No. 2022-07
30 June 2022

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. The FASB is now considering standard setting in this area.
- Crypto assets generally meet the definition of indefinite-lived intangible assets under ASC 350 and are initially measured at cost and tested for impairment.
- When investments in crypto 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 transaction 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

The Financial Accounting Standards Board (FASB) recently added a project to its technical agenda to consider the accounting for and disclosure of certain digital assets in response to calls from stakeholders. Many stakeholders said the current accounting for certain digital assets as intangible assets, carried at cost and evaluated for impairment each period, does not reflect the economic reality of those assets or provide users of the financial statements with decision-useful information.

Readers should monitor any standard-setting, regulatory and technological developments that may affect the accounting and control processes related to digital assets.

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

Background

"Digital assets" is an umbrella term for a wide range of assets that is typically powered by blockchain technology. These assets derive their name from their reliance on cryptography to verify and secure transactions on a ledger maintained by a decentralized network of participants. Some digital assets are nonfungible and represent ownership of a digital or physical asset (e.g., nonfungible tokens, or NFTs). Other digital assets are fungible and may entitle the holder to an underlying good or service from an identifiable party (e.g., utility tokens) or serve purely as a medium of exchange (e.g., crypto assets).

The characteristic that distinguishes crypto assets from other digital assets is their intended use as a medium of exchange. A crypto asset provides no rights or privileges to the holder and imposes no obligations on the holder. It has no intrinsic value and is not backed by any asset. Unlike government-issued fiat currencies that are considered legal tenders, crypto assets generally are not issued by or accepted as legal tender by sovereign nations. The holder of a crypto asset may only realize an economic benefit by finding a willing buyer that will accept it in exchange for another asset (e.g., cash, goods, services). Examples of crypto assets include bitcoin, ether, bitcoin cash and litecoin.

The AICPA's Practice Aid (the AICPA Guide), *Accounting for and auditing of digital assets,*[1] which is intended to provide nonauthoritative guidance on how to account for digital assets, clarifies that crypto assets generally do not represent any of the following:

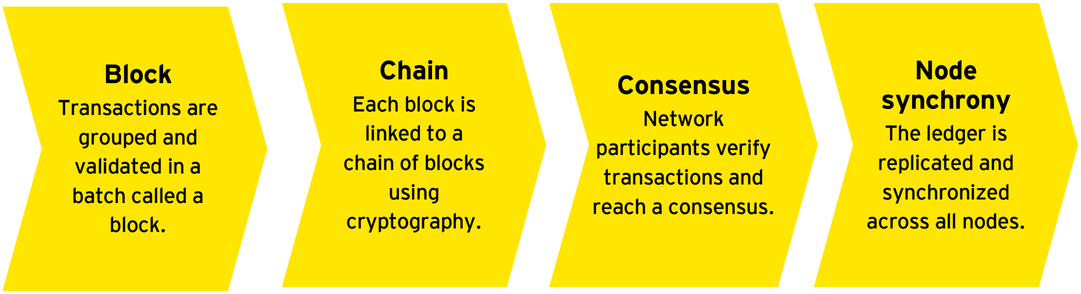
- A security under the US Securities Act of 1933 or the Securities Exchange Act of 1934
- A contract between the holder and another party
- An obligation issued or backed by a central government or jurisdictional authority

Stakeholders generally agree that crypto assets 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, specialized entities such as investment companies in the scope of ASC 946, *Financial Services — Investment Companies*, account for their investments in crypto assets at fair value, like their other investments.

Blockchain and digital assets

Digital assets are based on blockchain technology, a form of distributed ledger technology that keeps a record of every transaction across a network.

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. A miner that does this is rewarded with a newly issued digital asset. Bitcoin blockchain is an example of a proof-of-work network.

In a proof-of-stake network, users enter into smart contracts that put their digital assets at stake to operate nodes on the network and become validators. The network randomly chooses validators 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). Validators temporarily contribute, or stake, an amount of native digital assets (e.g., ether is the native crypto 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 receive a newly issued digital asset 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).

Smart contracts on a blockchain 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.

