Practice aid

Association of International Certified Professional Accountants™

AICPA® CIMA®

Accounting for and auditing of digital assets

Digital Assets Working Group

Accounting Subgroup

Matthew Schell, *Chair*
Crowe LLP

Michael Bingham
US Government Accountability Office

Brian Fields
KPMG LLP

Rahul Gupta
Grant Thornton LLP

Kevin Jackson
PwC

Jin Koo
BDO USA LLP

Corey McLaughlin
Cohen & Company

Lan Ming
Ernst & Young LLP

Christopher Moore
Crowe LLP

Mark Murray
RSM US LLP

Amy Park
Deloitte & Touche LLP

Beth Paul
PwC

Aleks Zabreyko
Connor Group

Auditing Subgroup

Amy Steele, *Chair*
Deloitte & Touche LLP

Michael Bingham
US Government Accountability Office

Jay Brodish
PwC

Damon Busse
Baker Tilly Virchow Krause, LLP

Mary Grace Davenport
PwC

Angie Hipsher-Williams
Crowe LLP

Michael Kornstein
Ernst & Young LLP

Sara Krople
Crowe LLP

Bryan Martin
BDO USA LLP

Dylan McDermott
Coinbase

Shelby Murphy
Deloitte & Touche LLP

Christian Randall
Cohen & Company

Jay Schulman
RSM US LLP

Robert Sledge
KPMG LLP

Jagruti Solanki
Aprio

AICPA Senior Committees

Financial Reporting Executive Committee

Angela Newell, *Chair*
Kelly Ardrey Jr.
Michelle Avery
Lee Campbell
Cathy Clarke

Mark Crowley
Sean Lager
Mark Northan
Bill Schneider
Rachel Simons

Jeff Sisk
Dusty Stallings
Lynne Triplett
Mike Winterscheidt
Aleks Zabreyko

Assurance Services Executive Committee

Jim Burton, *Chair*
Christine Anderson
Daniel Balla
Jennifer Burns

Mary Grace Davenport
Chris Halterman
Elaine Howle
Bryan Martin

Brad Muniz
Dyan Rohol
Kimberly Ellison-Taylor
Miklos Vasarhelyi

Auditing Standards Board

Tracy Harding, *Chair*

AICPA staff

Diana Krupica, *Lead Manager*
Assurance & Advisory Innovation,
AICPA

Ami Beers, *Senior Director*
Assurance & Advisory Innovation,
AICPA

Bob Dohrer, *Chief Auditor*
Audit & Attest Standards
AICPA

Ahava Goldman, *Associate Director*
Audit & Attest Standards
AICPA

Daniel Noll, *Senior Director*
Accounting Standards
AICPA

Amy Pawlicki, *Vice President*
Assurance & Advisory Innovation
AICPA

In addition, the working group gratefully acknowledges the contributions of Matthew Sickmiller of the Center for Audit Quality; Sean Prince, Mark Shannon, and Jonathan Sharpe of Crowe LLP; Anna Gosine of Ernst & Young LLP; Jeremy Goss, Mike Santay and Dan Voogt of Grant Thornton; Ian Wildenborg of KPMG LLP; Rick Day of RSM US LLP; and the following industry reviewers: Jeremy Dillard of Singer Lewak; Monica Blocker and Grant Casteel of Houlihan Capital; Timothy Singh of Circle; Matt Perona of Polychain Capital; Teddy Fusaro of Bitwise Investments; Nadine Taylor of Ripple; and Joey Ryan of Gilded.

Notice to readers

The objective of this practice aid is to develop nonauthoritative guidance on how to account for and audit digital assets under U.S. generally accepted accounting principles (GAAP) for nongovernmental entities and generally accepted auditing standards (GAAS), respectively. This guidance is intended for financial statement preparers and auditors with a fundamental knowledge of blockchain technology. For the purposes of this practice aid, *digital assets* are defined broadly as digital records that are made using cryptography for verification and security purposes, on a distributed ledger (referred to as a *blockchain*). The distributed ledger keeps a record of all transactions on a blockchain network. Digital assets, as defined herein, may be characterized by their ability to be used for a variety of purposes, including as a medium of exchange, as a representation to provide or access goods or services, or as a financing vehicle, such as a security, among other uses. The rights and obligations associated with digital assets vary significantly, as do the terms used to describe them. It is important to note that the accounting treatment for a digital asset will ultimately be driven by the specific terms, form, underlying rights, and obligations of the digital asset.

Digital assets and the associated underlying technology are an evolving area, and the expectations and experiences of stakeholders such as preparers, auditors, and regulators may change accordingly. Therefore, questions, examples, challenges, risks, considerations, and potential procedures listed in this practice aid should not be considered exhaustive. Preparers, auditors, and those charged with governance need to stay abreast of developments and consider the implications of those developments.

The guidance in this practice aid is based on existing professional literature and the experience of members of the Digital Assets Working Group. This nonauthoritative guidance represents the views of the Digital Assets Working Group and AICPA staff. This publication is not approved, disapproved, or otherwise acted on by the Auditing Standards Board, the membership, or the governing body of the AICPA, and are not official pronouncements of the AICPA.

Accounting content

The Financial Reporting Executive Committee (FinREC) is the designated senior committee of the AICPA authorized to speak for the AICPA in the areas of financial accounting and reporting. The accounting guidance in this practice aid has been reviewed by FinREC, who did not object to its issuance.

Auditing content

This information represents the views of AICPA staff based on the input of the Digital Assets Working Group and has not been approved by any senior committee of the AICPA. The auditing portion of this practice aid is an other auditing publication as defined in AU-C section 200, *Overall Objectives of the Independent Auditor and the Conduct of an Audit in Accordance With Generally Accepted Auditing Standards*,[1] and is intended to provide nonauthoritative guidance to auditors. Other auditing publications may help the auditor understand and apply GAAS but have no authoritative status. In applying the auditing guidance included in an other auditing publication, the auditor should exercise professional judgment and assess the relevance and appropriateness of such guidance to the circumstances of the audit.

[1] All AU-C sections can be found in AICPA Professional Standards.

Contents

Accounting subgroup

Questions [Published December 2019]

Contents

Accounting subgroup

Questions [Published October 2020]

NOTE: 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. See NOTE before Q&A 13 for additional information about considerations for an entity that reaches a conclusion that it is within the scope of FASB ASC 940.

NOTE: Q&As 16–21 interrelate and therefore are intended to be read in conjunction with one another.

[2] Refer to the definition of a *crypto asset* in Q&A 1 of this practice aid.

