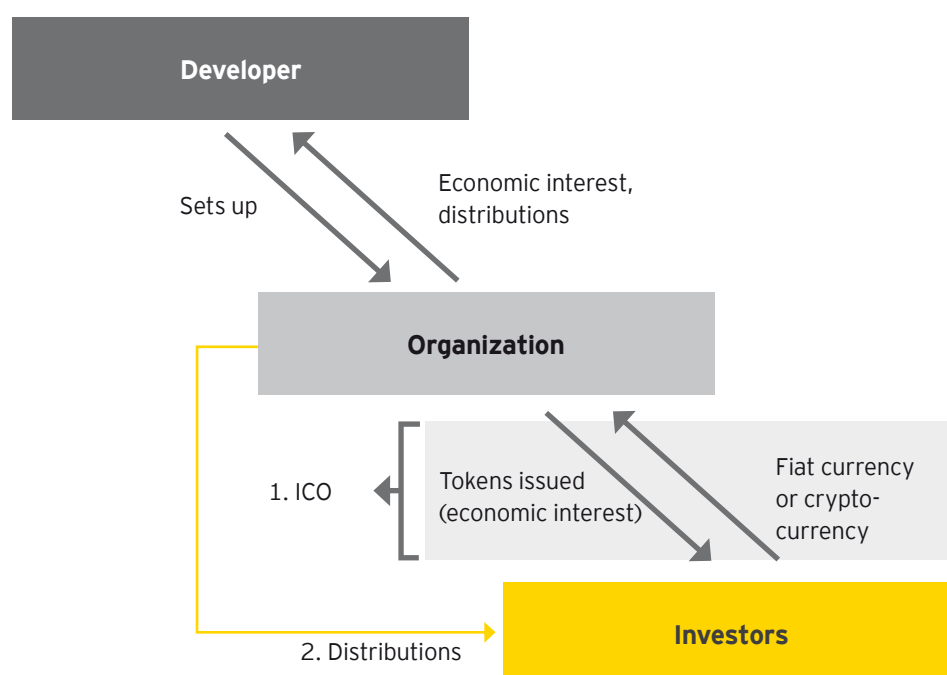
Ultimately, however, this key disintermediation advantage constitutes a pitfall. In most countries, there are strict regulations on not only the marketing and issuance but also the subsequent trading of securities, and ICOs may fall within the scope of these regulations.

In addition to the common risks relating to investment in any early-stage company, risks for investors include the potential failure of the formation of a secondary market and also the prevalence of scam ICOs taking advantage of the hype surrounding crypto-assets and distributed ledger technology. To this end, multiple governments around the world have issued investor warnings around ICOs during the second half of 2017, including the Financial Conduct Authority (UK), Bundesanstalt für Finanzdienstleistungsaufsicht (Germany) and the SEC (US).

2.2.2.2. "Miniature autocratic government" (MAG) tokens

Many ICOs break the mold of financial markets entirely by offering what has come to be known as a "utility token".

This ICO model involves the development of a distributed organization designed to share some resource in a peer-to-peer fashion (e.g., hard drive storage space, Storj being an example of such a system). Here, a developer designs a miniature economy of sorts, in which the token to be issued is to constitute the medium of exchange (e.g., the means of payment for the hard drive storage space).