It is important to distinguish between crypto assets and other digital assets that provide more than purely a medium of exchange. These digital assets may provide holders with a utility, such as access to a good or service from a counterparty, ownership rights in an entity (e.g., voting rights, rights to participate in profits), rights to payments in fiat currencies or rights similar to traditional financial instruments, such as equity shares or debt instruments. They may also provide a digital representation of an ownership interest in an underlying asset such as real estate, artwork or intellectual property. These types of digital assets will likely have different financial reporting considerations or regulatory implications than those of crypto assets.

Market trends

Decentralized finance (DeFi), which refers to the execution of financial transactions on a blockchain using smart contracts without the use of traditional intermediaries, has seen increased adoption. Other market activities include:

- **Traditional products on chain**: Companies are offering smart contract-based savings accounts, borrowing and lending agreements, exchanges and marketplaces.
- **Institutional interest:** Companies, particularly investment funds, are investing in crypto assets and diversifying holdings beyond the higher market capitalization assets, such as bitcoin and ether.
- **Digital assets as payment:** More companies are accepting digital assets as a payment medium, including crypto assets and stablecoins (see further description below). Many companies convert the assets into fiat currency immediately, while others are exploring holding the assets.

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

A holder’s accounting for crypto assets

In the following sections we focus on the accounting specifically for crypto assets from a holders’ perspective, including the classification, recognition, measurement and derecognition. The accounting for crypto assets should be evaluated based on the nature of the asset, the type of investor and how the asset is held. Specific accounting considerations for other digital assets such as stablecoins and NFTs are discussed later in this publication.

Entities may hold their crypto assets directly or indirectly through a third party. When an entity stores its crypto 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. However, the determination of ownership is more challenging when an entity holds its crypto 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 crypto assets. If this is the case, the entity needs to assess whether it owns the crypto assets or has a right to obtain crypto assets from the third party.

The evaluation of whether the entity or the third party is the owner of the crypto 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 crypto assets.

Questions an entity may consider when assessing ownership include:

- Who is the legal owner of the crypto 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 crypto assets it holds on behalf of others? How does the custodian satisfy those requirements?
- Does the agreement specify who owns the crypto assets held in the third party's digital wallets?
- If the third party files for bankruptcy protection, who has claim to the entity's crypto assets held in the third party's digital wallet?
- Does the third party segregate its customers' crypto assets into a different digital wallet from crypto assets it owns?
- Can the third party sell, transfer, loan, encumber or pledge crypto 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 crypto 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 crypto assets under custody?
- Who bears the risk of loss if the crypto assets under custody are lost due to security breach, hack, theft or fraud?
- Does access to customers' crypto 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 investments in crypto 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 crypto 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[2] — should recognize digital assets held in a hosted wallet.

Classification of crypto assets

Crypto assets meet the definition of intangible assets under ASC 350, even though they have some characteristics that are not typical of intangible assets. For example, unlike typical intangible assets, crypto assets may be traded on exchanges and experience significant price volatility. Also, unlike other intangible assets, units of a particular crypto asset are fungible.

The following table provides our analysis of why crypto assets 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.	Not met: Crypto assets are generally not accepted as legal tender and are not backed by sovereign governments. Crypto assets 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.	Not met: Crypto assets 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.	Not met: Crypto assets are not tangible property because they lack physical substance.
Intangible asset	Intangible assets are assets[3] (not including financial assets) that lack physical substance.	Met: Crypto assets are nonfinancial assets that lack physical substance and are not cash and cash equivalents, financial instruments or inventory.

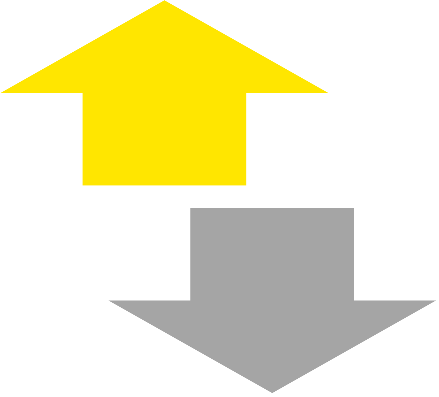
The analysis provided in the above table is consistent with the view provided by Securities and Exchange Commission (SEC) staff at the 2021 AICPA & CIMA Conference on Current SEC and PCAOB Developments. John Vanosdall, who at the time was the Deputy Chief Accountant in the SEC's Office of the Chief Accountant, said 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. In those circumstances, the SEC staff has also said that entities must follow the intangible asset model in ASC 350. However, the SEC 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.

