Technical Line

A holder's accounting for cryptocurrencies

What you need to know

- Cryptocurrencies meet the definition of indefinite-lived intangible assets, and holders generally should account for these assets at historical cost less impairment pursuant to ASC 350.

- However, investment companies as defined under ASC 946 should account for their cryptocurrency investments as "other investments" and subsequently measure these assets at fair value through earnings.

- Determining ownership of a cryptocurrency held through a third party may be challenging and could affect the determination of the appropriate accounting.

- Entities that engage in mining activities need to develop an accounting policy based on the application of current US GAAP to the economics of their mining transactions and disclose that policy.

- Entities that invest in cryptocurrencies need to have controls in place to safeguard the private key that provides access to the cryptocurrencies and to maintain complete and accurate books and records related to their cryptocurrency activities.

Overview

The proliferation of cryptocurrencies and the lack of US GAAP guidance that specifically addresses cryptocurrencies have raised questions about how holders of these assets should account for them.

EY

Building a better
working world

We believe that cryptocurrencies meet the definition of indefinite-lived intangible assets, and holders should account for them at historical cost less impairment, applying the guidance in Accounting Standards Codification (ASC) 350, *Intangibles — Goodwill and Other*. However, investment companies in the scope of ASC 946, *Financial Services — Investment Companies*, should account for their investments in cryptocurrencies as "other investments" and should subsequently measure these assets at fair value through earnings.

In this publication, we use the term cryptocurrency to refer to crypto-assets that serve purely as a medium of exchange (e.g., Bitcoin).

Some stakeholders have raised concerns about the application of the intangible asset guidance in ASC 350 to cryptocurrencies, saying it does not provide relevant information to financial statement users because it does not appropriately reflect the economics associated with cryptocurrencies. However, in the absence of standard-setting that specifically addresses the accounting for cryptocurrencies, entities that invest in cryptocurrencies must apply existing accounting standards.

The Financial Accounting Standards Board (FASB) does not have a standard-setting project on cryptocurrencies on its agenda, but an industry trade group has requested that the FASB address the accounting for cryptocurrencies. Accordingly, the FASB staff has researched blockchain technology and cryptocurrency market activities and the accounting challenges they present.

Readers should monitor any standard-setting, regulatory or technological developments that may affect an entity's accounting for cryptocurrencies or its controls and processes related to cryptocurrencies.

Blockchain, cryptocurrencies and tokens

Cryptocurrencies are based on blockchain technology, a form of distributed ledger technology that keeps a record of every transaction related to a digital asset across a network that no single party controls. Since the introduction of Bitcoin in 2009, cryptocurrencies have been promoted as alternatives to government-issued currency, but they are widely viewed today as speculative investments and have been the target of both manipulation and theft.

Blockchain technology gets its name from the way transactions are validated and stored on the network. Transactions are grouped and validated in a batch called a block, and each block is linked to a chain of blocks using cryptography. This chain of blocks is the ledger that is maintained by a network of participants rather than a central party, and anyone can join by downloading and running software that defines the rules for updating the ledger (i.e., the consensus protocol). Each computer that holds a copy of the ledger is called a node, and the ledger is replicated and synchronized across all nodes in real time.

Cryptocurrencies are often created by a process called mining. That is, parties that operate nodes on the network compete to be the first to solve the cryptographic algorithm called a hash that is required to securely add a new block to the chain. When a "miner" does this, the miner is rewarded with a newly issued digital asset.

To transact on a blockchain, a participant needs to use a private "key" (i.e., a string of letters and numbers) that is typically stored on hardware and/or software known as a "digital wallet." The private key is used to access digital assets recorded on the blockchain. Participants use digital wallet software to arrange a transaction and submit it into the blockchain network. Once a transaction is submitted, the nodes that maintain the network must then validate the transaction through the mining process. Typically, a miner who successfully validates the transaction also receives transaction fees in the form of cryptocurrencies from the transferor (i.e., the participant requesting the transaction).

Smart contracts that use computer code to automatically trigger an action can also be stored on a blockchain. For example, smart contracts can be used to send a digital asset from one party to another when a predefined condition is met.