Auditing subgroup

Client acceptance and continuance [Published July 2020]

Introduction

The AICPA formed the Digital Assets Working Group (the working group), a joint working group under the Financial Reporting Executive Committee (FinREC) and the Assurance Services Executive Committee (ASEC), with the objective of developing nonauthoritative guidance for financial statement preparers and auditors on how to account for and audit digital assets under U.S. generally accepted accounting principles (GAAP) for nongovernmental entities and generally accepted auditing standards (GAAS), respectively. The working group is split into two subgroups, one focusing on accounting topics and one focusing on auditing topics.

Each subgroup created a list of topics and prioritized those that it believes are the most relevant or critical for practitioners and accountants. As additional topics are completed, they will be added to this practice aid and posted to aicpa.org. The format of each of the accounting and auditing topics will vary based on the necessary context. For example, some topics will be addressed in question and answer (Q&A) format, whereas others requiring more context will be presented in a narrative format.

Help desk: For additional information on what blockchain technology is and how it is affecting the profession, see the white paper "Blockchain Technology and Its Potential Impact on the Audit and Assurance Profession", as well as AICPA-developed CPE courses related to blockchain: aicpa.org/interestareas/information technology/resources/blockchain.html

In addition, see the blockchain podcast series at aicpa-cima.com/disruption.

Accounting subgroup

The accounting subgroup focused on developing nonauthoritative guidance on accounting for digital assets and related transactions under GAAP. The scope of each question is defined within the question (for example, all digital assets versus digital assets that are classified as indefinite-lived intangible assets). The accounting Q&As do not address other factors such as compliance with laws and regulations.

Although many terms and colloquialisms that describe similar assets may be used to describe digital assets and related transactions, it is critical to consider that the accounting treatment for a digital asset and related transactions will ultimately be driven by the specific terms, form, underlying rights, and obligations of a digital asset. Therefore, the conclusions in any given topic may not be applicable to other types of digital assets that are outside the scope of such topic.

Auditing subgroup

The focus of the auditing portion of this practice aid is to provide nonauthoritative guidance on auditing digital assets under GAAS. Audits of issuers, audits performed in accordance with the PCAOB standards, and non-audit attest engagements are not currently contemplated.

Although auditor independence and ethical requirements should be considered prior to the performance of acceptance or continuance procedures for all engagements, such considerations are not within the scope of this practice aid.

> **Help desk:** For information regarding independence and ethics, see the AICPA Code of Professional Conduct at pub.aicpa.org/codeofconduct/Ethics.aspx.

The digital asset ecosystem is an evolving business environment, presenting practitioners with unique risks and more complex audit challenges ranging from obtaining sufficient appropriate evidence to understanding the complex IT environment of entities within the ecosystem. The guidance herein is not intended to be an exhaustive list of challenges or recommended procedures and does not address certain emerging enterprise use cases for blockchain technology such as supply chain use cases, but rather focuses on the present, most widely adopted use cases.

Although many blockchain applications share some fundamental principles of trust and security through cryptography and decentralization, the design of different blockchains may differ significantly. Some are entirely public and permissionless, while others are private and serve a very narrow purpose. Consequently, it is not practical to address every blockchain. The term blockchain, as used throughout this practice aid, does not refer to any particular application of blockchain technology and instead refers to the broad concept of a decentralized ledger that uses the principles of cryptography to transmit or store value securely. That value is generally in the form of one or more digital assets.

Throughout this practice aid, the term *digital asset ecosystem* is used, which is defined as all entities participating or involved with digital assets. This may include entities engaged in various elements of the ecosystem, including development; maintenance; use (for example, the purchase, sale, investment, trading, or exchange); custody or security (for example, hot or cold wallet providers, qualified custodians, or other custodial services); or validating.

Accounting subgroup

Classification and measurement when an entity purchases crypto assets

Question 1:

How should an entity that does not apply specialized industry guidance (for example, it is not applying FASB *Accounting Standards Codification* [ASC] 946, *Financial Services — Investment Companies*) account for purchases of crypto assets for cash?[3]

For purposes of this Q&A, the term *crypto asset* is specific to the type of digital assets that

a. function as a medium of exchange and

b. have all the following characteristics:

   i. They are not issued by a jurisdictional authority (for example, a sovereign government).

   ii. They do not give rise to a contract between the holder and another party.

   iii. They are not considered a security under the Securities Act of 1933 or the Securities Exchange Act of 1934.

These characteristics are not all-inclusive, and other facts and circumstances may need to be considered.

Examples of crypto assets meeting these characteristics include bitcoin, bitcoin cash, and ether.

Response 1:

The FASB ASC Master Glossary defines *intangible assets* as assets (not including financial assets) that lack physical substance. Accordingly, crypto assets with the previously described characteristics meet the definition of intangible assets and would generally be accounted for under FASB ASC 350, *Intangibles — Goodwill and Other*.

These crypto assets generally would not meet the definitions of other asset classes within generally accepted accounting principles (GAAP), and therefore, accounting for them as other than intangible assets may not be appropriate, as described in the following examples:

- Crypto assets will not meet the definition of *cash* or *cash equivalents* (as defined in the FASB ASC Master Glossary) when they are not considered legal tender[4] and are not backed by sovereign governments. In addition, these crypto assets typically do not have a maturity date and have traditionally experienced significant price volatility.
- Crypto assets will not be *financial instruments* or *financial assets* (as defined in the FASB ASC Master Glossary) if they are not *cash* (see previous discussion) or an ownership interest in an entity and if they do not represent a contractual right to receive cash or another financial instrument.
- Although these crypto assets may be held for sale in the ordinary course of business, they are not tangible assets and therefore may not meet the definition of *inventory* (as defined in the FASB ASC Master Glossary).

[3] This question and answer (Q&A) discusses purchases of certain crypto assets that are owned and held by an entity. Refer to Q&A 10 for a discussion of ownership determination when crypto assets are held through a custodian.

[4] Legal tender is specific to a jurisdiction. For example, the *U.S. Code* states, "United States coins and currency (including Federal reserve notes and circulating notes of Federal reserve banks and national banks) are legal tender for all debts, public charges, taxes, and dues" [*Money and Finance, U.S. Code*, Title 31, Section 5103, "Legal tender"]. This statute means that all forms of money identified within are a valid and legal offer of payment for debts when tendered to a creditor.

Under FASB ASC 350, an entity should determine whether an intangible asset has a finite or indefinite life. FASB ASC 350-30-35-4 states that if no legal, regulatory, contractual, competitive, economic, or other factors limit the useful life of an intangible asset to the reporting entity, the useful life of the asset should be considered indefinite. The term indefinite does not mean infinite or indeterminate. The useful life of an intangible asset is indefinite if that life extends beyond the foreseeable horizon — that is, there is no foreseeable limit on the period of time over which the asset is expected to contribute to the cash flows of the reporting entity.