Figure 2: Miniature autocratic government
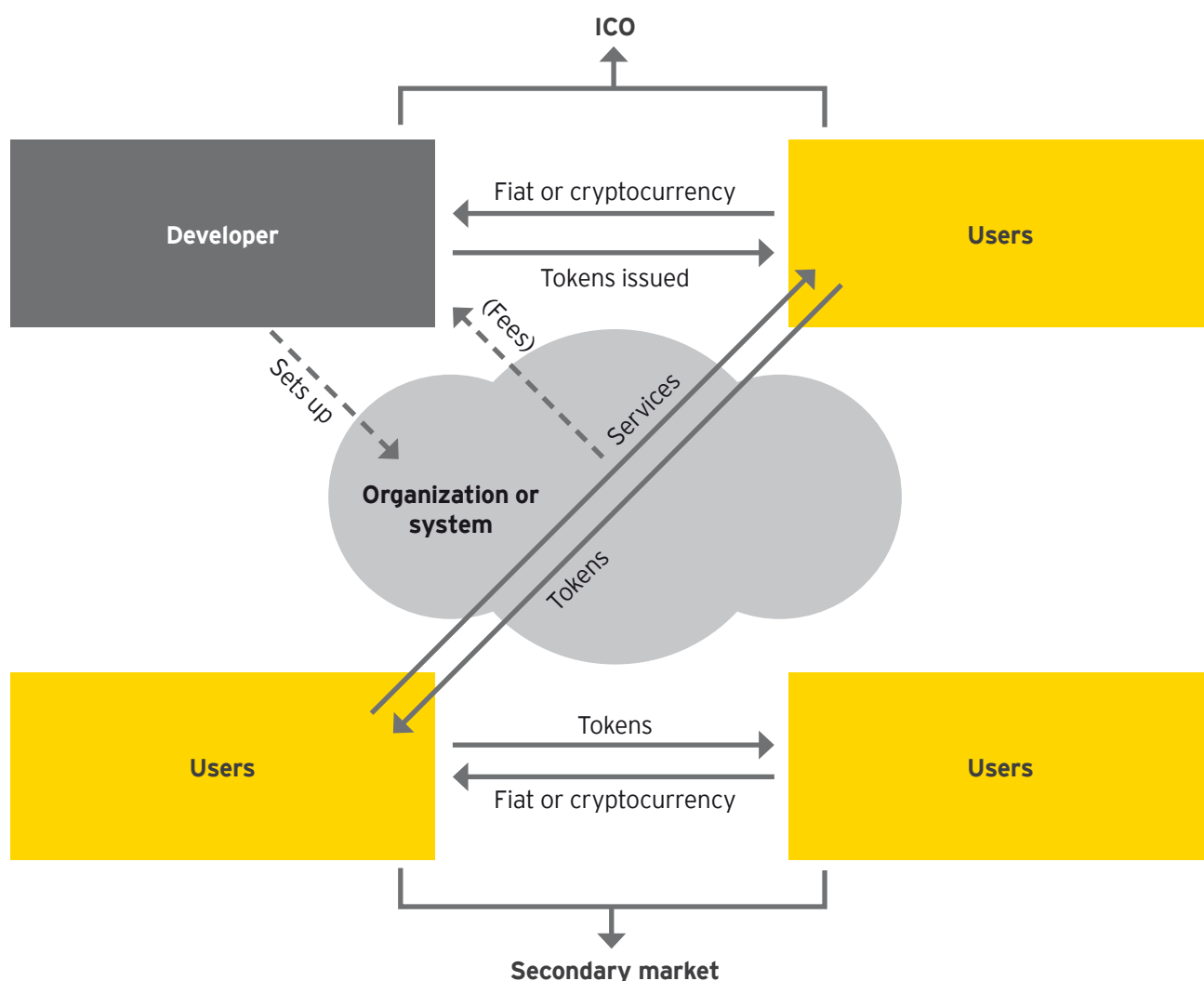
The developer (company) sells tokens in exchange for fiat currency or cryptocurrency, thus earning a return on the resources expended to set the system up. The developer may also earn commissions on transactions involving the tokens, and the proceeds may be further reinvested in the marketing of the system, thereby attracting demand for it and its tokens. For an illustration of this system, please refer to the MAG tokens diagram.

We derive our name for this ICO model from the fact that within it, the developer acts much like, if anything, a miniature autocratic government. Issuance gains can be likened to the seigniorage gains governments earn when they sell banknotes at a premium over the cost of cotton, paper and ink. Transaction commissions, which can be set unilaterally by the developer, function much like taxes. Reinvestment of commissions in the system and its marketing is akin to the roles played by public infrastructure investment and foreign direct investment promotion agencies.

The autocracy assertion stems from the fact that there are no voting rights and, legally, the developer owes nothing to token holders. At the point of issuance, the developer gains the right to the ICO proceeds and can do with them as it wishes. Token holders have no recourse and no right to receive interest or dividends.

Maintaining a miniature autocracy of this kind hinges on the attraction and retention of user demand. This, in turn, depends on the fundamental viability of the value proposition and the ongoing maintenance of user satisfaction. The investment case for MAG token ICOs, thus, builds upon an assessment of anticipated performance against these criteria, with the token price falling at the intersection of a variable demand and finite supply. Price discovery occurs through the secondary market, i.e., through crypto-exchanges, in the same way as for other types of crypto-assets.

2.2.2.3. Hybrids

It is crucial to note that security tokens and MAG tokens represent two ends of a continuum, rather than a binary choice. Ongoing innovation in the crypto-asset space continues to produce hybrid tokens that are part MAG token, part security. Volumes could be written on the variety of technologies observed and approaches taken, but we encourage companies to seek tailored professional advice if they wish to incorporate crypto-assets into their business models.