If an entity concludes that it has a right to obtain crypto assets rather than ownership of the crypto assets, judgment is required to determine the appropriate accounting. That is, the accounting for the right to a crypto asset may be different than that for ownership of a crypto asset. For example, an entity would need to determine whether the right to obtain crypto assets includes an embedded derivative that requires bifurcation pursuant to ASC 815.[4] 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 crypto assets to adequately settle the entity's claims).

Recognition and measurement of crypto assets

Entities that do not apply specialized industry guidance

As intangible assets, crypto assets are initially measured at cost. Since there is no limit on their useful life, crypto assets are generally classified as indefinite-lived intangible assets that are not subject to amortization. Instead, they are tested for impairment annually or more frequently if events or circumstances change that indicate that it's more likely than not that the asset is impaired. As a result, holders of crypto assets only recognize decreases in the value of a crypto asset, and any increase in value is recognized only upon disposition.



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

Decreases in value ***are*** recognized while the crypto asset is held.

Questions have arisen about what constitutes an impairment indicator between annual impairment tests. Entities need to assess all relevant events and circumstances that could adversely affect significant inputs used to measure fair value. For example, if a crypto asset 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 should perform a quantitative impairment test. The recognition of impairment losses is based solely on a comparison of the fair value to the cost basis. Once an impairment has been recognized, it cannot be reversed, even if the fair value of the crypto assets recovers above the cost basis within the current reporting period.

When evaluating indefinite-lived intangible assets for impairment under ASC 350, entities need to consider the unit of account (e.g., one bitcoin[5] 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 depends on the specific facts and circumstances, but the fact that holders can transact in individual units (e.g., one bitcoin) of a crypto asset indicates that each unit of crypto assets is likely a separate unit of account. Holders need to track the cost of each unit of crypto assets purchased or received for purposes of performing impairment testing.

Crypto assets received as consideration for goods or services provided

When evaluating how to account for crypto 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). Crypto 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 of the crypto assets (or other digital asset) 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 Financial reporting developments (FRD) publication, *Revenue from contracts with customers (ASC 606)*.

If an entity concludes that its receipt of crypto 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 blockchain networks:

<table>
<tr><th>Original chain</th><th>New chain</th></tr>
<tr><td>The original blockchain is comprised of nodes that operate the original software.</td><td>The new blockchain is comprised 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 records only transactions that occur on its network</td><td>After the hard fork event, the "forked" blockchain records only transactions that occur on its network</td></tr>
<tr><td colspan="2">Investors with a private key that controls access to the old crypto assets on the original blockchain also gain access to units of a new crypto asset that exists on the forked blockchain.</td></tr>
</table>

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

Accounting for new crypto assets 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 crypto assets without its knowledge or permission and at no cost. The crypto 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 crypto assets in a hard fork or airdrop should determine whether, when and how to recognize those crypto assets, and disclose its related accounting policy, as applicable.

Derecognition of crypto assets

An entity that holds crypto 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 crypto assets (e.g., bitcoin for ether).
- It may sell or transfer them in exchange for other resources (e.g., digital assets, financial assets, ownership interest in another entity).

As noted above, we believe that crypto assets meet the definition of intangible assets under ASC 350. ASC 350[6] states that entities should follow the guidance in ASC 610-20 for the derecognition of a nonfinancial asset unless a scope exception applies. Therefore, an entity that sells or transfers crypto assets to another party should first consider whether the sale or transfer is in the scope of ASC 606, ASC 610-20, ASC 845[7] or other guidance.

If an entity determines it has a contract to sell crypto 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 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 crypto assets for cash as an output of its ordinary activities, the sale of its crypto assets would be in the scope of ASC 606. Consideration received from the sale of crypto assets would be recognized as revenue from contracts with customers with the related costs to transfer the crypto assets recognized as costs of goods sold. In contrast, an entity that sells crypto 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. Consideration received from the sale of crypto assets would be included in the calculation of the gain or loss for each crypto asset.