Entities should consider the factors outlined in FASB ASC 350-30-35-3 when determining the useful life of an intangible asset. If there is no inherent limit imposed on the useful life of the crypto asset to the entity, then the crypto asset would be classified as an indefinite-lived intangible asset.

As intangible assets, these crypto assets purchased for cash would initially be measured at cost.

Recognition and initial measurement when an entity receives digital assets that are classified as indefinite-lived intangible assets

Question 2:

Entity A enters into a contract with a customer to deliver a good or service that is an output of its ordinary activities in a concurrent exchange for a fixed number of a digital asset that will be held in its own account and not through a custodian. At contract inception, Entity A transfers control of the good or service to the customer and concurrently receives the digital asset in return. The digital asset received is accounted for as an indefinite-lived intangible asset and the contract is within the scope of FASB ASC 606, *Revenue from Contracts with Customers*.

How should Entity A account for the receipt of the digital asset as consideration under a revenue contract with a customer?[5]

Response 2:

Entity A would treat the receipt of the digital asset as a form of noncash consideration under FASB ASC 606 when determining the transaction price. Entities should apply all aspects of FASB ASC 606 to the transactions in the scope of that guidance (for example, recognition, measurement, presentation, and disclosure).

To determine the transaction price for the revenue contract, Entity A would measure the noncash consideration (digital asset) at its estimated fair value[6] at contract inception — that is, the date that all the criteria in FASB ASC 606-10-25-1 are met.

As explained in FASB ASC 606-10-32-23, any changes in the fair value of the digital asset after contract inception due to the form of the consideration would not affect the transaction price for the revenue contract. The entity would apply the relevant accounting guidance for the form of noncash consideration to determine how any change in fair value of the digital asset should be recognized after contract inception. For example, an entity may need to consider the application of the subsequent measurement guidance in FASB ASC 350-30 as discussed in Q&As 4, 5, 6, and 7.

[5] Entities with transactions outside of FASB *Accounting Standards Codification* (ASC) 606, *Revenue from Contracts with Customers*, (for example, the sale of property, plant, and equipment to a noncustomer in exchange for digital assets) should look to other relevant generally accepted accounting principles (GAAP), such as FASB ASC 610-20.

[6] As discussed in FASB ASC 606-10-32-22, if the fair value of the noncash consideration is not reasonably estimable, the entity should measure the noncash consideration by reference to the stand-alone selling price of the goods or services promised to the customer.

Question 3:

If the facts in Q&A 2 changed and Entity A were to receive the digital asset in the future rather than concurrently with the exchange of the good or service, what additional considerations, outside of FASB ASC 606, might be necessary for Entity A?

Response 3:

Some transactions may be more complex than the simple concurrent exchange of an entity's good or service for a digital asset. In arrangements that involve the future receipt of a digital asset in exchange for the current delivery of a good or service, entities may need to consider the guidance in FASB ASC 815, *Derivatives and Hedging*, to determine whether the right to receive a digital asset in the future is a derivative or a hybrid instrument containing an embedded derivative.

Subsequent accounting for digital assets classified as indefinite – lived intangible assets

Question 4:

How should an entity account for digital assets that are classified as indefinite-lived intangible assets subsequent to their acquisition?

Response 4:

An indefinite-lived intangible asset is initially carried at the value determined in accordance with FASB ASC 350-30-30-1 and is not subject to amortization.[7] Rather, it should be tested for impairment annually or more frequently if events or changes in circumstances indicate it is more likely than not that the asset is impaired. Paragraphs 18B and 18C in FASB ASC 350-30-35 provide examples of relevant facts and circumstances that should be assessed to determine if it is more likely than not that an indefinite-lived intangible asset is impaired. If an impairment indicator exists and it is determined that the carrying amount of an intangible asset exceeds its fair value, an entity should recognize an impairment loss in an amount equal to that excess. After the impairment loss is recognized, the adjusted carrying amount becomes the new accounting basis of the intangible asset. Refer to paragraphs 15–20 in FASB ASC 350-30-35 for details on the subsequent accounting for intangible assets that are not subject to amortization.

[7] Indefinite-lived intangible assets do not meet the definition of a *financial asset* (as defined in the FASB ASC Master Glossary) or any other eligible items under FASB ASC 825-10-15-4 and therefore are not eligible for the fair value option under that paragraph.

Question 5:

If a digital asset is classified by an entity as an indefinite-lived intangible asset and identical digital assets are reportedly bought and sold on a market at a price below its current carrying value, is this activity an impairment indicator, and if so, should an impairment charge be recorded?

Response 5:

An intangible asset with an indefinite useful life should be tested for impairment annually or more frequently if events or changes in circumstances indicate it is more likely than not that it is impaired. Paragraphs 18B and 18C of FASB ASC 350-30-35 list examples of factors an entity may consider in determining whether it is more likely than not that an indefinite-lived intangible asset is impaired. These examples are not all-inclusive, and other facts and circumstances should be considered. Judgment may be required to identify whether an event has occurred that would result in the need to perform an impairment assessment.

When an identical digital asset is bought and sold at a price below the entity's current carrying value, this will often serve as an indicator that impairment is more likely than not. Entities should monitor and evaluate the quality and relevance of the available information, such as pricing information from the asset's principal (or most advantageous) market or from other digital asset exchanges or markets, to determine whether such information is indicative of a potential impairment.

If an entity determines it is more likely than not that the indefinite-lived intangible asset is impaired, the entity should determine its fair value, following the fair value framework in FASB ASC 820, *Fair Value Measurement*.

If, based on its assessment, the entity concludes that the fair value of the digital asset is less than its carrying value, an impairment loss should be recorded.

Question 6:

If the fair value of a digital asset that is classified as an indefinite-lived intangible asset has declined below the carrying value in the middle of a reporting period (that is, an impairment has occurred), does impairment need to be recorded if the fair value has recovered by the end of the same period?

Response 6:

Yes. Impairment testing of indefinite-lived intangible assets is required whenever events or changes in circumstances indicate it is more likely than not that impairment has occurred. If the entity concludes the fair value of the digital asset is less than its carrying value, an impairment loss is recorded at that time. Pursuant to FASB ASC 350-30-35-20, subsequent reversal of previously recorded impairment losses on indefinite-lived intangible assets is prohibited. This provision applies even if the fair value of the digital asset recovers above the original carrying value within the same accounting period.