2.2.3. Colored coins (e.g., Ripple issuances)

A distributed ledger can be used as a platform for maintaining a distributed record of any kind of data. Physical or financial assets, such as gold or stocks, can be "tokenized", i.e., recorded as tokens on a distributed ledger. The aim of this tokenization is to streamline trading through immediate settlement of transactions and the elimination of reconciliation processes.

Details of existing assets can be inscribed into a distributed ledger through the "coloring" of the ledger's tokens. This is technically possible even within the Bitcoin blockchain, but a system exists that has been specifically set up to facilitate it: Ripple.

Ripple is a distributed ledger technologically similar to Bitcoin or Ethereum, but conceptually much less radical. It effectively serves as a system of credit limits and a payment protocol.

"Gateways" on the network operate much like banks. They can issue tokens (colored coins) called "issuances". These issuances are distinguished from Ripple's native cryptocurrency XRP in that they constitute digital IOUs representing any off-ledger asset (preferably a non-perishable, fungible one). Issuances are always tied to a specific issuer, meaning that all currencies, such as euros or US dollars recorded on the Ripple ledger, take the form of issuances tied to a specific "issuing gateway".

Each user sets up "trust lines" to specific parties for specific amounts in specific instruments – effectively a form of counterparty risk management. Even if two users do not trust each other, they can transact as long as a trust path can be found between them, no matter how many gateways are involved. This is the concept of "rippling" payments, essentially a digital version of the hawala network, which has been used as a payment medium in the Arab world for centuries.

If there is no trust line between two parties, the native cryptocurrency, XRP, serves as a trustless fallback medium. This is possible because Ripple requires every gateway to quote XRP prices for any issuance it deals in.

Colored coins are relevant to our discussion of crypto-assets in that they benefit from distributed ledger technology and may, therefore, play a part in the innovation of market infrastructure and processes. However, the fundamental novelty lies not in the substance of these assets, but in the systems used to record and transact them. They can be thought of as "garden variety" crypto-assets.

2.2.4. Future innovations?

As a final note, we should reiterate that we have discussed various examples of tokens above, namely ICO tokens and colored coins. While the latter category is rather broad and could thus be expected to capture many new tokens, we acknowledge that ongoing innovation in the crypto-asset space may produce still other types of tokens in the future. We would therefore highlight that these two broad groups of tokens are not intended to be collectively exhaustive.

3

Accounting for crypto-assets

3.1. Selected activities of standard setters

3.1.1. Overview

Crypto-assets constitute an evolving, fast-growing, but still relatively new, asset class. As a result, there are no specific pronouncements from accounting bodies that deal with the accounting of such assets from the holder's perspective.

The purpose of this section is to provide a summary of selected activities by standard setters. Due to the diversity and pace of innovation associated with crypto-assets, the facts and circumstances of each individual case will differ, making it difficult to draw generally applicable conclusions on the accounting treatment. The accounting for crypto-assets has to be evaluated on the basis of individual fact patterns. However, the perspectives of the standard setters, as shown below, are general in nature and may not be applicable to all crypto-assets. It is further observed that there is currently no standardized definition of crypto-assets and the terminology and, hence, the definitions used by standard setters vary.

3.1.2. Perspectives from the AASB

In December 2016, the AASB released the paper, *Digital currency – A case for standard setting activity*.[1] The AASB examined the current IFRS literature and evaluated whether digital currencies should be accounted for as cash or cash equivalents, financial assets (other than cash), intangible assets, or inventories.

The paper concluded that, at present, digital currencies should not be considered as cash or cash equivalents under IAS 7 *Statement of Cash Flows*.[7] Specifically, it was commented that a digital currency lacks broad acceptance as a means of exchange[8] (at present) and it is not issued by a central bank.[9] In addition, a digital currency is not a financial instrument, as defined in IAS 32 *Financial Instruments: Presentation*, due to the lack of contractual relationship that results in a financial asset for one party and a financial liability for another.[10]

The paper further found that a digital currency meets the definition of intangible assets, as defined in *IAS 38 Intangible Assets*, because a digital currency is an identifiable nonmonetary asset without physical substance. Paragraph 3 of IAS 38 includes a scope exception for intangible assets held for sale in the ordinary course of business. Such intangibles are subject to *IAS 2 Inventories* and, hence, are accounted for at the lower of cost and net realizable value (except for inventories held by commodity broker-traders, as discussed below) rather than using the cost or revaluation model under IAS 38.[11] The paper commented, however, that it is not necessarily clear how "held in the ordinary course of business" should be interpreted in the context of digital currencies more broadly. For example, it is not necessarily clear if entities that accept digital currencies as a means of payment should be considered to hold them for sale in the ordinary course of business.

