No. 2022-07
Updated 28 March 2025

Technical Line

Accounting for digital assets, including crypto assets

In this issue:

What you need to know

- The accounting for digital assets that rely on blockchain technology requires judgment based on the facts and circumstances.
- Digital assets in the scope of ASC 350-60 (i.e., crypto assets as defined by that subtopic) are measured at fair value each reporting period, with changes from remeasurement reflected in net income. All other digital assets generally meet the definition of indefinite-lived intangible assets and are initially measured at cost and tested for impairment under ASC 350-30.
- When investments in digital assets are held through a third-party custodian or exchange, entities need to carefully consider the terms of the arrangement to determine the nature of the assets that should be recorded.
- Blockchain networks rely on miners or validators to validate and add blocks of transactions to the distributed ledger. The fees and rewards they receive should be evaluated to determine whether there is a contract with a customer under ASC 606.
- The digital asset landscape is still evolving, and our views may change as new issues are identified and addressed by stakeholders, including regulators and standard setters.

Overview

This publication primarily addresses the accounting for digital assets by a holder. It also highlights accounting considerations for specialized entities engaged in digital asset activities, including investment companies, brokers and dealers, and miners, as well as certain emerging market activities in digital assets more broadly.

The publication has been updated to reflect the final guidance issued by the Financial Accounting Standards Board (FASB) on the accounting for and disclosure of crypto assets, as well as the Securities and Exchange Commission (SEC) Staff Accounting Bulletin (SAB) No. 122 (SAB 122) to rescind the staff's interpretative guidance on the accounting for obligations to safeguard digital assets that an entity holds for platform users. The updates also include other conforming and editorial changes.

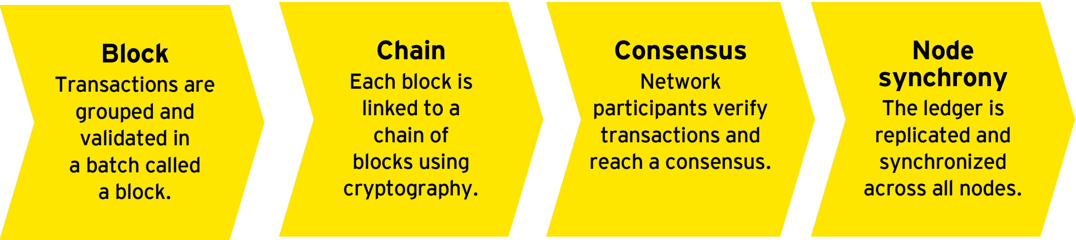
Because the digital asset landscape is evolving, we encourage readers to continue monitoring any standard-setting, regulatory and technological developments that may affect the accounting and control processes related to digital assets.

Background

"Digital assets" is an umbrella term used in practice to describe a wide range of assets that are typically powered by blockchain (or other similar "distributed ledger") technology. Distributed ledger technology relies on cryptography, a mathematical communication technique that is used to verify and secure transactions on a ledger maintained by a decentralized network of participants.

Blockchain and digital assets

Blockchain derives its name from the way transactions are validated and stored on the network and is generally comprised of the following steps:



Block
Transactions are grouped and validated in a batch called a block.

Chain
Each block is linked to a chain of blocks using cryptography.

Consensus
Network participants verify transactions and reach a consensus.

Node synchrony
The ledger is replicated and synchronized across all nodes.

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 relies on rules for updating the ledger (i.e., the consensus protocol). Each device that holds a copy of the ledger is called a node, and the ledger is replicated and synchronized across all nodes in real time.

The consensus protocols of a blockchain provide agreement, trust and security across the decentralized nodes in the network. There are many different consensus protocols used by blockchain networks, but the two most common are the proof-of-work and proof-of-stake protocols.

In a proof-of-work network, digital assets are created by a process called mining. That is, parties that operate nodes on the network validate new transactions and construct new blocks from transactions requested by network participants. "Miners" compete to be the first to solve the cryptographic algorithm, called a hash, that is required for the miner to have the right to broadcast the new block to the network. The winning miner is typically rewarded with transaction fees and newly issued digital assets. The bitcoin blockchain is an example of a proof-of-work network.

In a proof-of-stake network, users commit their digital assets by putting them at stake in order to operate nodes on the network and become validators. The network chooses validators based on protocol-specific consensus rules to help build the next block of transactions and verify transactions on the blockchain based on a combination of factors (e.g., the size of the stake, randomization, the length of time of the stake, validator uptime). Validators temporarily contribute, or stake, an amount of native digital assets (e.g., ether is the native digital asset to the Ethereum network) in exchange for the opportunity to earn a reward from the network. Similar to miners in a proof-of-work blockchain, validators typically receive transaction fees and newly issued digital assets as a reward for validating new transactions and completing a block.

To access digital assets and transact on a blockchain, a participant must use a string of letters and numbers called a private key, which is typically stored on hardware and/or software known as a digital wallet and is used to access digital assets recorded on the blockchain. Participants use digital wallet software to initiate transactions on the blockchain network. Once a transaction is submitted, the nodes that maintain the network validate the transaction through the validation processes described above. Typically, the miner(s) or validator(s) who successfully validate the transaction receive transaction fees in the form of digital assets from the transferor (i.e., the participant requesting the transaction).

Some smart contracts on a blockchain may use code to automatically trigger an action when specified conditions are met. For example, smart contracts can be used to send a digital asset from one party to another when an asset meets a certain price.

Some digital assets may be traded on an exchange (because units of the asset are fungible) and need to be transferred or sold to another party for an entity to realize an economic benefit (i.e., they have little to no intrinsic value). Other digital assets are backed by other assets or may entitle the holder to receive an underlying good or service from another party (e.g., utility tokens), while still other digital assets represent ownership of a digital or a physical asset and are nonfungible (e.g., nonfungible tokens (NFTs)).