Example: ABC Entity holds 1 million units of a digital asset, which it purchased for cash on January 1, 20X1, for $10 per unit. ABC Entity accounts for its holdings of digital asset as an indefinite-lived intangible asset. During the last week of January 20X1, units of the same digital asset were traded on an exchange at prices below ABC Entity's carrying value. After considering the quality and relevance of the available information, ABC Entity concluded that the January

trades indicated that it was more likely than not that its digital asset was impaired. ABC Entity determined that the fair value at that time was $8 per unit based on the guidance in FASB ASC 820. ABC Entity concluded that an impairment loss of $2 million had occurred as of January 31, 20X1.

As of March 31, 20X1 (the balance sheet reporting date), units of the digital asset were traded above ABC Entity's original carrying value. Although this may be an indication that the fair value of the digital asset has increased above the original carrying value as of the reporting date, subsequent reversal of previously recognized impairment is prohibited. Accordingly, ABC Entity's results of operations for the period should include a charge for the impairment loss of $2 million.

Question 7:

How should an entity determine the unit of account when assessing impairment of digital asset holdings accounted for as an indefinite-lived intangible asset?

Response 7:

Entities often engage in multiple acquisitions and dispositions of digital assets during a period. Entities should determine the unit of account for purposes of testing the indefinite-lived intangible asset for impairment by applying guidance in paragraphs 21–27 of FASB ASC 350-30-35. Consistent with FASB ASC 350-30-35-24, because entities usually have the ability to sell or otherwise dispose of each unit (or a divisible fraction of a unit) of a digital asset separately from any other units, entities will generally reach the determination that the individual unit (or a divisible fraction of a unit) represents the unit of account for impairment testing purposes. To perform impairment testing, entities should track the carrying values of their individual digital assets (or a divisible fraction of an individual unit).

When performing the impairment testing for an individual digital asset, the entity should compare the carrying value of that specific asset with its fair value. If an entity determines that an individual unit (or a divisible fraction of a unit) represents the unit of account for impairment testing purposes, it would not be appropriate to perform such comparison for a bundle of digital assets of the same type purchased at different prices. This approach could lead to an inappropriate reduction in the amount of the impairment loss by netting (1) losses on units with carrying values above the current fair value against (2) unrealized gains on units with carrying values below the current fair value.

Practically speaking, entities could perform impairment testing for batches of digital asset units (or divisible fractions of a unit) with the same acquisition date and the same carrying value.

Measurement of cost basis of digital assets that are classified as indefinite-lived intangible assets when derecognized

Question 8:

When selling a portion of an entity's digital asset holdings that are accounted for as indefinite-lived intangible assets, how should an entity determine the cost basis of the units sold?

Response 8:

Entities should track the cost (or subsequent carrying value) of units of digital assets they obtain at different times and use this value for each unit of digital assets upon derecognition when they sell or exchange digital assets for other goods or services. Digital assets typically represent fungible units that can be subdivided into smaller fractional units. It may not be possible to identify which specific units of digital assets were sold or transferred in certain cases. For instance, it may be clear that the number of units of digital assets held has gone down (for example, from 10 units to 9 units in the entity's wallet) but not whether the first, last, or some other unit purchased was the one sold. 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.

Derecognition of digital asset holdings that are classified as indefinite-lived intangible assets

Question 9:

How should an entity account for the sale of digital asset holdings that are accounted for as indefinite-lived intangible assets?

Response 9:

An entity may transfer digital assets by exchanging them for fiat currencies (for example, digital asset X for U.S. dollars), in which case, the seller should assess whether the transaction is with a customer. If the counterparty is a customer (that is, selling digital asset X is an activity that constitutes part of the entity's ongoing major or central operations), an entity should account for the sale under FASB ASC 606 and present the sale as revenue when control of the digital assets sold has transferred. If the counterparty is not a customer (that is, selling digital asset X is not part of the entity's ongoing major or central operations), an entity should account for the sale under FASB ASC 610-20, *Other Income — Gains and Losses from the Derecognition of Nonfinancial Assets*, or FASB ASC 845, *Nonmonetary Transactions*, depending on the nature of the transfer. In those circumstances, any gain or loss upon derecognition would typically be presented net, outside of revenue (net gain or loss as determined by subtracting the cost [or subsequent carrying value] from the measured consideration).

Recognition of digital assets when an entity uses a third-party hosted wallet service

Question 10:

When an entity (the depositor) holds its digital asset in a third-party hosted wallet service (the custodian),[8] should the digital asset be recognized on the financial statements of the depositor or the custodian?

Response 10:

It depends. The digital asset should be recognized on the financial statements of the entity that has control over the digital asset. Determining which entity — the depositor or the custodian — has control[9] of the digital asset should be based on the specific facts and circumstances of the agreement between the depositor and custodian and applicable laws and regulations. In that regard, a legal analysis may be needed to evaluate certain aspects of the agreement, including legal ownership.

The form of the agreement between the depositor and the custodian may vary but often will be included within the terms and conditions or initial account-opening documents provided by the custodian.

In addition to assessing the terms of the agreement, an analysis of the characteristics of an asset as defined by FASB Concepts Statement No. 6, *Elements of Financial Statements*, may help determine which party should recognize the digital asset. Some factors an entity may consider include the following:

- Are there legal or regulatory frameworks applicable to the custodian and the depositor (which may also depend on the jurisdiction)? If so, does the framework specify who the legal owner of the digital asset is?
- Do the terms of the arrangement between the depositor and custodian indicate whether the depositor will pass title, interest, or legal ownership of the digital asset to the custodian?
- When the depositor transfers its digital assets out of the custodian's wallet, is the custodian required to transfer the depositor's original units of the digital asset deposited with the custodian?
- Does the custodian have the right (under contract terms, law, or regulation) to sell, transfer, loan, encumber, or pledge the deposited digital asset for its purposes without depositor consent or notice, or both?
- Would the digital asset deposited with the custodian be isolated from the custodian's creditors in the event of bankruptcy, liquidation, or dissolution of the custodian? If not, do the depositors have a preferential claim in such circumstances?
- Can the depositor withdraw the deposited digital asset at any time and for any reason? If not, what contingencies are associated with the rights to receive the deposited digital asset? Are there technological or other factors that would prevent timely withdrawal notwithstanding contractual, legal, or regulatory rights?
- Are there side agreements affecting rights and obligations of the depositor and the custodian?
- Are there "off-chain" transactions recorded outside of the underlying blockchain that should be considered?
- Is the digital asset held in a multisignature wallet, and if so, what are the digital signatures that are required to execute a transaction? Who holds the private keys to the multisignature wallet and how is ownership evidenced through any applicable account agreements?