Furthermore, IAS 2 does not apply to the measurement of inventories held by commodity broker-traders who measure their inventories at fair value less costs to sell and recognize changes in fair value less costs to sell in profit or loss in the period of the change. Broker-traders are those who buy or sell commodities for others or on their own account. However, it is not necessarily clear whether digital currencies should be considered a commodity in the context of IAS 2.

The AASB also notes that there is currently a lack of accounting guidance around intangible assets and commodities held for investment purposes.

The AASB concludes that there is a lack of guidance on digital currencies and that the measurement guidance under IAS 2 and IAS 38 does not provide relevant and useful information to users of financial statements (except for instances where an entity is

considered to be a commodity broker-trader). It proposes that the digital currencies be accounted for at fair value with changes in fair value recognized in profit or loss. Thus, standard setting activity is needed.

The AASB's paper was discussed at the Accounting Standards Advisory Forum (ASAF), a consultative body of the IASB (the Board), in December 2016. It was suggested that the IASB continue to monitor developments in this area.[1]

3.1.3. Research performed by the FASB

The Financial Accounting Standards Board (FASB) noted in the *Report of the FASB Chairman 1 July, 2017 through 30 September 2017*[1] that the FASB staff performed significant research activities on digital currencies. However, the FASB has yet to discuss this research.

3.1.4. Exposure draft issued by the ASBJ

In December 2017, the ASBJ issued for public comment, the Exposure Draft, *Practical Solution on the Accounting for Virtual Currencies under the Payment Services Act*.[1] The public comment period ends in early February 2018.

3.1.4.1. Accounting for virtual currencies held by an entity on its own behalf

According to the Exposure Draft, a holder of virtual currencies as defined by the Payment Services Act,[12] excluding those held by a virtual currency dealer on behalf of its customers, measures the virtual currency at market price at the balance sheet date if there is an active market. Any difference between the market price and the carrying amount is recognized as a gain or loss. If an active market does not exist for the virtual currency, it is measured at the lower of the cost or the estimated disposal value (including zero or a memorandum value). To the extent that the estimated disposal value is used for measurement purposes, the difference between the estimated disposal value and the carrying amount is recognized as a loss, which is not reversible in subsequent periods.

3.1.4.2. Accounting for virtual currencies held by a virtual currency dealer on behalf of its customers

The Exposure Draft states that a virtual currency dealer is required to recognize an asset when a virtual currency is deposited from the customer on the basis of an agreement between the virtual currency dealer and the customer. Upon initial recognition, the virtual currency should be measured using the market price at the date when the virtual currency was deposited. At the same time, a virtual currency dealer is required to recognize the obligation to return the virtual currency to the customer as a liability. The liability is measured at the same amount as the corresponding asset.

At the balance sheet date, a virtual currency dealer is required to measure the virtual currency held on behalf of its customers consistent with the measurement requirement in section 3.1.4.1 Accounting for virtual currencies held by an entity on its own behalf, on the basis of whether an active market exists for that virtual currency. A virtual currency dealer is also required to measure the liability recognized in relation to the virtual currency held on behalf of its customers on the balance sheet at the same amount as the corresponding asset. Accordingly, no gain or loss should arise from virtual currencies held by a virtual currency dealer on behalf of its customers.

3.1.5. Discussion at the IASB

In January 2018, the IASB discussed a number of issues, including transactions such as those involving digital currencies that might form part of a research project to be added to its agenda. The Board will discuss, at a future meeting, whether to add a research project on some or all of these transactions.[1]

3.2. Special situations

3.2.1. Forked currencies (and short-selling)

Certain cryptocurrencies have experienced an event described as a "fork" in the past few years. A fork is a change to the underlying protocol in the relevant blockchain. It requires all nodes connected to the blockchain to update to the new version of protocol software, and adopt that version going forward.

There are currently two possible types of forks. A hard fork and a soft fork. A hard fork changes the protocol code to create a new version of the blockchain, alongside the old version. This also potentially creates new coins. A soft fork is also an update to the blockchain protocol; however, one version (assumed the updated or new version) is supposed to be adopted by the majority and will become the dominant one.