Tokens

It is important to distinguish between cryptocurrencies and other crypto-assets that provide something more than purely a medium of exchange. While these non-cryptocurrency digital assets (commonly referred to as tokens) are also recorded on a distributed ledger and usually issued in a process called an initial coin offering (ICO), they have different financial reporting considerations than cryptocurrencies and may have different regulatory implications.

Certain tokens provide holders with some kind of utility, such as access to a good or service from an identifiable counterparty. Others may provide the holder with ownership rights in an entity (e.g., voting rights, rights to participate in profits) or rights to payments in fiat currencies, similar to traditional financial instruments such as equity shares or debt instruments. Asset-backed tokens digitize an ownership interest in an underlying asset by recording information about it on a blockchain.

Tokens may also serve a combination of purposes. For example, a token may provide its holder with rights to fiat currency profits of the issuing entity while also allowing the holder to redeem the token for goods or services provided by that entity.

This publication does not address the accounting for tokens.

A holder's accounting for cryptocurrencies

US GAAP does not specifically address a holder's accounting for cryptocurrencies. The accounting therefore has to be evaluated based on the nature of the asset, the type of investor and how the asset is held.

Determining the nature of assets

Entities may hold their cryptocurrencies directly or indirectly through a third party, such as a custodian or an exchange that may control access to the entity's cryptocurrency holdings. For example, an entity that buys or sells cryptocurrencies on an exchange may store its cryptocurrency holdings in a digital wallet hosted by the exchange, and the exchange may control the private key. If this is the case, the entity must determine whether it owns the cryptocurrencies or whether it has a right to obtain cryptocurrencies from the exchange.

When a cryptocurrency is held through a third party, the evaluation of whether the entity or the third party is the owner of the cryptocurrency can be complex. It requires careful consideration of the terms of an entity's agreement with the third party, the laws governing the jurisdiction(s) in which the third party operates and how the third party manages and stores the cryptocurrencies.

Questions an entity may consider when assessing ownership include:

▸ Who is the legal owner of the cryptocurrencies?

▸ Does the agreement with the third party state that there is a custodial relationship?

> When a cryptocurrency is held through a third party, the evaluation of whether the entity or the third party owns the cryptocurrency can be complex.

- What legal and regulatory requirements apply to the third-party custodian with respect to the custody of cryptocurrencies it holds on behalf of others? How does the third-party custodian satisfy those requirements?

- Does the agreement specify the ownership of cryptocurrencies held in the third party's digital wallets?

- If the third party files for bankruptcy court protection, who will have claims to the entity's cryptocurrencies held in the third party's digital wallet?

- Does the third party segregate its customers' cryptocurrencies into a different digital wallet from cryptocurrencies it owns?

- Can the third party transfer cryptocurrencies held in its digital wallets on the customer's behalf to another party without being instructed to do so by the entity?

- Does the access to customers' cryptocurrencies in the third party's digital wallet require a multi-signature authorization by both the entity and the third party?

How we see it

When investments in cryptocurrency are held through a third-party custodian or exchange, entities will need to carefully consider the terms and structure of the arrangement with the third party that controls access to those cryptocurrency holdings, as well as the legal and regulatory environment in which the custodian or exchange operates, to determine the nature of assets they hold.

If an entity concludes that it has a right to obtain cryptocurrencies rather than ownership of the cryptocurrencies, judgment will be required to determine the appropriate accounting. That is, the right to a cryptocurrency may be accounted for differently from ownership of a cryptocurrency. For example, an entity would need to determine whether the right to obtain cryptocurrencies includes an embedded derivative that requires bifurcation pursuant to ASC 815.[1] In determining the appropriate accounting (i.e., recognition and measurement), the entity will have to consider its rights, its claims on the third party and the third party's performance risk (e.g., the possibility that it does not hold sufficient cryptocurrencies to adequately settle the entity's claims).

The rest of this publication describes accounting considerations for cryptocurrencies that an entity determines that it owns.