[8] For purposes of this Q&A, we assume that the custodian is not subject to any industry-specialized guidance.

[9] *Control* is discussed in various parts of GAAP, such as FASB ASC 606.

- Is the custodian required (by contract, law, or regulation) to segregate the digital assets of depositors from the digital assets owned for the custodian's own account? Does the custodian commingle digital assets of multiple depositors?
- Does the depositor bear the risk of loss if the deposited digital asset is not retrievable by the custodian (for example, due to security breach, hack, theft, or fraud)?
- Could the depositor be impeded by the custodian in any way from receiving all economic benefits of controlling the digital asset, including price appreciation?

The previous list is not exhaustive, and there is no single factor that is considered determinative to the control of the digital asset held through a custodian's digital wallet. Each arrangement should be assessed separately.

If it is determined that the depositor has control over the digital asset, then the depositor should recognize the digital asset in its financial statements.

If it is determined that the depositor does not have control over the digital asset — that is, the custodian has control — then the depositor should recognize a right to receive the digital asset (from the custodian) as an asset in its financial statements. The custodian should recognize the digital asset as its asset and recognize a corresponding liability to return the digital asset to the depositor in its financial statements.

The right to receive the digital asset that is recognized by the depositor and the liability to return the digital asset to the depositor that is recognized by the custodian may require further assessment for accounting purposes, including subsequent measurement considerations and assessment for embedded derivatives that may require bifurcation pursuant to FASB ASC Attachment B.

Meeting the definition of an investment company when engaging in digital asset activities

Question 11:

Would participation in digital asset activities (for example, mining activities) disqualify an entity from classification as an investment company within the scope of FASB ASC 946, *Financial Services—Investment Companies*?

Response 11:

It depends. In accordance with FASB ASC 946-10-15-5, a company that is not regulated under the Investment Company Act of 1940 may be an investment company, if it possesses the fundamental characteristics in FASB ASC 946-10-15-6, which are as follows:

a. It is an entity that does both of the following:
   1. Obtains funds from one or more investors and provides the investors with investment management services
   2. Commits to its investors that its business purpose and only substantive activities are investing the funds solely for returns from capital appreciation, investment income, or both.
b. The entity or its affiliates do not obtain or have the objective of obtaining returns or benefits from an investee or its affiliates that are not normally attributable to ownership interests or that are other than capital appreciation or investment income.

As stated in FASB ASC 946-10-15-7, typically, an investment company also has the following characteristics:

a. It has more than one investment.
b. It has more than one investor.
c. It has investors that are not related parties of the parent (if there is a parent) or the investment manager.
d. It has ownership interests in the form of equity or partnership interests.
e. It manages substantially all of its investments on a fair value basis.

However, the absence of one or more of those typical characteristics does not necessarily preclude an entity from being an investment company. An entity should apply judgment and determine how its activities are consistent with those of an investment company.

In accordance with FASB ASC 946-10-55-4, an investment company should have no substantive activities other than its investing activities and should not have significant assets or liabilities other than those relating to its investing activities, subject to certain exceptions outlined in FASB ASC 946-10-55-5.

It is important for an entity to consider evidence of its business purpose and substantive activities in determining appropriate classification as an investment company. Evidence of the business purpose and substantive activities may be included in the entity's offering memorandum, publications distributed by the entity, and other corporate or partnership documents that indicate the investment objectives of the entity. Additional evidence also may include the manner in which the entity presents itself to other parties (such as potential investors or potential investees). An entity's investment plans (for example, potential exit strategies to realize capital appreciation) also provide evidence of its business purpose and substantive activities.

It is important for an entity participating in digital asset activities (for example, buying and selling, mining) to use judgment and determine, considering all available evidence, whether these activities are consistent with those of an investment company in accordance with FASB ASC 946-10. For example, an entity's purchases of digital assets with the objective of selling them for capital appreciation would be considered investing activities consistent with those of an investment company. In contrast, an entity's activities in devoting resources to mining, such as procuring and operating significant computer and networking equipment in order to obtain digital assets in return for providing computing resources to a blockchain, would generally be considered "other than investing activities" that are inconsistent with those of an investment company.

If an entity or its affiliates participates in "other than investing" activities, it would need to evaluate whether those "other than investing activities" are substantive. If they are substantive, the entity would not meet the definition of an investment company. Determining whether noninvestment activities are substantive may require significant judgment.

In addition to the guidance in FASB ASC 946, an entity could consider Q&A section 6910.36, "Determining Whether Loan Origination Is a Substantive Activity When Assessing Whether an Entity Is an Investment Company,"[10] found in Technical Questions and Answers, which provides a framework to evaluate whether an entity's activities represent substantive activities that are inconsistent with the activities of an investment company. For example, the significance of income generated through noninvestment activities should be compared to income generated from capital appreciation, investment income, or both. If such activities are determined to be substantive, it would preclude the entity from qualifying as an investment company.

[10] See https://www.aicpa.org/interestareas/frc/recentlyissuedtechnicalquestionsandanswers.html.

Accounting by an investment company for digital assets it holds as an investment

Question 12:

How should an entity that qualifies as an investment company under FASB ASC 946, *Financial Services — Investment Companies*, account for investments in digital assets?

Response 12:

An investment company applying FASB ASC 946 should determine whether its holdings of digital assets represents a debt security, equity security, or an other investment and apply the guidance in FASB ASC 946-320 for investments in debt and equity securities or FASB ASC 946-325 for other investments. Irrespective of the type of investment, FASB ASC 946 requires an investment company to initially measure its investments at their transaction price, inclusive of commissions and other charges that are part of the purchase transaction.

Subsequently, the investment company should measure investments in digital assets at fair value in accordance with the applicable guidance in FASB ASC 946-320-35-1 or FASB ASC 946-325-35-1, unless an exception applies that would require equity method accounting or consolidation, for example, if the digital asset provides control over an operating entity whose purpose is to provide services to the investment company. See additional guidance in FASB ASC 946-323 and FASB ASC 946-810.

Recognition, measurement, and presentation of digital assets specific to broker-dealers

NOTE: Q&As 13–15 address the recognition, measurement and presentation of digital assets specific to broker-dealers in the scope of FASB ASC 940, *Financial Services — Brokers and Dealers*, and the AICPA's Audit and Accounting Guide *Brokers and Dealers in Securities* (Broker-Dealer guide).

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,[11] 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.[12] 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[13] the discussion of the SEC's financial responsibility rules provided in the Joint Staff Statement on Broker-Dealer Custody of Digital Asset Securities.[14] 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).