Holders will have to track the cost of units of crypto assets they purchase or receive at different times, including previously recorded impairment losses, and use the appropriate cost for each unit of crypto asset upon derecognition when they sell the crypto asset or exchange it for other goods or services. Furthermore, units of crypto assets are fungible, and, for that reason, we understand that entities may not be able to specifically identify units of a crypto asset they hold in their wallet(s). If an entity sells a portion of its crypto asset holdings, the entity should apply a systematic and rational method to track the cost of the units of crypto assets sold for purposes of derecognizing the crypto assets, consistent with Question 8 of the AICPA Guide, which says:

> An entity may apply the guidance in these circumstance by developing a reasonable and rational methodology for identifying which units of digital assets were sold and apply it consistently. For example, one reasonable and rational approach could be using the first-in, first-out method.

Entities should apply a systematic and rational method to track the cost of the units of crypto assets sold so they can derecognize the assets.

How we see it

We generally believe that it would be inappropriate for entities to apply a method that results in units of crypto assets being remeasured (e.g., average cost) because such an outcome is inconsistent with the guidance in ASC 350. Entities should disclose the cost method applied.

Crypto-to-crypto transactions

A transaction involving the transfer of one crypto 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 crypto assets to a counterparty in exchange for another type of crypto 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 crypto asset for a different type of crypto asset (*e.g.*, bitcoin for ether) to determine the appropriate guidance to apply.

Specialized industry guidance

Investment companies

While a crypto asset meets the definition of an intangible asset under ASC 350, investment companies in the scope of ASC 946 may invest in crypto assets as an asset class for purposes of capital appreciation. Investment companies generally account for their investments in crypto assets as "other investments" in accordance with ASC 946-325. Under this guidance, these investments are subsequently measured at fair value through earnings.

Brokers and dealers

Entities may facilitate the buying, selling and storing of crypto 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 crypto assets on behalf of customers
- Providing a source of market liquidity (market makers) by standing ready to buy crypto assets from or sell crypto assets to their customers
- Providing "digital wallet services" to allow customers to store and manage crypto assets

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

ASC 940 provides accounting and reporting guidance for brokers and dealers in securities.[8] Under that guidance, a broker-dealer's security positions held for its own account, including both inventory and obligations for short of inventory positions, are initially and subsequently measured at fair value, with any unrealized gains or losses resulting from remeasurement recorded in earnings.

Question 13 to Question 15 of the AICPA Guide provide recognition, measurement and presentation guidance for digital assets held by broker-dealers within 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)."*

Fair value measurement of crypto assets

Fair value measurement is required when a crypto asset is (1) held as an "other investment" by an investment company in the scope of ASC 946 or (2) held by a broker-dealer in the scope of ASC 940. Further, in instances where a crypto asset is recognized as an intangible asset by an entity that is not in the scope of ASC 946 or ASC 940, fair value measurement is required for a quantitative impairment analysis under ASC 350.

How an entity measures the fair value of a crypto 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 crypto 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 crypto assets may not.

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

In determining the fair value of a crypto 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 crypto asset is generally the entity's principal market for that crypto asset. This determination may require 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 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 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 crypto asset holdings is an active market, ASC 820[9] 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.

When determining the fair value of its crypto asset holdings, an entity should consider restrictions on the sale or use of the assets (e.g., restrictions placed on staked assets) and whether the restrictions are taken into account 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 does not transfer in an assumed sale and therefore is not considered when measuring fair value. Determining whether a restriction is a characteristic of the asset or the entity requires judgment based on the facts and circumstances.

Level 1 fair value hierarchy classification would be appropriate if the crypto 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 crypto asset is not active or if the crypto 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 crypto asset if market conditions change.

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 crypto 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 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.

In the absence of specific guidance, we believe it would be appropriate for a mining entity to apply ASC 606 recognition and measurement guidance 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 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 crypto 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 crypto assets at stake (i.e., the more crypto 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 crypto 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 crypto 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 crypto 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.