Classifying cryptocurrencies

We believe that cryptocurrencies meet the definition of intangible assets under ASC 350, even though we recognize that they have some characteristics that are not typical of intangible assets. For example, unlike typical intangible assets, they may be traded on exchanges, their value may be volatile and they must be exchanged for an entity to realize their value. Also, unlike other intangible assets, units of a particular cryptocurrency are fungible.

The following table provides our analysis of why cryptocurrencies meet the definition of intangible assets:

	US GAAP definitions	Classification conclusion
Cash and cash equivalents	Cash includes currency, demand deposits with financial institutions and other accounts that have the general characteristics of demand deposits. Cash equivalents are short-term, highly liquid investments that are readily convertible to known amounts of cash and represent insignificant risk of changes in value.	<u>Not met:</u> Cryptocurrencies are not accepted as legal tender and are not backed by sovereign governments. Cryptocurrencies do not have maturities and may experience significant price volatility.
Financial instrument	A financial instrument is cash, an ownership interest in an entity or a contract that imposes an obligation to deliver or a right to receive cash or another financial instrument.	<u>Not met:</u> Cryptocurrencies are not cash or an ownership interest in an entity, and they do not represent a contractual obligation to deliver or a right to receive cash or another financial instrument.
Inventory	Inventory is tangible property held for sale in the ordinary course of business, in process of production for sale or to be consumed in the production of goods or services.	<u>Not met:</u> Cryptocurrencies are not tangible property because they lack physical substance.
Intangible asset	Intangible assets are assets[2] (not including financial assets) that lack physical substance.	<u>Met:</u> Cryptocurrencies are nonfinancial assets that lack physical substance.

Accounting for owned cryptocurrencies

Entities other than investment companies — intangible asset

As intangible assets, cryptocurrencies are initially measured at cost. Since there is no limit on their useful life, cryptocurrencies would generally be classified as indefinite-lived intangible assets.

Because they are indefinite-lived intangible assets, they are not subject to amortization. Instead, they must be tested for impairment annually and more frequently if events or circumstances change that indicate that it's more likely than not that the asset is impaired (i.e., if an impairment indicator exists). As a result, holders of cryptocurrencies will only recognize decreases in the value of a cryptocurrency, and any increase in value will be recognized only upon disposition.

Increases in value *are not* recognized while the cryptocurrency is held.

Decreases in value *are* recognized while the cryptocurrency is held.

Questions have arisen about what constitutes an impairment indicator between annual impairment tests. Entities will need to assess all relevant events and circumstances that could adversely affect significant inputs used to measure fair value. For example, if a cryptocurrency is traded on an exchange where there are observable prices in an active market, a decline in

the quoted price below an entity's cost is generally viewed as an impairment indicator. If an entity determines that an impairment indicator exists, the holder would have to perform a quantitative impairment test.

When evaluating indefinite-lived intangible assets for impairment under ASC 350, entities need to consider the unit of account (e.g., one Bitcoin[3] or a portfolio of Bitcoins held). ASC 350 requires that indefinite-lived intangible assets be combined into a single unit of accounting for purposes of impairment testing if the assets operate as a single asset and, as such, are essentially inseparable from one another. A holder's determination of the unit of account for impairment testing purposes will depend on the specific facts and circumstances, but the fact that holders can transact in individual units (e.g., one Bitcoin) of a cryptocurrency indicates that each unit of cryptocurrency is likely a separate unit of account for impairment testing purposes.

Holders will have to track the cost of units of cryptocurrencies they purchase or receive at different times and use the appropriate cost for each unit of cryptocurrency when performing an impairment test and upon derecognition when they sell the cryptocurrency or exchange it for other goods or services.

When they derecognize a cryptocurrency, holders should evaluate the nature of the transaction to determine the appropriate accounting guidance to apply. For example, holders should understand whether the counterparty to the transaction resulting in derecognition is a customer, whether they are receiving cryptocurrencies or other goods or services in exchange for their cryptocurrencies and whether the transfer has commercial substance. Generally, holders should consider the guidance in ASC 606,[4] ASC 845[5] and ASC 610-20[6] when determining the appropriate accounting for the exchange transaction.