Question 13:

How should an entity that is a broker-dealer in the scope of FASB ASC 940, *Financial Services — Brokers and Dealers*, present digital assets held or received[15] on behalf of customers on its statement of financial condition?

Response 13:

When an entity holds or receives digital assets on behalf of a customer and has determined that such activities are within the scope of FASB ASC 940-20, the entity should consider the guidance in FASB ASC 940-20-25-1 and, for registered broker-dealers, the discussion of the SEC's financial responsibility rules provided in the Joint Staff Statement on Broker-Dealer Custody of Digital Asset Securities. In accordance with FASB ASC 940-20-25-1, when a broker-dealer is an agent for a customer, the transaction should not be reflected on its statement of financial condition.

NOTE: 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. See NOTE before Q&A 13 for additional information about considerations for an entity that reaches the conclusion that it is within the scope of FASB ASC 940.

[11] See https://www.fasb.org/jsp/FASB/Document_C/DocumentPage?cid=1218220140741&acceptedDisclaimer=true.

[12] See https://www.sec.gov/page/oca-form-delivery-and-content-correspondence-oca-consultations.

[13] Importantly, if the entity is a registered broker-dealer, it must comply with broker-dealer financial responsibility rules, including, as applicable, custodial requirements under Rule 15c3-3 under the Securities Exchange Act of 1934, which is known as the Customer Protection Rule.

[14] See https://www.sec.gov/news/public-statement/joint-staff-statement-broker-dealer-custody-digital-asset-securities#_ftn1.

Question 14:

How should a broker-dealer in the scope of FASB ASC 940 recognize revenue for purchases or sales transactions in digital assets on behalf of its customers?

Response 14:

A broker-dealer may buy and sell digital assets on behalf of its customers in return for a commission. The Broker-Dealer guide notes that *agency transactions* are transactions in which the broker-dealer "is simply a middleman between two counterparties … [and] is acting in a broker capacity."[16] In accordance with FASB ASC 940-20-25-2, commission income is recognized in revenue when (or as) the broker-dealer satisfies its performance obligations under the contract in accordance with FASB ASC 606, *Revenue from Contracts with Customers*.

NOTE: 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. See NOTE before Q&A 13 for additional information about considerations for an entity that reaches the conclusion that it is within the scope of FASB ASC 940.

Question 15:

How should the digital assets owned by a broker-dealer in the scope of FASB ASC 940 as part of its proprietary trading portfolio be measured?

Response 15:

In accordance with paragraphs 1–2 of FASB ASC 940-320-35, positions resulting from proprietary trading should be measured at fair value with changes in fair value recognized in profit and loss.[17] Given that industry practice has been to interpret the definition of inventory held by a broker-dealer under FASB ASC 940 to include assets such as financial instruments and physical commodities held as proprietary positions, extending the interpretation of inventory to include digital assets that are held for proprietary trading is reasonable.

NOTE: 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. See NOTE before Q&A 13 for additional information about considerations for an entity that reaches a conclusion that it is within the scope of FASB ASC 940.

[15] Receipt refers to a transaction in which the customer transfers the digital asset to the broker-dealer, and the transfer is recorded on the blockchain native to the digital asset.

[16] See paragraph 5.66 of chapter 5, "Accounting Standards," of the AICPA Audit and Accounting Guide *Brokers and Dealers in Securities* (Broker-Dealer guide).

[17] Paragraph 5.02 of the Broker-Dealer guide states that a broker-dealer accounts for inventory and derivative positions (such as futures, forwards, swaps, and options) at fair value.

Considerations for crypto assets that require fair value measurement

Question 16:

When determining the fair value for crypto assets,[18] what is the principal market?

Response 16:

In accordance with FASB ASC 820-10-35-3, a fair value measurement assumes that the asset or liability is exchanged in an orderly transaction between market participants to sell the asset or transfer the liability at the measurement date under current market conditions. Furthermore, FASB ASC 820-10-35-5 states that a fair value measurement assumes that the transaction to sell the asset or transfer the liability takes place either (*a*) in the principal market for the asset or liability or (*b*) in the absence of a principal market, in the most advantageous market for the asset or liability. Therefore, a fair value measurement contemplates an orderly transaction to sell the asset or transfer the liability in its principal market (or in the absence of a principal market, the most advantageous market).

There are various markets in which crypto assets trade. The reliability and sufficiency of the information produced could vary market by market. It is important for entities to consider whether these markets provide reliable volume and level of activity information in their determination of the principal market (or in the absence of a principal market, the most advantageous market).

Under FASB ASC 820, *Fair Value Measurement*, a *principal market* is the market with the greatest volume and level of activity for the asset or liability. The determination of the principal market should be based on the market with the greatest volume and level of activity that the reporting entity can access and not on the entity's own level of activity in a particular market. In that regard, it is important for an entity to assess whether there are any regulatory or other restrictions that prevent it from accessing a particular market.

When identifying the principal market — or in the absence of a principal market, the most advantageous market — an entity is not required to undertake an exhaustive search of all possible markets for the asset, but it should consider all information that is reasonably available. In accordance with FASB ASC 820-10-35-5A, the market in which an entity normally transacts for the crypto asset is presumed to be the principal market, unless contrary evidence exists.

To overcome the presumption, an entity must obtain evidence that the market it normally transacts in is not the market with the greatest volume and level of activity for the crypto asset. For example, if an entity normally buys and sells crypto assets through an intermediary or a broker, it would generally identify that market as the principal market, unless it has obtained evidence (considering all information that is reasonably available) that another market (for example, an exchange) has a greater volume and level of activity. For this purpose, a comparison would be made between the other market and the market the entity normally transacts in. Although numerous market participants may transact in crypto assets through intermediaries or brokers, each individual intermediary or broker is not a market. Generally, there is a lack of information regarding volume and pricing of crypto asset transactions in non-exchange markets. Therefore, it may be difficult for an entity to make a comparison between markets in order to conclude that another market (for example, an exchange) has a greater volume and level of activity than the market in which it normally transacts through an intermediary or broker. In this situation, it would be difficult to overcome the presumption that the market it normally transacts in is the principal market.

[18] Refer to the definition of a *crypto asset* in Q&A 1 of this practice aid.

When there is a principal market for the crypto asset being valued, the price in that market should be used to measure fair value, even if there is a more advantageous price in a different market at the measurement date. That is, the most advantageous market concept is applied under FASB ASC 820 only in situations when the entity determines there is no principal market for the crypto asset being valued. The most advantageous market is the market that maximizes the amount that would be received to sell the crypto asset, after taking into account transaction costs (for example, exchange or broker fees). Although transaction costs may factor into determining the most advantageous market, consistent with FASB ASC 820-10-35-9B, such costs are not included in the fair value of the crypto asset.