Market trends

Digital assets, transactions in digital assets, and entities that operate and/or provide services in the digital asset sector continue to evolve. Recent market activities include:

- **Traditional products on chain**: Companies are offering smart contract-based savings accounts, borrowing and lending agreements, brokerage and trading services, and on-chain marketplaces (i.e., where transactions are conducted directly on the blockchain and are publicly recorded and validated).
- **Private key and digital asset management:** Custodial and non-custodial private key services and digital asset wallet solutions continue to evolve based on the needs of users. There has been an increasing number of companies that use multi-party computational or multi-signature digital wallets to self-custody digital assets.
- **Institutional interest:** Companies, particularly investment funds, are investing in digital assets and diversifying holdings beyond the higher market capitalization assets, such as bitcoin and ether. Institutions are showing increased interest in adopting public blockchains with appropriate privacy features to enhance business processes.
- **Digital assets as payment:** More companies are accepting digital assets as a payment medium, including stablecoins (see further description below). Many companies convert the assets into fiat currency immediately, while others hold the assets.

A holder's accounting for digital assets

The emergence and proliferation of a variety of digital assets in recent years have raised questions about how holders of these assets should account for them.

In December 2023, the FASB issued ASU 2023-08, *Intangibles — Goodwill and Other — Crypto Assets (Subtopic 350-60): Accounting for and Disclosure of Crypto Assets*, to address the accounting for and disclosure of a subset of digital assets that meet certain criteria (this subset is referred to in US GAAP and throughout the remainder of this publication as crypto assets). The guidance, which is codified in new subtopic ASC 350-60, requires all entities to subsequently measure the crypto assets they hold at fair value and recognize any changes from remeasurement in net income each reporting period in accordance with ASC 820, *Fair Value Measurement*.

Refer to Appendix B of our Financial reporting developments (FRD) publication, ***Intangibles — Goodwill and other***, for interpretive guidance on determining whether the digital assets they hold are in the scope of ASC 350-60, as well as their initial and subsequent accounting under that framework.

Digital assets that do not meet all six scope criteria described in ASC 350-60 should be accounted for in accordance with other applicable US GAAP. It may be helpful to consider the US GAAP definitions of other types of assets included in the following table when determining which accounting framework to apply.

	US GAAP definitions	**Questions to consider**
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.	‣ Is the asset generally accepted as legal tender? ‣ Is the asset backed by a sovereign government? ‣ Does the asset have a maturity date? ‣ Has the asset experienced 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.	‣ Does the asset represent cash or an ownership interest in an entity? ‣ Does the asset represent a contractual obligation to deliver or a right to receive cash or another financial instrument?
Inventory	Inventory is tangible property that is held for sale in the ordinary course of business, in process of production for sale or consumed in the production of goods or services.	‣ Does the asset have physical substance?

We generally believe that digital assets that are not crypto assets (i.e., not in the scope of ASC 350-60) and do not meet any of these definitions are likely intangible assets.[1] Since there is no limit on their useful life, such digital assets are generally classified as indefinite-lived intangible assets that are not subject to amortization. Indefinite-lived intangible assets are tested for impairment annually, and more frequently if impairment indicators exist, under the subsequent accounting model in ASC 350-30. As a result, holders of such digital assets only recognize decreases in the asset's value. Any increase in value is recognized only upon disposition (digital assets accounted for as indefinite-lived intangible assets are referred to throughout the remainder of this publication as digital assets in the scope of ASC 350-30).

Refer to our **FRD, *Intangibles — Goodwill and other***, for interpretive guidance on the subsequent accounting under ASC 350-30. Also see Questions 5, 6 and 7 of The AICPA's Practice Aid (the AICPA Guide), *Accounting for and auditing of digital assets*, which is intended to provide nonauthoritative guidance on how to account for digital assets, for additional guidance on evaluating impairment indicators, unit of account considerations and recording impairment losses under ASC 350-30.

Other stakeholders have similar views. SEC staff said at the 2021 AICPA & CIMA Conference on Current SEC and PCAOB Developments that under US GAAP, digital assets that are not considered securities or otherwise subject to specialized accounting guidance will likely be accounted for as intangible assets. The SEC staff has also said in these circumstances entities must follow the intangible asset model in ASC 350-30. However, the staff acknowledged that not all digital assets are the same, and registrants will need to consider the characteristics and rights and obligations associated with the digital assets that they transact in to determine the appropriate accounting.

It is important to note that US GAAP does not address what it means to "hold" a digital asset. Accordingly, we believe it is important that an entity evaluates whether it is the owner of a digital asset when determining whether to recognize the asset in the financial statements.

In practice, entities may hold their digital assets directly or indirectly through a third party. When an entity stores its digital assets in a digital wallet it owns (i.e., it has the private key to access the wallet), the analysis of ownership is straightforward because a third-party storage provider is not involved.

The determination of ownership is more challenging when an entity holds its digital assets indirectly through a third party, such as an exchange or a custodian that stores in its digital wallets the private keys that provide access to the digital assets. If this is the case, the entity needs to assess whether it owns the digital assets or has a right to obtain digital assets from the third party.

The evaluation of whether the entity or the third party is the owner of the digital assets requires consideration of the terms in the agreement, the laws governing the jurisdiction(s) in which the third party operates and how the third party manages and stores the digital assets.

Entities need to carefully evaluate digital assets held through a third-party custodian or exchange.

Questions an entity may consider when assessing ownership include:

- Who is the legal owner of the digital assets?
- Does the agreement with the third party establish a custodial relationship?
- What legal and regulatory requirements apply to the custodian with respect to the custody of digital assets it holds on behalf of others? How does the custodian satisfy those requirements?
- Does the agreement specify who owns the digital assets held in the third party's digital wallets?
- If the third party files for bankruptcy protection, who has claim to the entity's digital assets held in the third party's digital wallet?
- Does the third party commingle its customers' digital assets with digital assets it owns?
- Can the third party sell, transfer, loan, encumber or pledge digital assets held in its digital wallets on the customer's behalf to another party without being instructed to do so by the entity?
- Can customers of the third party withdraw their digital assets from the third party's digital wallet at any time and for any reason? If not, what are the reasons preventing customers from withdrawing digital assets under custody?
- Who bears the risk of loss if the digital assets under custody are lost due to a security breach, hack, theft or fraud?
- Does access to customers' digital assets in the third party's digital wallet require a signature authorization by both the entity and the third party?