Investment companies — other investments

While cryptocurrencies meet the definition of an intangible asset under ASC 350, investment companies in the scope of ASC 946 may invest in cryptocurrencies as an asset class for purposes of capital appreciation. Investment companies generally account for their investments in cryptocurrencies as "other investments" under ASC 946-325. Under that guidance, these investments are subsequently measured at fair value through profits or losses.

Cryptocurrency's fair value measurement

A fair value measurement is required for accounting purposes when a cryptocurrency is (1) held as an "other investment" by an investment company in the scope of ASC 946 or (2) held by an entity that is not an ASC 946 investment company as an intangible asset when fair value measurement is required (e.g., an impairment analysis is required by ASC 350).

How an entity measures the fair value of a cryptocurrency will depend on whether the principal market is active (i.e., transactions occur with sufficient frequency and volume to provide pricing information on an ongoing basis) and whether the entity can access the principal market on the measurement date. While the most common cryptocurrencies (e.g., Bitcoin, Ether) are currently considered to be actively traded on exchanges or over-the-counter markets, other cryptocurrencies may not be.

In determining the fair value of a cryptocurrency, an entity needs to identify its principal market or in the absence of a principal market, the most advantageous market. The market with the greatest volume and level of activity that an entity has access to for the cryptocurrency generally will be an entity's principal market for that cryptocurrency. This determination requires an assessment of whether there are any barriers that prevent the entity from accessing a particular market.

When identifying the principal (or most advantageous) market, an entity is not required to undertake an exhaustive search of all possible exit markets for the asset, but it should consider all information that is reasonably available. In the absence of evidence to the

How an entity measures the fair value of a cryptocurrency will depend on whether there is an active market the entity can access on the measurement date.

contrary, the market in which an entity normally would enter into a transaction to sell an asset is presumed to be the principal or most advantageous market. An entity should also evaluate whether there are any indicators of manipulation in the market. If there are indicators of manipulation, the entity needs to assess whether that market provides relevant and reliable price and volume information.

If an entity determines that the principal market for its cryptocurrency holdings is an active market, ASC 820[7] requires fair value to be calculated as the quoted price for identical assets multiplied by the quantity held by the entity. However, even if the entity's principal market is not active (i.e., there has been a significant decrease in the volume and level of activity in the principal market), quoted prices may still be observed in that market. In this case, the entity should assess the relevance and reliability of the observed prices and prioritize observable inputs in arriving at fair value. Because cryptocurrencies lack intrinsic value and have limited usage, it would be challenging to use an income approach (e.g., discounted cash flow approach) to determine the fair value.

Level 1 fair value hierarchy classification would be appropriate if the cryptocurrency's valuation is based on a quoted price for the identical asset in an active market. If an entity's principal market for a cryptocurrency is not active, the measurement would be classified in level 2 or level 3 of the fair value hierarchy, depending on the nature of the adjustments made to the quoted price in the inactive market. An entity should be aware that it may need to change the hierarchy level for a cryptocurrency if market conditions change.

Other matters

Hard forks and airdrops

Entities that control the private keys required to access their cryptocurrency holdings may receive access to other digital assets (including cryptocurrencies) as a result of various events. Two of the most common events are hard forks and airdrops.

A hard fork results from a certain type of change in the software of an existing blockchain network that is not adopted by all nodes. After a hard fork, there are two different blockchain networks: (1) the original blockchain comprising nodes that operate the original software and (2) the new blockchain comprising nodes that operate the new software. The original blockchain and the "forked" blockchain share the same history of transactions (i.e., same copy of the distributed ledger) that occurred before the hard fork event. However, after the hard fork event, the original blockchain and the "forked" blockchain will each record only transactions that occur on their separate network and ledger.

Investors with a private key that controls access to the old cryptocurrency on the original blockchain will also control access to a number of units of a new cryptocurrency that exists on the forked blockchain.