NOTE: The scope of Q&As 16–21 is specific to crypto assets. In addition, the Q&As interrelate and therefore are intended to be read in conjunction with one another.

Question 17:

What are some items an entity should consider about the markets in which crypto assets[19] trade when determining the fair value of a crypto asset holding?

Response 17:

Crypto assets trade in various markets. The reliability and sufficiency of the information produced that could be used to determine if the market's reported transactions are orderly or the market is active can vary widely from market to market. To determine the fair value of a crypto asset in accordance with FASB ASC 820, *Fair Value Measurement*, an entity would need to, among other things, determine the principal (or most advantageous) market in which a crypto asset trades, assess whether that market is active or inactive, evaluate whether reported market trades are orderly, and determine if the information produced by the market is reliable.

An entity's assessment of these items may significantly affect how the fair value of a crypto asset should be measured. Examples follow:

- If an entity determines that information provided by a market is not reliable, it should not place weight on the information.
- If an entity participates in transactions in its principal market, it would generally not be appropriate to place zero weight on the market information.
- If trades are between willing buyers and sellers, and the exposure to the market allowed for usual and customary marketing activities, it would be difficult to assert that the trades are not orderly because the transaction is not a forced transaction.
- If any entity concludes that the market is inactive, the amount of weight placed on that transaction price when compared with other indications of fair value will depend on the facts and circumstances.

Ultimately, entities need to carefully assess the markets in which crypto assets trade to determine the appropriate inputs or techniques for determining the fair value of a crypto asset. Refer to Q&A 18–20 for further information.

NOTE: The scope of Q&As 16–21 is specific to crypto assets. In addition, the Q&As interrelate and therefore are intended to be read in conjunction with one another.

[19] Refer to the definition of a *crypto asset* in Q&A 1 of this practice aid.

Question 18:

Assume the principal (or most advantageous) market for a given crypto asset[20] is an active market with quoted prices for identical assets. Given the characteristics of the principal market, an entity concludes the fair value would be classified as Level 1. How is the fair value of the crypto asset determined in this circumstance?

Response 18:

If there is a principal market for the crypto asset, the fair value measurement of the crypto asset should be based on the quoted price in that market, even if prices in a different market are potentially more advantageous at the measurement date (FASB ASC 820-10-35-6). FASB ASC 820-10-35-44 states that if a reporting entity holds a position in a single asset or liability (including a position comprising a large number of identical assets or liabilities, such as a holding of financial instruments) and the asset or liability is traded in an active market, the fair value of the asset or liability should be measured within Level 1 as the product of the quoted price for the individual asset or liability and the quantity held by the reporting entity. That is the case, even if a market's normal daily trading volume is not sufficient to absorb the quantity held, and placing orders to sell the position in a single transaction might affect the quoted price.

Accordingly, except in certain circumstances identified in FASB ASC 820-10-35-41C, there should be no adjustment to Level 1 inputs, and the fair value of the crypto asset should be determined based on price times quantity (commonly referred to as "P × Q").

For markets that provide information on bid-ask spreads, FASB ASC 820-10-35-36C requires fair value to be based on the price within the bid-ask spread that is most representative of fair value. Entities may use the bid, ask, mid-point between bid and ask, or some other point within the range. Although the guidance in FASB ASC 820-10-35-36D does not preclude midpoint (or mid-market) pricing convention, there may be situations in which the use of such a convention is not appropriate (for example, when a large bid-ask spread exists).

NOTE: The scope of Q&As 16–21 is specific to crypto assets. In addition, the Q&As interrelate and therefore are intended to be read in conjunction with one another.

Question 19:

Is it appropriate for a reporting entity to adjust the fair value measurement of a crypto asset[21] to reflect the size of the entity's holding of the crypto asset?

Response 19:

No. FASB ASC 820-10-35-36B states the following:

> A reporting entity should select inputs that are consistent with the characteristics of the asset or liability that market participants would take into account in a transaction for the asset or liability (see FASB ASC 820-10-35-2B through 35-2C). In some cases, those characteristics result in the application of an adjustment, such as a premium or discount (for example, a control premium or noncontrolling interest discount). However, a fair value measurement should not incorporate a premium or discount that is inconsistent with the unit of account in the Topic that requires or permits the fair value measurement. Premiums or discounts that reflect size as a

[20] Refer to the definition of a *crypto asset* in Q&A 1 of this practice aid.
[21] Refer to the definition of a *crypto asset* in Q&A 1 of this practice aid.

characteristic of the reporting entity's holding (specifically, a blockage factor that adjusts the quoted price of an asset or a liability because the market's normal daily trading volume is not sufficient to absorb the quantity held by the entity, as described in FASB ASC 820-10-35-44), rather than as a characteristic of the asset or liability (for example a control premium when measuring the fair value of a controlling interest) are not permitted in a fair value measurement.

The response to Q&A 7 indicates that entities will generally reach a determination that the unit of account for a crypto asset is the individual unit (or divisible fraction of a unit.) Further, the response to Q&A 1 explains that a crypto asset is not a financial instrument, financial asset, or a nonfinancial item accounted for as a derivative in accordance with FASB ASC 815, *Derivatives and Hedging*. As a result, the portfolio exception at FASB ASC 820-10-35-18D is not applicable to a crypto asset and, therefore, it would be inappropriate to adjust the fair value measurement of a crypto asset to reflect the size of an entity's holding of a crypto asset.

NOTE: The scope of Q&As 16–21 is specific to crypto assets. In addition, the Q&As interrelate and therefore are intended to be read in conjunction with one another.

Question 20:

Crypto asset[22] markets often operate continuously, without a traditional market close. How should entities determine the fair value of the crypto asset in such circumstances?

Response 20:

In such circumstances, an accounting convention may establish a cut-off time for determining the fair value of the crypto asset. For example, it may be reasonable for an entity to establish an accounting convention based on prices at

- the close of the business day of the entity.
- a fixed Coordinated Universal Time (UTC).
- other timing as deemed reasonable, such as traditional close time based on local market jurisdictions.

Entities should consider transactions that take place after the cut-off time but before the end of the reporting period, similar to the guidance in FASB ASC 820-10-35-41C.

Any convention used should be reasonable and consistently applied, and changes should be made only if facts and circumstances support a change.

NOTE: The scope of Q&As 16–21 is specific to crypto assets. In addition, the Q&As interrelate and therefore are intended to be read in conjunction with one another.

[22] Refer to the definition of a *crypto asset* in Q&A 1 of this practice aid.