For example, the Bitcoin blockchain has experienced multiple forks. The "Segwit" fork occurred in August 2017 and changed the data stored within each block in order to improve scalability and speed. There were two other forks in 2017 which produced two alternative Bitcoins: Bitcoin Cash (BCH) and Bitcoin Gold (BTG). In these cases, new bitcoins were created and, for example, as a result of the first fork, the holder of each BTC in the "core" blockchain received one BCH for every original bitcoin held.

From a financial reporting perspective, the occurrence of a hard fork can be likened to a spin-off. When a parent spins off its subsidiary by distributing the subsidiary's shares pro rata to investors in the parent, the parent investors record a stock dividend. This is recorded in the holder's financial statements as a new asset (debit) and dividend income (credit). Similarly, if a cryptocurrency is subjected to a hard fork, the holder is left with an existing asset (most likely now worth less than before) and a new asset. Because the relationship is not one of equity ownership, one cannot speak of dividend income. It is probable that, as in the case of Bitcoin and Bitcoin Cash, the existing and new assets will be of the same type and will therefore be classified identically on their holder's statement of financial position. However, it is possible that future forks of different cryptocurrencies will not adhere to this principle.

Another interesting situation arises where an investor holds a short position in a cryptocurrency. There is no way to record short positions in a cryptocurrency directly on the blockchain, and therefore the short position will take the form of a separate contract to sell in the future. That would be akin to a more traditional type of asset and liability to buy or sell a financial instrument. This would typically be an asset or liability as at fair value through profit or loss (FVTPL).

When a fork occurs, the cryptocurrency short-seller's position should be similar to that of a short-seller of an equity instrument, which pays a dividend while the short position is outstanding. Securities lending agreements typically specify that the short-seller shall be liable to not only surrender the share to its owner but also reimburse the amount of the dividend. However, no best practice appears to have been established in this area for cryptocurrency as yet. It is therefore uncertain whether the short-seller has any additional liability in the case of a hard fork.

3.2.2. Token presale (vs. ICO)

A distinction can be drawn between those tokens issued in an ICO at the same time as or after the network or service is launched, and those issued before the launch in a "presale". The Simple Agreement for Future Tokens (SAFT) project by Protocol Labs and Cooley sets out a framework for the use of such future tokens.

The token itself (if a MAG token) does not constitute a security, as discussed elsewhere in this paper. However, a presale involving the agreement to purchase future tokens gives rise to a security according to Cooley and Protocol Labs. The agreement essentially represents a forward contract on the token that is yet to be created. Therefore the contract itself constitutes a security under US law, and would be subject to securities regulation under the SEC (in the US), according to Cooley and Protocol Labs.

It is worth mentioning this distinction in the context of financial reporting because it shows the wide range of legal and regulatory interpretations of different types and structures of tokens. The fact that the industry is growing rapidly means that new and complex structures will be possible, requiring companies to consider up front how they operate in the token space along with legal and accounting implications.

3.3. Conclusion

The nuanced, constantly evolving nature of the crypto-asset phenomenon, coupled with the lack of relevant formal accounting pronouncements, presents complex challenges for preparers of financial information. Underlying economic relationships must be understood in their substance, and the best fit found under existing accounting standards. Dealing with crypto-asset accounting therefore requires a detailed understanding of both distributed ledger technology and relevant accounting concepts. In the absence of further action by accounting standard setters, holders of crypto-assets may be unable to achieve the accounting treatment they consider most appropriate. We caution that each individual situation will require a unique approach, tailored with appropriate professional advice.

4

Supporting details

1. Perspectives from accounting standards boards

"About the Exposure Draft: Practical Solution on the Accounting for Virtual Currencies under the Payment Services Act," *ASB*, https://www.asb.or.jp/en/wp-content/uploads/2017-1206_2_e.pdf, accessed 6 February 2018.

"Digital currency − A case for standard setting activity. A perspective by the Australian Accounting Standards Board (AASB)," *AASB*, http://www.aasb.gov.au/admin/file/content102/c3/AASB_ASAF_DigitalCurrency.pdf, accessed 6 February 2018.

"IASB Update January 2018," *IFRS*, http://www.ifrs.org/news-and-events/updates/iasb-updates/january-2018/, accessed 26 January 2018.

"Summary Note of the Accounting Standards Advisory Forum," *IFRS*, http://www.ifrs.org/-/media/feature/meetings/2016/december/asaf/asaf-summary-dec-2016.pdf, accessed 5 February 2018.