How we see it

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

Question 10 of the AICPA Guide provides a list of factors an entity may consider when determining whether it should recognize the digital assets held in a third-party hosted wallet. Furthermore, Question 10 highlights that an analysis of the characteristics of an asset as defined by Statement of Financial Accounting Concepts No. 8, *Elements of Financial Statements*, may also be helpful in determining which party — the entity or the third party — should recognize digital assets held in a hosted wallet.

If an entity concludes that it has a right to obtain digital assets rather than ownership of the digital assets, judgment is required to determine the appropriate accounting. That is, the accounting for the right to a digital asset may be different than that for ownership of a digital asset. For example, an entity would need to determine whether the right to obtain digital assets includes an embedded derivative that requires bifurcation pursuant to ASC 815.[2] In determining the appropriate recognition and measurement, the entity should 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 digital assets to adequately settle the entity's claims).

Specialized industry guidance

Investment companies

Investment companies generally account for their investments in digital assets as "other investments" in accordance with ASC 946-325. Under this guidance, these investments are subsequently measured at fair value. Investment companies that hold crypto assets are subject to the enhanced disclosure requirements of ASC 350-60.

Brokers and dealers

Entities may facilitate the buying, selling and storing of digital assets for their customers, similar to brokers and dealers in securities. They may provide any combination of services, including:

- Marketing and facilitating the purchase and sale of digital assets on behalf of customers
- Providing a source of market liquidity (market makers) by standing ready to buy digital assets from or sell digital assets to their customers
- Providing "digital wallet services" to allow customers to store and manage digital assets

These entities may hold "inventory" in their own account for sale to customers in connection with market-making activities and proprietary positions, or they may offer digital wallet services for storing the private keys to the digital assets that their customers purchase.

ASC 940 provides accounting and reporting guidance for brokers and dealers in securities.[3] Under that guidance, a broker-dealer's security positions held for its own account, including both inventory and obligations for short inventory positions, are initially and subsequently measured at fair value, with any unrealized gains or losses resulting from remeasurement recorded in earnings.

Questions 13,14 and 15 of the AICPA Guide provide recognition, measurement and presentation guidance for digital assets held by broker-dealers in the scope of ASC 940. As noted in the following excerpt from the AICPA Guide, an SEC registrant that determines it is in the scope of ASC 940 should consider preclearing that conclusion and its application with the SEC's Office of the Chief Accountant:

> *"Q&As 13–15 do not address how an entity determines whether it is within the scope of FASB ASC 940 and the Broker-Dealer guide. FASB's Emerging Issues Task Force (EITF), in Issue 06-12 considered providing additional guidance on how to determine whether an entity is included in the scope of the Broker-Dealer guide; however, no consensus was reached. The EITF observed that this is an issue for which there is diversity in practice.*
>
> *If an entity that is an SEC filer, or plans to become an SEC filer, reaches a conclusion that it is within the scope of FASB ASC 940 and the Broker-Dealer guide, it should consider discussing such a conclusion with the SEC's Office of the Chief Accountant. In addition, any entity that applies broker-dealer guidance in FASB ASC 940 and the Broker-Dealer guide should (a) not selectively apply certain portions of FASB ASC 940 and the Broker-Dealer guide; rather, it should apply all the guidance, and (b) consider the discussion of the SEC's financial responsibility rules provided in the Joint Staff Statement on Broker-Dealer Custody of Digital Asset Securities. The SEC and Financial Industry Regulatory Authority (FINRA) staffs have not provided guidance on how a broker-dealer may demonstrate physical possession or control with respect to a digital asset security, nor have they provided guidance on how a broker-dealer may engage in a digital asset business in compliance with the financial responsibility rules. Moreover, these Q&As do not address other broker-dealer regulatory questions (for example, the deduction from net capital for digital assets or digital asset securities held by a broker-dealer on a proprietary basis)."*

Initial recognition and measurement

An entity should evaluate the nature of the transaction through which it obtains digital assets to determine their initial accounting. For example, crypto assets and digital assets in the scope of ASC 350-30 that are acquired individually or in a group that is not a business are recognized at cost in accordance with ASC 350-10 (which references the asset acquisition guidance in ASC 805-50).

However, digital assets may be obtained in other ways. Entities will need to consider other relevant accounting guidance when determining their initial accounting, including the topics discussed below. Judgment may be required, and other US GAAP may apply depending on an entity's facts and circumstances.

Digital assets received as consideration for goods or services provided

When evaluating how to account for digital assets received as consideration in exchange for goods or services, an entity should first determine whether it has a contract with a customer in the scope of ASC 606. 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."

If the entity determines that the transaction is in the scope of ASC 606, it should apply all aspects of that standard to the transaction (i.e., recognition, measurement, presentation and disclosure). Digital assets received as consideration in exchange for goods or services should be evaluated as noncash consideration under the guidance. To determine the transaction price for the contract, an entity should measure the estimated fair value of the noncash consideration at contract inception, the date that all the criteria of ASC 606-10-25-1 are met. Any subsequent changes in fair value after contract inception would not affect the transaction price. For more information on accounting for noncash consideration received from a customer for goods or services, refer to section 5.6 of our FRD, *Revenue from contracts with customers (ASC 606)*.

If an entity concludes that its receipt of digital assets is not the result of a contract with a customer and therefore not in the scope of ASC 606, it needs to determine the appropriate accounting guidance to apply, including consideration of ASC 610-20 and ASC 845.

Hard forks and airdrops

A hard fork results from a change in the software of an existing blockchain network that is not adopted by all nodes. After a hard fork, there are two different blockchains and blockchain networks:

<table>
<tr><th>Original chain</th><th>New chain</th></tr>
<tr><td>The original blockchain network is composed of nodes that operate the original software.</td><td>The new blockchain network is composed of nodes that operate the new software.</td></tr>
<tr><td colspan="2">The original blockchain and the “forked” blockchain share the same history of transactions that occurred before the hard fork event.</td></tr>
<tr><td>After the hard fork event, the original blockchain network records only transactions that are compatible with the original software and occur on its blockchain.</td><td>After the hard fork event, the “forked” blockchain network records only transactions that are compatible with the new software and occur on its blockchain.</td></tr>
<tr><td colspan="2">Network participants with a private key that controls access to the digital assets on the original blockchain also gain access to units of a new digital asset that exists on the forked blockchain.</td></tr>
</table>

In an airdrop of digital assets, a random selection of wallet addresses, or a specified list of wallet addresses, receive digital assets free of charge to promote awareness and/or adoption of the new digital asset.