Illustration 1: Bitcoin hard fork

In August 2017, the Bitcoin network experienced a hard fork, resulting in the creation of Bitcoin Cash. A holder of a private key for Bitcoin was able to use the same key to access an equivalent number of units of Bitcoin Cash. The price of Bitcoin Cash was only a fraction of the price of Bitcoin.

In an airdrop, a digital asset (including a cryptocurrency) is distributed, usually free of charge, to either a random selection of wallet addresses or a specified list of wallet addresses, generally as a way to promote the digital asset.

> **Illustration 2: OMG airdrop**
>
> In July 2017, OmiseGo (OMG) conducted a large-scale airdrop in which 5% of all its OMG cryptocurrency was distributed across any wallet address that held more than 0.1 Ether as of a specified block (i.e., block 3,988,888) on the Ethereum public blockchain.

Accounting for new cryptocurrencies granted to an entity in a hard fork or airdrop event can present several challenges. Under ASC 350, an entity recognizes an intangible asset when it is acquired. However, in a hard fork or airdrop, an entity may gain the opportunity to access new cryptocurrencies (i.e., intangible assets) without its knowledge or permission. Another challenge is that an entity does not pay for these new cryptocurrencies. Additionally, the cryptocurrencies resulting from these events may be very thinly traded or have little or no value. A holder that is granted the right to new cryptocurrencies in a hard fork or airdrop will need to carefully determine whether, when and how to recognize those cryptocurrencies and disclose its related accounting policy.

Mining

Determining when an entity should recognize a cryptocurrency as a result of a hard fork or airdrop can be challenging.

As previously discussed, some blockchain networks rely on miners that compete to validate and add blocks of transactions to the distributed ledger. In order to incentivize these miners to compete in processing the transactions for the next block, the winning miner is entitled to transaction fees and a block reward. Transaction fees are specified in each transaction request and deducted from the digital wallet of the transferor. Unlike transaction fees, which are paid by the transferor, block rewards are newly created cryptocurrency units granted to the winning miner pursuant to the blockchain's consensus protocol.

An entity should apply the guidance in ASC 606 if it concludes that it has a contract with a customer to transfer goods or services in exchange for consideration. A customer is defined in ASC 606 as "a party that has contracted with an entity to obtain goods or services that are an output of the entity's ordinary activities in exchange for consideration," and a contract is defined as "an agreement between two or more parties that creates enforceable rights and obligations."

Mining entities will need to carefully consider whether (1) the contract is with a customer, (2) validating the transaction creates enforceable rights and obligations and (3) mining is considered an output of the entity's ordinary activities. Determining whether the contract is with a customer may be particularly challenging because a block reward is issued by the consensus protocol for successfully mining a block, not by an identifiable party (e.g., the participants that requested the transactions in the block). As a result, a mining entity may apply a different accounting model for the transaction fees and a block reward.

A mining entity that determines that its receipt of a block reward is not pursuant to a contract with a customer and therefore not in the scope of ASC 606 will need to determine the appropriate accounting model to apply. For example, if the mining entity determines that its receipt of the block reward is an exchange transaction with commercial substance and the fair value of the block reward is determinable, it may be acceptable for the miner to account for the receipt of the block reward as a nonmonetary exchange for its mining activities. If that's the case, the entity would recognize the intangible asset received at fair value with a corresponding amount on the income statement (e.g., as other income).

Alternatively, if the mining entity views the block reward as an internally developed intangible asset (rather than the receipt of a nonmonetary asset in exchange for mining services), the block reward would generally be reflected in earnings only upon derecognition (i.e., when realized in connection with a subsequent exchange transaction).

Miners may incur costs directly related to mining activity, including paying for equipment and electricity. We believe that entities should record the costs of their mining activities as expenses when they are incurred. This is because the costs are not incurred to acquire a specifically identifiable intangible asset, and there is uncertainty about the future economic benefits when the costs are incurred.

Because US GAAP does not specifically address cryptocurrency mining activities, entities will need to develop an accounting policy based on the appropriate application of current US GAAP to the economics of their mining transactions and disclose that policy.