"Report of the Chairman July 1, 2017 through September 30, 2017," *FASB*, http://www.fasb.org/jsp/FASB/Document_C/DocumentPage&cid=1176169470918, accessed 8 February 2018.

2. Of pseudonymity and privacy

There is a prevalent misconception that all transactions on a blockchain are anonymous, but this is not the case. Transactions on public, permission-less blockchains such as the Bitcoin blockchain are pseudonymous. Anyone can view the ledger, which records ownership of bitcoins and all transactions that have occurred upon it, but there is still a lack of connection between the Bitcoin address and an identifiable legal or natural person.

Therefore, with enough information or data overview, one could track activity to particular addresses, and addresses to individuals or parties involved in the blockchain.

A number of cryptocurrencies have been created specifically to solve the issue of privacy and pseudonymity. These include Z-Cash and Monero, which use various methods to mask the identity of participants. These methods involve "zero-knowledge proofs" in the case of Z-Cash and ring signatures, ring confidential transactions (RingCT), and stealth addresses for Monero.

The technical workings of each method are beyond the scope of this paper, but the principle is that the amounts involved as well as all parties to a transaction are not made public on either network. This is despite the fact that both Z-Cash and Monero operate on public, permission-less blockchains.

3. Proof of work vs. proof of stake (vs. other mechanisms)

Proof of work

Proof of work is the original blockchain consensus protocol, pioneered by Bitcoin. In a proof-of-work system, network participants compete to be the fastest to solve the cryptographic puzzles required to add a new block to the blockchain. The input to these puzzles consists of all previously recorded information on the blockchain, along with the new set of transactions to be added in the next block. Therefore, the input becomes larger and the calculation more complex over time, necessitating increased processing power. This causes the high energy intensity discussed above.

When the puzzle is solved, the machine involved proves that it completed the work, and is rewarded in any given system with a token of value. In the Bitcoin blockchain, this comes in the form of a newly-mined bitcoin.

Note that while successful mining is rewarded with new bitcoins, one does not have to own any bitcoins as a prerequisite to engage in bitcoin mining.

Proof of stake

Proof of stake is the most common consensus protocol after proof of work. We have chosen to illustrate its functionality on the example of the NXT cryptocurrency, which uses a pure proof-of-stake system in transaction validation.

In the NXT system, anyone can set up a node and buy NXT cryptocurrency. A validator must prove ownership of a certain amount of NXT in order to participate in forging, i.e., transaction validation. The validator's probability of forging the next block is equal to its share of all NXT in existence. This is a clear distinction from proof of work, in that NXT ownership is a prerequisite to participation in "forging" and therefore to earning the associated fees. Note that transaction fees earned by the validator are paid by the transacting parties. Forging creates no new tokens, as all NXT is pre-mined.

"Transparent forging" constitutes a recent improvement to the protocol, its aim being to increase the threshold for an attack on the system from 51% to 90%, i.e., with transparent forging, a bad actor would have to own over 90% of all NXT in issue in order to manipulate the ledger. Under this system, the node which will validate the next block is randomly selected in advance, but only the next 10 validators are known. A node that fails to take up its role is penalized by temporary exclusion from forging.

One node forges each block, which allows data to be sent directly to it, speeding up the forging process. Unlike proof-of-work mining, forging requires little computing power and electricity. Even the simplest computers, such as the Raspberry Pi, can forge.

Proof-of-stake systems such as NXT's can thus deliver transaction speeds approaching those of the Visa network, and may therefore prove useful in driving wider adoption of cryptocurrency. In that context, it is worth noting that the already popular Ethereum network is expected to adopt proof of stake in 2018.

Other mechanisms

A range of other mechanisms exist, such as proof of activity, proof of burn, proof of capacity or proof of elapsed time. Details of these mechanisms fall outside the scope of this paper, as they would not directly support the primary discussion of financial reporting.

4. The DAO hack

For further information on the DAO hack, refer to the following outline by Coindesk:

"Understanding The DAO Attack," *Coindesk*, https://www.coindesk.com/understanding-dao-hack-journalists/, accessed 15 January 2018.

5. ERC-20: crypto-fueling the ICO phenomenon

Ethereum was created as a platform to enable the creation of decentralized applications, and ICOs simply constitute one such application. Their proliferation has been fueled by the availability of a token protocol called ERC-20, which was designed to create a standardized list of rules to which all Ethereum tokens must conform. This creates a welcome island of predictability within the ICO wilderness.