Accounting for new digital assets granted to an entity in a hard fork or airdrop event can present several challenges. As noted above, under ASC 350-10, an entity recognizes a digital asset when it is acquired (i.e., generally as either a crypto asset under ASC 350-60 or as an intangible asset under ASC 350-30). However, in a hard fork or airdrop, an entity may gain the opportunity to access new digital assets without its knowledge or permission and at no cost. The digital assets resulting from these events may be very thinly traded and have little or no value. A holder that is granted the right to new digital assets in a hard fork or airdrop should determine whether, when and how to recognize those digital assets, and disclose its related accounting policy, as applicable.

How we see it

Entities need to carefully evaluate whether the digital assets they receive in a hard fork or airdrop are in the scope of ASC 350-60, even though they may incur no cost to obtain such assets. That is because ASC 350-60 requires remeasurement at fair value in subsequent reporting periods.

Fair value measurement considerations

Fair value measurement is required when a digital asset is held:

- As a crypto asset in the scope of ASC 350-60
- As an "other investment" by an investment company in the scope of ASC 946
- By a broker-dealer in the scope of ASC 940
- As an intangible asset in the scope of ASC 350-30 by an entity that is not in the scope of ASC 946 or ASC 940, and it is tested for impairment (ASC 350-30 requires a comparison of the fair value of the digital asset to its carrying amount as the measure of impairment)

The application of several key aspects of the fair value framework in ASC 820 in the context of digital assets is discussed below. Refer to our **FRD, *Fair value measurement***, for comprehensive guidance on applying ASC 820.

Identifying the principal market

A fair value measurement contemplates an orderly transaction to sell the asset in its principal market. ASC 820 defines "principal market" as the market with the greatest volume and level of activity for the asset or liability. The determination of the principal market (and, as a result, the market participants in the principal market) is made from the perspective of the reporting entity.

In determining the fair value of a digital asset, an entity needs to identify its principal market or, in the absence of a principal market, the most advantageous market (i.e., the market that maximizes the amount that would be received to sell the asset). The market with the greatest volume and level of activity that an entity has access to for the digital asset is generally the entity's principal market for that digital asset. This determination may require an assessment of whether there are any barriers that prevent the entity from accessing a particular market.

An entity may identify different principal markets for different types of digital assets based on where and how it transacts in those digital assets. Further, different entities may identify different principal markets for the same digital asset depending on which markets those entities normally transact in or otherwise have access to.

How an entity measures the fair value of a digital asset depends 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 digital assets (e.g., bitcoin, ether) generally trade with sufficient frequency and volume to be considered actively traded on exchanges or over-the-counter markets, other digital assets may not.

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 contrary, the market in which an entity normally transacts to sell an asset is presumed to be the principal or most advantageous market.

An entity should also evaluate whether there are any indicators that transactions in the principal market are not orderly. If there are, the entity needs to assess whether that market provides relevant and reliable price and volume information. Circumstances that may indicate that a transaction is not orderly include:

- The seller is in or near bankruptcy or receivership (i.e., the seller is distressed).
- The seller was required to sell to meet regulatory or legal requirements (i.e., the seller was forced).

- The transaction price is an outlier when compared with other recent transactions for the same asset.

While an entity need not undertake exhaustive efforts to determine whether a transaction is orderly, information that is reasonably available cannot be ignored.

If an entity determines that the principal market for its digital asset holdings is an active market, ASC 820 requires fair value to be calculated as the quoted price for identical assets multiplied by the quantity held by the entity. 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.

Question: If an entity normally buys and sells digital assets through a broker, can that entity identify a market other than the broker market (e.g., an exchange) as the principal market?

Answer: Generally, no. To overcome the presumption that the market in which the entity normally transacts (i.e., the broker market) is the principal market, the entity would need to obtain sufficient evidence from readily available information indicating that the volume and level of activity in the exchange market is greater than that of the broker market. Performing a sufficient comparison of the volume and the level of activity in these markets is generally not possible because there is typically a lack of publicly available information about the volume and pricing of digital asset transactions in non-exchange markets (e.g., broker markets).

Entities should apply a systematic and rational method to track the cost of digital assets in the scope of ASC 350-30 so they can derecognize them upon sale.

Restrictions on the sale of digital assets

ASC 820 is clear that a fair value measurement should consider the characteristics of the asset that market participants would consider when pricing the asset. ASC 820 indicates that the effect on fair value of a restriction on the sale or use of an asset will depend on whether the restriction is deemed to be a characteristic of the asset or the entity holding the asset. When determining the fair value of its digital asset holdings, an entity should consider restrictions on the sale or use of the digital assets (e.g., restrictions placed on staked assets) and whether the restrictions are taken into consideration by a market participant when valuing the assets. The effect of a restriction on the fair value measurement depends on whether the restriction is deemed to be a characteristic of the asset or the entity holding the asset.

A restriction that transfers with the asset in an assumed sale would generally be deemed a characteristic of the asset and, therefore, would likely be considered by a market participant when pricing the asset. Conversely, a restriction that is specific to the entity holding the asset and does not transfer in an assumed sale is not considered when measuring the fair value of the digital asset. Determining whether a restriction is a characteristic of the asset or the entity requires judgment based on the facts and circumstances.

Fair value hierarchy

Although a fair value measurement contemplates the price in an assumed transaction, pricing information from actual transactions for identical or similar assets and liabilities is considered in determining fair value. ASC 820 establishes a fair value hierarchy to prioritize the inputs used to measure fair value, based on the relative reliability of those inputs. ASC 820 requires that valuation techniques maximize the use of observable inputs and minimize the use of unobservable inputs.