Disclosures and presentation

Entities should provide disclosures required by the relevant accounting guidance (e.g., ASC 350, ASC 606, ASC 610-20, ASC 820). Entities should also provide disclosures about risks and uncertainties[10] and any loss contingencies,[11] including for potential illegal acts relating to their crypto 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 crypto 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 crypto assets holdings and the entity's reason for holding those crypto assets	The accounting policies the entity applies (e.g., measurement basis and where transactions are reflected within the statements)	The historical volatility of the crypto asset holdings	The risks associated with holding crypto assets

Entities are also required to disclose the details of related party transactions pursuant to ASC 850.[12] At the 2018 AICPA National Conference on Banks & Saving Institutions, Wesley Bricker, who at the time was the SEC's Chief Accountant, highlighted the importance of disclosing transactions with related parties and the resulting balances in his remarks.[13]

Entities should strive to be transparent about their involvement in crypto 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 crypto assets on their financial position, financial performance and cash flows.

Statement of cash flows

The cash receipts and payments related to crypto assets should be classified as operating, investing or financing transactions according to their nature and purpose as prescribed by ASC 230, *Statement of Cash Flows*. If the cash receipts and payment are classified as an investing or financing activity, they should be presented gross in the statement of cash flows unless they are eligible for net presentation. See 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 crypto assets on their financial position, financial performance and cash flows.

Digital assets and related transactions

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.

The SEC staff recently issued Staff Accounting Bulletin (SAB) No. 121,[14] which expresses the staff's views on the accounting for obligations to safeguard "crypto assets"[15] that an entity holds for others. It states that entities responsible for safeguarding these assets for customers should present a liability to reflect the obligation to safeguard the assets, measured at initial recognition and each reporting date at the fair value of the assets held for customers. Additionally, the staff stated that a corresponding asset should be recognized, similar to an indemnification asset as described in ASC 805, at the time the liability is recorded. The asset should also be measured at initial recognition and each reporting date at the fair value of the assets held on behalf of customers.

SAB 121 applies to existing SEC registrants and certain other entities. However, it is not required to be applied by private companies. See our **To the Point publication, *SEC staff issues guidance on obligations to safeguard crypto assets***,[16] for a summary of SAB 121.

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 crypto 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 crypto 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 crypto 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.

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. Management should design and implement controls to address all 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 that makes 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

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. This may be accomplished by obtaining and reviewing an internal control report from the third party.

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. They should be aware of the heightened risk of criminals trying to take advantage of the anonymity and weak regulation in certain digital asset markets.

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

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. They should also design well-controlled 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] AICPA & CIMA, *Accounting for and auditing of digital assets*, Question 1: https://www.aicpa.org/resources/download/accounting-for-and-auditing-of-digital-assets-practice-aid-pdf.

[2] Third-party entities should consider whether the service provided to customers would be in the scope of the guidance in Staff Accounting Bulletin No. 121.

[3] ASC 350-30-25-4 states, "Intangible assets that are acquired individually or with a group of assets in a transaction other than a business combination or an acquisition by a not-for-profit entity may meet asset recognition criteria in" CON 5. One of the four criteria in CON 5 is that the item meets the definition of an element of the financial statements (e.g., an asset). The definition of such elements is included in CON 8.

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

[5] Crypto assets 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).

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

[7] 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.

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

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

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

[11] ASC 450, *Contingencies*.

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

[13] 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.

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

[15] Footnote 3 of SAB 121 defines that "[f]or purposes of this SAB, the term 'crypto-asset' refers to a digital asset that is issued and/or transferred using distributed ledger or blockchain technology using cryptographic techniques".

[16] *To the Point - SEC staff issues guidance on obligations to safeguard crypto assets*: https://www.ey.com/en_us/assurance/accountinglink/to-the-point---sec-staff-issues-guidance-on-obligations-to-safeg.

EY | Building a better working world

SCORE No. 16494-221US

ey.com/en_us/assurance/accountinglink

EY exists to build a better working world, helping to create long-term value for clients, people and society and build trust in the capital markets.

Enabled by data and technology, diverse EY teams in over 150 countries provide trust through assurance and help clients grow, transform and operate.

Working across assurance, consulting, law, strategy, tax and transactions, EY teams ask better questions to find new answers for the complex issues facing our world today.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation are available via ey.com/privacy. EY member firms do not practice law where prohibited by local laws. For more information about our organization, please visit ey.com.

Ernst & Young LLP is a client-serving member firm of Ernst & Young Global Limited operating in the US.

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax or other professional advice. Please refer to your advisors for specific advice.