6. US SEC report of investigation regarding the DAO

U.S. Securities and Exchange Commission Release No. 81207, Report of *Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO*, United States Securities and Exchange Commission, 2017

7. "Money has no intrinsic value*", and yet we consider it an asset

* While this statement is intuitively acknowledged by many, it appears explicitly in, e.g., Niall Ferguson's *The Ascent of Money*: "Banknotes … are pieces of paper which have next to no intrinsic worth". Leading investment valuation authority, NYU Stern Professor Aswath Damodaran, states that "currencies cannot be valued. … May be [one] can set fire to it if [one is] cold, [but] paper currency does not fulfill any fundamental need" other than as a medium of exchange. He goes on to make the distinction that currencies can only be priced against each other, and this is most appropriately based on their purchasing power and adoption.

Money is a social construct, used to facilitate the exchange of goods and services humans deem valuable to them. Trading via a mutually recognized medium of exchange is much smoother than barter exchange of, e.g., shirts for cauliflowers. Historically, various forms of money have been used, some with a real use value (e.g., salt) and some with virtually no use value (e.g., paper banknotes, which might otherwise only be used as wallpaper or kindling). Gold falls far closer to the latter end of the spectrum, as it has few industrial applications and its use in consumer products, such as jewelry, is itself dependent on social acceptance of the material as valuable and therefore suitable for displaying wealth. Indeed, financial market participants frequently describe gold as more similar to currencies than to other metals.

This is therefore also a counterargument to those who would deem a new, digital medium of exchange, such as cryptocurrency, not to constitute an asset at all due to its "virtual" nature and the lack of "backing" by a real asset. One might state that modern

fiat currencies are backed by the gold held by their issuing central banks, but this fails to consider the fact that one cannot actually exchange banknotes for gold at the central bank and the fact that the central bank typically has the authority to issue an indeterminate amount of banknotes "backed" by its finite supply of gold (as was the case in Weimar Germany or, more recently, in Zimbabwe). Thus, the value of fiat currency is a matter of its social acceptance and of trust in the central bank — hence the term "fiat". And even if it were not (as in the case of a gold (or salt, or colored bead) standard), it would be a matter of social acceptance of and trust in the value of gold (or salt, or colored beads).

As a final note, consider the recent discussion regarding the appropriate path of monetary policy as developed economies emerge from the financial crisis. One popular protagonist of this debate, the Taylor Rule, effectively calls for an automatic formula to determine the level of interest rates, the fundamental lever in the government's control over the money supply. What is Bitcoin, then, but a radical Taylor-Rule-driven Fed?

Sources:

"The Bitcoin Boom: Asset, Commodity, Currency or Collectible?" *YouTube — Aswath Damodaran*, https://www.youtube.com/watch?v=8iNeXCAM_lk, accessed 24 October 2017.

Niall Ferguson, *The Ascent of Money: A Financial History of the World* (The Penguin Press, 2008).

8. Pseudo-acceptance of cryptocurrency by multinationals

Some might present the counterargument that a number of large, multinational corporations have announced their acceptance of payments in cryptocurrency (specifically Bitcoin). However, closer examination reveals that for this to function, they, in fact, require an intermediary that converts the cryptocurrency to fiat currency. That is, these firms do not truly accept cryptocurrency and hold it for their own transactional needs.

9. "Insignificant risk of changes in value" counterargument

An argument can be made that not all fiat currencies are as stable as those in the developed world, as evidenced by hyperinflation in economies such as Zimbabwe or Venezuela. This does not prevent the classification of the Zimbabwean dollar or Venezuelan bolivar as "cash".

We note above that cryptocurrency is not cash because of its lack of widespread acceptance as a medium of exchange (as institutionalized by the almost universal lack of recognition as legal tender by governments and central banks), and therefore it is seen as existing as another asset alongside fiat money. Therefore, the "insignificant change in value" argument is directed at comparing cryptocurrency with other cash equivalents and not cash itself. These other cash equivalents are characterized by insignificant fluctuations in value relative to the currency they are denominated in, which would remain true for, e.g., a certificate of deposit denominated in Zimbabwean dollars or Venezuelan bolivars. This is consistent with the arguments presented by the AASB, which goes on to clarify that since the significance of the risk of changes in value of a digital currency can only be assessed with "cash" existing in the same currency, cryptocurrency, therefore, also fails the definition of a cash equivalent as it is not "cash".

10. Cryptocurrency as an investment

This is despite the fact that millennials in particular have highly favorable views of bitcoin, even compared to traditional investments in stocks and bonds. Some financial advisors have gone so far as to suggest a portfolio allocation to cryptocurrency as a distinct asset class.