We believe a Level 1 fair value hierarchy classification would be appropriate if the digital asset's valuation is based on a quoted price for the identical asset in an active market. If an entity's principal market for a digital asset is not active or if the digital asset is subject to a restriction that is deemed to be a characteristic of the asset, the measurement would be classified as Level 2 or Level 3, depending on the nature of the adjustments made to the quoted price. An entity may need to change the hierarchy level for a digital asset if market conditions change.

Derecognition

An entity that holds digital assets may transfer them in one of the following ways:

- It may transfer them to a vendor in exchange for goods and services.
- It may sell them for fiat currencies (e.g., bitcoin for US dollars) or exchange them for other types of digital assets (e.g., bitcoin for ether).
- It may sell or transfer them in exchange for other resources (e.g., other digital assets, financial assets, ownership interest in another entity).
- It may lend them to a borrower (see Questions 25 and 26 of the AICPA Guide).

Entities are required to account for the transfer or sale of crypto assets and digital assets in the scope of ASC 350-30 in accordance with the guidance on the derecognition of nonfinancial assets in ASC 610-20, unless a scope exception applies.[4] Therefore, an entity that sells or transfers digital assets to another party should first consider whether the sale or transfer is in the scope of ASC 606, ASC 610-20, ASC 845[5] or other guidance.

If an entity determines it has a contract to sell digital assets that are an output of its ordinary activities to a customer, the contract is likely in the scope of ASC 606. If the transaction is not in the scope of ASC 606 or other guidance that is a scope exception to ASC 610-20, the guidance in ASC 610-20 would likely apply to the transaction. ASC 610-20 refers to the guidance in ASC 606 for certain recognition and measurement principles. The accounting for the sale of a nonfinancial asset is generally the same under both standards, but the financial statement presentation and disclosures are different. Refer to the scoping guidance in section 2 of our **FRD, *Gains and losses from the derecognition of nonfinancial assets (ASC 610-20)***, for considerations on whether the transaction is in the scope of ASC 610-20.

The determination of whether the counterparty is a customer is critical in the evaluation of whether ASC 606 or ASC 610-20 applies. For example, if an entity's business model is to regularly sell digital assets for cash as an output of its ordinary activities, the sale of its digital assets would be in the scope of ASC 606. Consideration received from the sale of digital assets would be recognized as revenue from contracts with customers with the related costs to transfer the digital assets recognized as costs of goods sold. In contrast, an entity that sells digital assets may conclude that the sale of the assets is not an output of its ordinary activities and, therefore, the sale agreement is not a contract with a customer. In this case, the transaction would likely be in the scope of ASC 610-20.

Entities that hold crypto assets at fair value under ASC 350-60 recognize changes in their fair value in net income as they occur. Accordingly, gains or losses are not separately recognized when such crypto assets are sold. Refer to section B.5 of our **FRD, *Intangibles — Goodwill and other***, for additional guidance on accounting for the sale or disposition of crypto assets in accordance with ASC 610-20.

In contrast, consideration received from the sale of digital assets in the scope of ASC 350-30 would be included in the calculation of a gain or loss for each digital asset. Holders of these digital assets will also have to track the cost of the units they purchase or receive at different times, including previously recorded impairment losses, and use the appropriate cost for each unit of digital asset upon derecognition when they sell the digital asset or exchange it for other goods or services. Furthermore, units of digital assets are fungible, and, for that reason, we understand that entities may not be able to specifically identify units of a digital asset they hold in their wallet(s). An entity that sells a portion of its digital asset holdings should apply a systematic and rational method to track the cost of the units of digital assets sold for purposes of derecognizing them. This is consistent with Question 8 of the AICPA Guide, which says:

> An *entity may apply the guidance in this circumstance by developing a reasonable and rational methodology for identifying which units were sold and applying it consistently*. *For example, one reasonable and rational methodology could be the first-in, first-out (FIFO) method*.

How we see it

We generally believe that it would be inappropriate for entities holding digital assets in the scope of ASC 350-30 to apply a method that results in the asset's units being remeasured (e.g., average cost) because such an outcome is inconsistent with the cost-less-impairment model applied under that framework. Entities should disclose the cost method applied.

Digital assets received in exchange for other digital assets

A transaction involving the transfer of one digital asset in exchange for another may be in the scope of ASC 606, ASC 610-20, ASC 845 or other guidance.

If an entity transferred digital assets to a counterparty in exchange for another type of digital asset in its ordinary course of business and the transfer is not to an entity in the same line of business to facilitate a sale to a customer, the transaction may be in the scope of ASC 606. If the counterparty in the transaction is not the entity's customer or if the transaction is not considered part of the entity's ordinary activities, the transaction may be in the scope of ASC 610-20.

We believe an entity should apply the guidance in ASC 845 if it concludes that the transaction is a nonmonetary transaction between entities in the same line of business to facilitate sales to customers (e.g., the exchange of bitcoin for ether to facilitate a sale of ether to a third party who is a customer), and the transaction is not in the scope of ASC 606 or ASC 610-20. Entities need to understand the purpose of an exchange of one type of digital asset for a different type of digital asset (e.g., bitcoin for ether) to determine the appropriate guidance to apply.

Disclosures and presentation

Entities should provide disclosures required by the relevant accounting guidance (e.g., ASC 350-60, ASC 350-30, ASC 606, ASC 610-20, ASC 820). Entities should also provide disclosures about risks and uncertainties[6] and any loss contingencies,[7] including for potential illegal acts relating to their digital asset activities.

As a matter of transparency, entities should also provide additional disclosures that are useful to users of the financial statements in evaluating the effect of digital assets on their financial condition and performance, which may include:

Description of holdings	Accounting policies	Market volatility	Risks
A description of the quantity and nature of digital assets holdings and the entity's reason for holding those digital assets	The accounting policies the entity applies (e.g., measurement basis and where transactions are reflected within the statements)	The historical volatility of the digital asset holdings	The risks associated with holding digital assets

Entities are also required to disclose the details of related party transactions pursuant to ASC 850.[8] At the 2018 AICPA National Conference on Banks & Saving Institutions, Wesley Bricker, Chief Accountant of the SEC at the time, highlighted the importance of disclosing transactions with related parties and the resulting balances in his remarks.[9] Entities should strive to be transparent about their involvement in digital assets and related activities, as well as the associated risks. Additionally, they need to use their judgment to make sure they provide sufficient disclosures to enable users of financial statements to understand the effect of holding digital assets on their financial position, financial performance and cash flows.