Disclosures

US GAAP does not specifically address disclosures for cryptocurrencies. As a result, entities need to provide disclosures required by the relevant accounting guidance (e.g., ASC 350, ASC 820). Entities should provide disclosures about risks and uncertainties[8] and any loss contingencies,[9] including for potential illegal acts, relating to their cryptocurrency activities.

We believe that entities should also provide additional disclosures that would be useful to users of the financial statements in evaluating the effect of cryptocurrencies on their financial condition and performance. These disclosures may include (1) a description of the quantity and nature of its cryptocurrency holdings; (2) the accounting policies the entity applies (e.g., measurement basis); (3) the historical volatility of the cryptocurrency holdings; (4) the entity's reason for holding those cryptocurrencies and (5) the risks associated with holding cryptocurrencies.

Entities are also required to disclose the details of related party transactions pursuant to ASC 850.[10] Because cryptocurrency transactions can be anonymous (even when they are conducted on a public exchange or over-the-counter market), identifying related parties and their transactions can be challenging. Wesley Bricker, Chief Accountant of the Securities and Exchange Commission (SEC), highlighted the importance of disclosing transactions with related parties and the resulting balances in remarks at the 2018 AICPA National Conference on Banks & Saving Institutions.[11]

Entities should strive to be transparent about their involvement in cryptocurrencies and related activities, as well as the associated risks.

How we see it
Entities need to use their judgment in providing sufficient disclosures to enable users of financial statements to understand the effect of holding cryptocurrencies on their financial position, financial performance and cash flows.

Internal control over financial reporting

In his recent speech, Mr. Bricker reminded issuers that they must "continue to maintain appropriate books and records — regardless of whether distributed ledger technology (such as blockchain), smart contracts and other technology-driven applications are (or are not) used."

Mr. Bricker also said issuers should "act appropriately within the parameters of the existing requirements of the federal securities laws, such as those relating to books and records, internal accounting controls, internal control over financial reporting (ICFR), and custody. Distributed ledger technology and digital assets, despite their exciting possibilities, do not alter this fundamental responsibility."[12]

An entity's accounting and technical staff who perform controls relating to investments in cryptocurrencies should have the necessary competencies. Some controls, particularly those relating to the safeguarding of private keys and assessing the reliability of information available in a blockchain, may require special skills in areas such as blockchain technology,

cryptography and encryption. Management should evaluate whether the individuals implementing and performing the controls have the right skills to effectively prevent or detect errors or fraud that could result in material misstatements in the financial statements.

Safeguarding of digital wallets and private keys

When entities directly control cryptocurrency holdings, they need appropriate controls to make sure the private key used to authorize a transfer of the cryptocurrency from one public address to another is safeguarded. If the key is lost or destroyed and backups are not properly secured, the entity will be unable to access the cryptocurrency. Further, if the key is stolen, the cryptocurrency could be transferred to another party, and the transfer could be irreversible.

A digital wallet (or private key) can be connected to the internet (hot wallet) via cloud-based or desktop applications or stored offline (cold wallet). How a private key is stored may affect the risks involved and the type of controls that are needed to address them. Management must design and implement controls to address all of the relevant risks, including those related to the initial generation of the private key and the safeguarding of the key after it is created.

Private keys should be created and safeguarded in a controlled environment. For example, such controls can be designed to make sure that no single person has knowledge of the entire sequence of letters and numbers that make up the private key. Controls should also be in place to secure backups and restrict access to applications, devices and the locations where the devices containing the private key are maintained.

Understanding and evaluating counterparties and other third parties

As discussed above, some entities hold their cryptocurrency investments through a third party such as a custodian or an exchange. In many cases, these parties control access to the cryptocurrency and have responsibility for the security of the private key. When this is the case, management needs to understand the controls the third party has in place to safeguard the private key and the third party's controls over services such as processing cryptocurrency transactions, tracking customer balances and reporting this information to customers.

Entities must evaluate new third-party relationships and obtain a complete understanding of both parties' rights and obligations. Entities should consider whether a third party is reputable, regulated, insured and audited and/or whether it provides a service organization control report, as appropriate.