According to Bloomberg, a survey by venture capital firm Blockchain Capital found that only 2% of Americans have ever owned cryptocurrency.

Perhaps more interestingly, however, about 30% of people aged 18 to 34 would rather own US$1,000 worth of bitcoins than US$1,000 of government bonds or stocks.

Even some investment managers have suggested a specific portfolio allocation to cryptocurrency. For example, a separate Bloomberg article quoted a Union Square Ventures managing partner's recommended range of 0% to 10% of one's assets, on the basis of individual risk appetite.

These observations underscore the argument that the public sees cryptocurrency as an effective store of value, but has not (yet) adopted it as a medium of exchange.

Source:

"Nearly a Third of Millennials Say They'd Rather Own Bitcoin Than Stocks," *Bloomberg*, https://www.bloomberg.com/news/articles/2017-11-08/millennials-ready-to-ditch-stocks-to-keep-bitcoin-rally-alive, accessed 8 November 2017.

"Early Bitcoin Investor Has Some Advice On How Much Money to Hold in Bitcoin," *Bloomberg*, https://www.bloomberg.com/news/articles/2017-10-16/with-bitcoin-pushing-6000-early-investor-says-how-much-to-buy, accessed 16 October 2017.

11. IAS 38 cost and revaluation models

Under the cost model, an intangible asset is carried at its cost less any accumulated amortization and any accumulated impairment losses. Under the revaluation model, an intangible asset is carried at a revalued amount, being its fair value at the date of the revaluation less any subsequent accumulated amortization and any subsequent accumulated impairment losses. IAS 38 includes specific guidance as to when the revaluation difference should be recognized in profit or loss or other comprehensive income.

12. Payment Services Act (Japan)

In 2016, the Payment Services Act (Act No. 59 of 2009) was amended to define virtual currencies and to introduce a registration system for virtual currency dealers. From the annual period following the annual period to which 1 April, 2017 belongs, the financial statements of registered virtual currency dealers will be subject to financial statement audit by a certified public accountant or an audit corporation.

5. Contacts

EY Technical Leadership – IFRS & Blockchain

Paul Brody
Partner
EY Global Blockchain Innovation Leader
Ernst & Young LLP (USA)

T: +1 415 902 3613
E: paul.brody@ey.com

Laure Galcéran
Partner
EY EMEIA FS Assurance
Financial Accounting Advisory Services Leader
Ernst & Young Audit SAS (France)

T: +33 1 46 93 45 23
E: laure.galceran@fr.ey.com

Shaun Carazzo
Partner
UK FS Assurance
Financial Accounting Advisory Services Leader
Ernst & Young LLP (UK)

T: +44 20 7951 0441
E: scarazzo@uk.ey.com

Victor Chan
International Director
EY IFRS Services, Global Professional Practice
Ernst & Young Global Limited

T: +44 20 7980 0677
E: victor.chan@uk.ey.com

UK FS Assurance FinTech Leadership

Hitesh Patel
Associate Partner
EY EMEIA FS Assurance
Banking & Capital Markets
Ernst & Young LLP (UK)

T: +44 20 7951 7643
E: hpatel2@uk.ey.com

Michael Heap
Senior Manager
EY EMEIA FS Assurance
Banking & Capital Markets
Ernst & Young LLP (UK)

T: +44 20 7951 2160
E: mheap@uk.ey.com

Francis Malaspina
Senior Manager
EY EMEIA FS Assurance
Banking & Capital Markets
Ernst & Young LLP (UK)

T: +44 20 7951 0810
E: fmalaspina@uk.ey.com

Andrew Probert
Director
EY EMEIA FS Assurance
Financial Accounting Advisory Services
Ernst & Young LLP (UK)

T: +44 20 7951 0219
E: aprobert@uk.ey.com

IFRS (#) – Accounting for crypto-assets Authors

Jiří (George) Daniel
Senior
EY EMEIA FS Assurance
Wealth & Asset Management
Ernst & Young LLP (UK)

T: +44 20 7197 7149
E: gdaniel2@uk.ey.com

Amanda Green
Senior
EY EMEIA FS Assurance
Banking & Capital Markets
Ernst & Young LLP (UK)

T: +44 20 7980 9543
E: agreen51@uk.ey.com

EY | Assurance | Tax | Transactions | Advisory

About EY

EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

In line with EY's commitment to minimize its impact on the environment, this document has been printed on paper with a high recycled content.

ey.com