Entities should be transparent about their involvement in digital assets and related activities, as well as the associated risks.

Statement of cash flows

ASC 350-60 requires an entity to classify as cash flows from operating activities cash receipts from the sale of crypto assets that it receives as noncash consideration in the ordinary course of business and converts nearly immediately into cash. Refer to Appendix B of our **FRD, *Intangibles – Goodwill and other***, for additional guidance.

For all other transactions involving crypto assets and digital assets in the scope of ASC 350-30, entities should apply the guidance in ASC 230, *Statement of Cash Flows*, to determine the appropriate classification of cash flows as operating, investing or financing activities according to their nature and purpose, based on an entity's facts and circumstances. Cash flows that are classified as an investing or financing activity should be presented on a gross basis in the statement of cash flows unless they are eligible for net presentation. Refer to section 2.3 of our **FRD, *Statement of cash flows***, for examples of when net presentation may be appropriate.

How we see it

Entities need to use judgment to determine how much information to disclose to help users of financial statements understand the effect of transactions in digital assets on their financial position, financial performance and cash flows.

Considerations for certain digital assets and related transactions

Mining companies

Blockchain networks that use a proof-of-work consensus protocol rely on miners that compete to validate and add blocks of transactions to the distributed ledger. To incentivize these miners to compete in processing the transactions for the next block, the winning miner receives transaction fees and a block reward. The transaction fees are paid by the transferor from its digital wallet, and block rewards are newly created digital asset units granted to the miner by the blockchain. An entity should evaluate the guidance in ASC 606 to determine how to recognize the transaction fees and block rewards.

Determining whether the entity has a contract with a customer to transfer goods or services in exchange for consideration may be straightforward for transaction fees paid by transferors. However, the determination may be more challenging for block rewards because they are issued by the blockchain's predetermined protocol, and therefore, there is not an identifiable party. As a result, a mining entity may apply different accounting models for transaction fees and block rewards because the facts and circumstances differ.

Transaction fees

If an entity concludes that mining is an output of its ordinary activities, it should apply the guidance in ASC 606 to account for transaction fees. Often, when a block is successfully mined, the contract criteria in ASC 606 have been met. That is, (1) both the miner and the transferor have approved the arrangement, (2) both the miner and the transferor have performed their respective obligations, (3) each party's rights and the payment terms have been identified, (4) the miner has received payment for its services (i.e., collection is probable since it has already occurred) and (5) the arrangement has commercial substance since the miner has satisfied its performance obligation to the transferor by validating the block. However, all entities should carefully evaluate their individual facts and circumstances to determine when the ASC 606 contract criteria have been met.

Block rewards

Block rewards are distributed by the blockchain network's protocol, and therefore, there is typically not an identifiable party that is contracting with the miner to obtain goods or services in exchange for consideration (i.e., no enforceable rights and obligations). A mining entity that determines 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.

In the absence of specific guidance, we believe it would be appropriate for a mining entity to apply the recognition and measurement guidance in ASC 606 by analogy to account for block rewards. However, the mining entity presents the block rewards separately from its revenue from contracts with customers in the statement of comprehensive income (or provides separate disclosure).

Question 27 of the AICPA Guide also addresses the accounting for transaction fees and block rewards in mining arrangements.

Mining pools

As participation in a proof-of-work blockchain increases, the network's protocol adjusts to make it more difficult for miners to solve the cryptographic algorithm that results in a new block reward. Some miners may form mining pools and combine their computing power to increase the pool's chances of solving the network's algorithm and earning a block reward. Mining pools are typically comprised of participants who allow their computing power to be used by the pool and pool operators who distribute the work among the participants and maintain the pool's administrative functions (e.g., calculating the reward to be distributed to each participant based on a predetermined formula). Generally, pool participants are compensated based on the amount of computing power they provide.

Since mining pool arrangements are complex, the accounting guidance applied by a participant will depend on the facts and circumstances. A mining pool participant should first consider whether the arrangement with the pool operator is a lease under ASC 842. If the arrangement allows the pool operator to direct the use of the computing infrastructure and obtain substantially all the asset's economic benefits, the participant may conclude it is a lessor in a leasing arrangement. However, if the participant retains the ability to direct the use of its computing infrastructure, the participant is likely to conclude that the arrangement is not a lease under ASC 842.

If the arrangement is not a lease, the participant should evaluate whether the arrangement is in the scope of ASC 606 or other applicable accounting guidance. In doing that, the participant should first identify the counterparty for its services. That is, the participant needs to determine whether it provides mining services directly to the blockchain network (e.g., using computing power to solve the hash, validate new transactions and add the new block to the blockchain) or to the mining pool operator (e.g., provides computational power to facilitate the pool operator's mining activities). The participant's evaluation should consider the activities that comprise its service, the individual terms and conditions of the arrangement, and how the participant is compensated for its services.

Because a mining pool arrangement involves multiple parties, the participant should consider the principal versus agent guidance in ASC 606 to help inform its identification of the counterparty for its services. As part of the evaluation, the participant should consider whether the operator controls the mining services that are provided to the blockchain network.

- If the participant concludes the blockchain network is its counterparty (i.e., the pool operator is an agent arranging for the participant to provide services to the blockchain), we believe it is appropriate for the participant to apply ASC 606 by analogy to the transaction and recognize its proportionate share of block rewards on a gross basis with any amounts paid to the mining pool operator recorded as expense. Refer to our discussion on accounting for mining transactions by analogy to ASC 606 above.

- If the participant concludes the pool operator is its counterparty (i.e., the participant is providing computing power to the pool operator, assisting the operator in providing services to the blockchain), it should recognize revenue for the amount the participant is entitled to receive from the operator, which is typically net of any payments made by the participants to the operator.