Entities must also apply their know-your-counterparty (KYC) and anti-money-laundering (AML) processes to cryptocurrency transactions. They should be aware of the heightened risk that criminals might try to take advantage of the anonymity and weak regulation in certain cryptocurrency markets.

Understanding and evaluating the risks associated with underlying technology

When information from a cryptocurrency's blockchain is used as part of an entity's controls, management should assess the reliability, completeness and accuracy of this information. Management should gain a sufficient understanding of the underlying technology (e.g., blockchain protocol, smart contracts, digital wallets) for each cryptocurrency investment in order to understand how transactions are processed, evaluate related risks and assess the design attributes of those technologies, or design company-specific controls, to address those risks. The entity should have a clear policy for developing this understanding before investing in each new cryptocurrency.

Selecting and applying appropriate accounting policies

Entities should have controls in place to make sure they select and apply appropriate accounting policies. These controls should address an entity's policies for determining the nature of the asset when a third party holds the cryptocurrency, the value of the cryptocurrency holding, the unit

> Special skills may be needed by the individuals who perform controls that relate to safeguarding private keys.

of account, the cost basis, the measurement and recognition of gains and losses, impairment (including the identification of interim impairment indicators) and cryptocurrencies received in hard forks and airdrops. Entities also should have controls in place to make sure their disclosures are sufficient, including disclosures required by ASC 275, ASC 450 and ASC 850.

When fair value measurement is required, an entity's controls need to address the identification of the principal (or most advantageous) market and the ongoing determination of whether the market is active, the nature and amount of any adjustments to quoted prices, the level in the fair value hierarchy and whether the principal (or most advantageous) market provides relevant and reliable price and volume information. An entity's controls over the relevance and reliability of price and volume information should consider whether there are any indicators of manipulation in the market and whether transactions contributing to the fair value measurement reflect arm's length transactions between market participants.

Transaction controls

Entities should make sure they have appropriate authorization controls and that they segregate duties associated with the initiation of cryptocurrency transactions. They should also design well-controlled manual reconciliations or programmed interfaces between the blockchain(s) and the entity's books and records, including adequate cut-off procedures.

Entities also need effective controls over the identification and disclosure of related party transactions. As noted above, it may be difficult to identify related party transactions involving cryptocurrencies because parties to transactions on a blockchain are identified only by their public addresses, which are strings of letters and numbers.

Lastly, an entity may run afoul of laws or regulations or otherwise engage in cryptocurrency activities that expose it to litigation, claims and assessments, which might require accruals and/or disclosures. Entities should consider whether they need to accrue for or disclose loss contingencies arising from their cryptocurrency activities, including contingencies relating to pending or threatened litigation and noncompliance with applicable laws and regulations.

Endnotes:

[1] ASC 815, *Derivatives and Hedging*.

[2] Paragraph 25 of FASB Concept Statement 6, *Elements of Financial Statements,* defines assets as "probable future economic benefits obtained or controlled by a particular entity as a result of past transactions or events." An entity that exchanges assets for cryptocurrencies, or receives cryptocurrencies as payment, would generally expect economic benefit upon transferring or selling the cryptocurrencies. Therefore, cryptocurrencies would generally meet the definition of an asset.

[3] Cryptocurrencies are typically designed to be divisible into very small units. For example, one Bitcoin can be transacted down to eight decimal places (i.e., 0.00000001 Bitcoin).

[4] ASC 606, *Revenue from Contracts with Customers*.

[5] ASC 845, *Nonmonetary Transactions*.

[6] ASC 610-20, *Other Income − Gains and Losses from the Derecognition of Nonfinancial Assets*.

[7] ASC 820, *Fair Value Measurement*.

[8] ASC 275, *Risks and Uncertainties*.

[9] ASC 450, *Contingencies*.

[10] ASC 850, *Related Party Disclosures*.

[11] Wesley Bricker, Chief Accountant of the SEC, *Remarks before the AICPA National Conference on Banks & Savings Institutions, dated 17 September 2018.*

[12] Ibid.