Question 28 of the AICPA Guide also addresses the accounting for the arrangement.

Staking

Other blockchains, such as Cosmos and Tezos, are governed by a proof-of-stake consensus protocol, under which a validator can contribute a specified number of digital assets for a period of time to the blockchain (or stake) for a chance to earn the right to validate the next block and earn block rewards. The probability of being chosen to validate the next block is generally proportional to the amount of digital assets at stake (i.e., the more digital assets at stake, the higher the chances of being chosen as the validator).

A proof-of-stake protocol is a less resource-intensive alternative to the proof-of-work model, which requires miners to use large amounts of computing power to solve cryptographic algorithms in exchange for a reward.

In a proof-of-stake network, entities engage directly by staking their own digital assets. Some networks may use a variation of the proof-of-stake protocol that allows entities to delegate their stake to another party that acts as a validator. The delegating entity is commonly referred to as the delegator, and the other party is commonly referred to as the lead validator. The digital assets at stake are earmarked on the blockchain and cannot be used for any other purpose in the period during which they are staked. The digital assets are not transferred on the blockchain to another public address when staked (or delegated).

Accounting considerations for rewards obtained through a proof-of-stake protocol are similar to those for rewards obtained by mining companies through a proof-of-work protocol, as discussed above.

Custodians and exchanges

Custodians provide digital wallet services that allow customers to store and manage digital assets. Online trading platforms (exchanges) allow investors to buy and sell digital assets, price orders, execute trades and provide transaction data. Exchanges may also host digital wallets for customers to store their digital assets.

In January 2025, the SEC issued SAB 122[10] to rescind the interpretive guidance in SAB 121,[11] regarding the accounting for obligations to safeguard digital assets that an entity holds for platform users.

The SEC staff previously issued SAB 121 to address the risks and uncertainties associated with the increase in the number of entities that offer platform users the ability to transact in digital assets, often providing services that obligate them or their agents to safeguard users' digital assets. SAB 121 stated that entities that are obligated to safeguard a platform user's digital assets should present a liability and a related asset measured at the fair value of the user's digital assets. It also stated that an entity should include certain disclosures in the notes to the financial statements about the digital assets the entity holds for its users.

The interpretive guidance in SAB 122 clarifies that an entity that has an obligation to safeguard digital assets for others should determine whether to recognize, and how to measure, a liability related to the risk of loss under such an obligation by applying the recognition and measurement requirements for liabilities arising from contingencies in ASC 450-20, *Loss Contingencies*, under US GAAP, or International Accounting Standard (IAS) 37 *Provisions, Contingent Liabilities and Contingent Assets*, under IFRS® Accounting Standards.

SAB 122 also states that entities should continue to consider existing requirements under US GAAP[12] and existing SEC rules[13] to provide disclosures that allow investors to understand an entity's obligation to safeguard digital assets held for others.

SAB 122 is effective and applies to entities on a fully retrospective basis in annual periods beginning after 15 December 2024. The changes can be applied in any earlier interim or annual period included in filings after the effective date. Refer to our To the Point publication, ***SEC staff rescinds guidance on obligations to safeguard crypto assets under SAB 121***, for a summary of SAB 122 and further transition guidance.

Stablecoins

Stablecoins are a subset of digital assets that are pegged to a reference asset (e.g., cash, gold). The main difference between a stablecoin and a digital asset is the mechanism designed to minimize price volatility by linking the value of the stablecoin to that of a more traditional asset such as a fiat currency. The appropriate accounting for stablecoins depends on the specific rights and obligations associated with holding the asset, especially any potential redemption rights held by the holder.

When determining the rights and obligations associated with a stablecoin, a holder may consider the following questions:

Understanding the terms of a stablecoin

- Who issues the stablecoin, and what is the legal form (e.g., debt, equity interest)?
- What is the purpose of the stablecoin, and how does it achieve that purpose?
- What are the rights and obligations of the holder or issuer of the stablecoin?
- If the stablecoin is pegged to or collateralized by other assets, how are the peg/reserve/collateral assets maintained and lien perfected?
- What is the ability of holders to redeem the stablecoin, including:
  - How is the stablecoin redeemed?
  - How often can the holders redeem it?
  - Are there fees associated with redemption?

Because of the variety of terms and conditions associated with stablecoins, it is difficult to provide a general framework for a holder's accounting for a stablecoin. Depending on its terms, the stablecoin may meet the definition of a financial asset that is subject to ASC 310 or ASC 320, represent an ownership in an entity that needs to be evaluated under ASC 321 or ASC 323, or meet the definition of an intangible asset under ASC 350.

Non-fungible tokens

A non-fungible token (NFT) is created, maintained and transferred on a blockchain (typically, a public blockchain, such as the Ethereum) that represents ownership of a digital or physical asset. For instance, NFTs are generally unique or serialized (i.e., one of a limited number) while digital assets like bitcoin are fungible (i.e., trading one bitcoin for another bitcoin leaves you with the same asset).

NFTs are generally used to convey the ownership or rights in purely digital assets, such as songs, pictures, images or art, though they could also be used to reflect rights to tangible assets or the delivery of services. An NFT is created through a process known as "minting" — the same term used to describe the creation of certain digital assets. While an NFT is intangible, it is certifiably unique, similar to many tangibles that exist today, such as a signed baseball with a hologram from a certified authenticator.

Accounting considerations for NFTs

To determine the appropriate accounting model to apply, entities need to evaluate the nature of the NFT activity and the parties involved.

Purchasers of NFTs

An entity that purchases NFTs should identify the rights conveyed through the purchase of the NFT. For example, an NFT may convey the right to an underlying digital asset or physical good. The rights affect the nature of assets recorded and the subsequent measurement. Based on the nature of the assets, the entity may need to determine the fair value of the recognized asset and evaluate it for impairment. Determining fair value often can be difficult because relevant, observable data from active markets may not be available and there may be few other observable inputs (e.g., similar third-party transactions).

Sellers of NFTs

The following are some accounting considerations that an entity may encounter when transacting with NFTs:

- *License of IP* — An entity may license its functional IP to a counterparty that mints and sells NFTs from the licensed content. The terms of the arrangement may involve obtaining an equity stake in or entering into a profit share with the counterparty.
- *Directly minting NFTs* — An entity that mints its own NFTs should assess the accounting for costs incurred to mint the NFTs, including whether those expenses should be recorded in the period incurred or initially capitalized and recognized as expenses in future periods.
- *Operating a platform* — If an entity provides an exchange or marketplace for buying and selling NFTs, the entity should assess whether it is a principal or agent with respect to minting and selling the NFTs.

In each of these situations, an entity needs to assess whether it has contracted with a customer to provide a good or a service that is an output of its ordinary activities in exchange for consideration under ASC 606. If the entity determines that it has a contract with a customer, it should evaluate the timing and amount of revenue to recognize for the contract. If the entity determines that it does not have a contract with a customer, it needs to identify the appropriate accounting guidance to apply, including consideration of ASC 610-20.

When considering the performance obligations in a contract with a customer, an entity should evaluate the rights conveyed by the NFT and whether there are any ongoing performance obligations associated with the initial sale or transfer of the NFT.

Internal control over financial reporting

Entities should maintain appropriate books and records, regardless of whether distributed ledger technology (such as blockchain), smart contracts and other technology-driven applications are used. Likewise, an entity that uses a third party to hold digital assets or execute transactions in those assets on the entity’s behalf should not solely rely on statements from that third party for purposes of maintaining books and records.

An entity’s accounting and technical staff that performs controls relating to investments in or transactions involving digital assets 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 digital asset holdings, they need appropriate controls to make sure the private key used to authorize a transfer of the digital assets 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 digital assets. Further, if the key is stolen, the digital assets could be irreversibly transferred to another party. Internal controls over financial reporting should be in place to prevent or timely detect the loss of digital assets and the loss or destruction of the private key.

A digital wallet (or private key) can be connected to the internet (hot wallet) through 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 needed to address them. For example, such controls can be designed to make sure no single person has knowledge of the entire sequence that makes up the private key. Controls may need to be in place to restrict access to applications, devices and the locations where the devices containing the private key are maintained, to limit the amount and/or frequency of transactions and restrict movement of digital assets to pre-approved public addresses. Entities are expected to maintain a combination of prevent and detect controls. Prevent controls, while important, would not be sufficient by themselves to address these risks.

Understanding and evaluating counterparties and other third parties

Entities that hold their digital assets through a third party such as a custodian or an exchange need to understand the controls the third party has in place to safeguard the private key. Management needs to understand the third party's controls over services such as processing transactions, tracking customer balances and reporting this information to customers to inform its own design of controls related to the associated risks. This may be accomplished by obtaining and reviewing an internal control report from the third party. Management's understanding of the controls at the third party could inform management's design of its controls — for instance, controls related to reconciling its transactions and balances to the public blockchain and verifying that the private key continues to be accessible and operational.

Individuals who perform controls related to safeguarding private keys need to have the necessary competencies.

Entities should 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.

Entities should also apply their know-your-counterparty (KYC) and anti-money-laundering (AML) processes to digital asset transactions as applicable. They should be aware of the heightened risk of criminals trying to take advantage of the anonymity and still nascent regulation in certain digital asset markets.

Understanding and evaluating the risks associated with underlying technology

When information from a digital asset's blockchain is used as part of an entity's controls, management should assess the reliability, completeness and accuracy of the information. Management should gain a sufficient understanding of the underlying technology (e.g., blockchain protocol, smart contracts, digital wallets) to understand how transactions are processed, evaluate related risks, assess the design attributes of those technologies and design appropriate controls to address those risks. Depending on the degree of reliance that management places on information from the blockchain, it may be appropriate for management to identify controls that address how the blockchain functions.

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 digital asset, the value of the digital assets, the unit of account, the cost basis, the measurement and recognition of gains and losses, and impairment (including the identification of interim impairment indicators). Entities also should have controls in place to make sure their disclosures are sufficient.

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 have appropriate authorization controls and segregate duties associated with the initiation of transactions. These controls may include requirements for multiple authorizers, transaction authorization limits and restrictions on which public addresses digital assets may be sent to. Entities should also perform frequent and detailed 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 digital assets because parties to transactions on a blockchain are identified only by their public addresses, which are strings of letters and numbers.

Lastly, applicable laws and regulations and blockchain-based business models continue to evolve. An entity may run afoul of laws or regulations or otherwise engage in 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 such activities, including contingencies relating to pending or threatened litigation and noncompliance with applicable laws and regulations.

Endnotes:

[1] The ASC Master Glossary defines intangible assets other than goodwill as "assets (not including financial assets) that lack physical substance."

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

[3] ASC 940-10-15-2.

[4] ASC 350-10-40-1.

[5] ASC 606-10-15-2(e) provides a scope exception that excludes nonmonetary exchanges between entities in the same line of business to facilitate sales to customers or potential customers from the scope of ASC 606. Accordingly, the scope of ASC 845 includes exchanges of products that are held for sale in the ordinary course of business to facilitate sales to customers (i.e., parties outside of the exchange), while the scope of ASC 606 includes transfers to customers of goods or services that are an output of an entity's ordinary activities in exchange for noncash consideration.

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

[7] ASC 450, *Contingencies*.

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

[9] Wesley Bricker, former Chief Accountant, Office of the Chief Accountant, *Remarks before the AICPA National Conference on Banks & Savings Institutions,* dated 17 September 2018: **SEC.gov | Remarks before the AICPA National Conference on Banks & Saving Institutions**.

[10] Staff Accounting Bulletin No. 122: **https://www.sec.gov/rules-regulations/staff-guidance/staff-accounting-bulletins/staff-accounting-bulletin-122.**

[11] Staff Accounting Bulletin No. 121: **https://www.sec.gov/oca/staff-accounting-bulletin-121.**

[12] ASC 450-20, *Loss contingencies*, and ASC 275, *Risks and uncertainties* (or in IAS 1).

[13] Items 101, 105 and 303 of Regulation S-K.