Question 21:

If the principal (or most advantageous) market is not active or does not have orderly transactions (that is, not Level 1), how does management weigh inputs from different sources in the determination of the fair value of a crypto asset? [23]

Response 21:

When evaluating the relevance of transaction prices as inputs into the fair value measurement of a crypto asset, entities may consider using the following approach, which is consistent with the guidance in FASB ASC 820-10-35-54J and the related framework in paragraph 8.07 of the AICPA Guide *Valuation of Privately Held Company Equity Securities Issued as Compensation* and paragraph 10.34 of the AICPA Guide *Valuation of Portfolio Company Investments of Venture Capital and Private Equity Funds and Other Investment Companies*.

- If the transaction is orderly and for an identical instrument in an active market that is not the principal (or most advantageous) market, the transaction may require adjustments that market participants would apply to arrive at a fair value consistent with the entity's principal (or most advantageous) market.
- If the transaction is for an identical instrument but not in an active market, or for a related instrument, and the evidence indicates that the transaction is orderly, then that transaction price would be considered. The amount of weight placed on the transaction price when compared with other indications of fair value will depend on the facts and circumstances.
- If evidence indicates that the transaction is not orderly, then little, if any, weight would be placed on the transaction price.
- If the investor does not have sufficient information to conclude[24] whether a transaction is orderly, it should consider the transaction price in its analysis (that is, give it some weight) but may also supplement the transaction price with other valuation inputs or techniques.[25] However, the entity should maximize the use of relevant observable inputs and minimize the use of unobservable inputs when developing a fair value estimate consistent with FASB ASC 820, *Fair Value Measurement*.

NOTE: The scope of Q&As 16–21 is specific to crypto assets. In addition, the Q&As interrelate and therefore are intended to be read in conjunction with one another.

[23] Refer to the definition of a *crypto asset* in Q&A 1 of this practice aid.

[24] FASB ASC 820-10-35-54J states that a reporting entity need not undertake exhaustive efforts to determine whether a transaction is orderly, but it should not ignore information that is reasonably available. When a reporting entity is a party to a transaction, it is presumed to have sufficient information to conclude whether the transaction is orderly.

[25] It would be rare that valuation techniques of a crypto asset apply any other approaches besides a market approach based upon observed transactions or market quotes.

Accounting for stablecoin holdings

Question 22:

How should investors that do not apply specialized industry guidance account for a holding of a stablecoin?

Response 22:

It depends. There are differences among digital assets that are referred to as stablecoins in the market. Some are collateralized and redeemable into the assets used to collateralize the stablecoin, such as U.S. dollars, a specific commodity, a specific crypto asset, or a combination of multiple different assets. Others may not be collateralized or may not be redeemable. Generally, stablecoins differ from a typical crypto asset in that they include mechanisms designed to minimize price volatility by linking their values (for example, a "peg") to the value of a more traditional asset, such as a fiat currency or a commodity. Given the differences in the underlying rights and obligations across digital assets referred to as stablecoins, the proper accounting for an investment in a stablecoin will depend on the relevant facts and circumstances.

When evaluating the relevant facts and circumstances, some key questions an entity may want to consider when determining the accounting for a holding in a stablecoin include the following:

- What is the purpose of the stablecoin, and how does it achieve that purpose?
- What are the rights and obligations of the stablecoin holder? For example, is the stablecoin collateralized? If so, what are the eligible forms of collateral? Can the stablecoin be traded with parties other than the issuing entity?
- Who is the issuing entity or group of entities that is pooling resources to support the stablecoin?
- Does a legal entity that issues the stablecoin exist? If so, does the stablecoin convey to the holder an interest in the issuing entity?
- What is the legal form of the stablecoin (for example, debt or equity)?
- What mechanisms exist to minimize the price volatility? For example, can the stablecoin be redeemed for, exchanged for, or converted into its underlying asset? How do these mechanisms work, and how are the mechanisms governed?
- If it is redeemable, how and how often can it be redeemed?
- If it is collateralized, how is the collateral verified and perfected? If it is collateralized, what is the level of collateral (that is, is it partially, fully or over-collateralized?)
- How well do the mechanisms to minimize the price volatility work? For example, how volatile is the price of the stablecoin versus its intended peg?
- Do any credit or liquidity concerns exist?
- What laws and regulations apply to the stablecoin?

Because of the variety of facts and circumstances that may exist, it is impossible to provide a general rule for accounting for stablecoins. Relevant generally accepted accounting principles (GAAP) should be considered. For example, the ownership of a stablecoin may provide the holder with an ownership interest in the issuing entity. In this case, the stablecoin should be evaluated under relevant GAAP (for example, FASB ASC 321, *Investments — Equity Securities*; FASB ASC 323, *Investments—Equity Method and Joint Ventures*; or FASB ASC 810, *Consolidation*). Other types of stablecoins may be financial assets or financial instruments containing an embedded derivative that should be evaluated under FASB ASC 815, *Derivatives and Hedging*. However, the accounting for stablecoins is not limited to the aforementioned FASB ASC topics.

Question 23:

Entity A owns 100 units of a stablecoin, a digital asset that has a stated value of one U.S. dollar and is collateralized on a one-for-one basis by dollars held in a segregated bank account by the issuing entity. The holders of the units only have the right to redeem each unit for one U.S. dollar. How should Entity A account for its stablecoin?

Assume Entity A does not apply any specialized industry guidance (for example, FASB ASC 946 or FASB ASC 940).

Response 23:

Entity A's stablecoin holding would not be a derivative[26] but does meet the definition of a *financial asset* under U.S. GAAP because it can be redeemed for cash. If the stablecoin also meets the definition of a *security* (as defined in the definition 2 in the FASB ASC Master Glossary), it would generally be accounted for under FASB ASC 320, *Investments — Debt Securities*. If the stablecoin does not meet the definition of a security, it would generally be accounted for under FASB ASC 310, *Receivables*, because it is contractually redeemable for cash. A stablecoin that meets the definition of a *financial asset* would also typically be eligible for the fair value option under FASB ASC 825, *Financial Instruments*. Depending on the relevant facts and circumstances of the stablecoins, entities may also need to consider the definitions of *cash or cash equivalent*.

[26] This is because the stablecoin requires a payment in cash equal to the stated value of the stablecoin at inception — that is, it does not meet the "no initial or small initial net investment" criteria of a derivative. An entity may need to evaluate if an embedded derivative exists under FASB ASC 815, *Derivatives and Hedging*.

Auditing subgroup

Client acceptance and continuance

1. Overview

The topics in this section of the practice aid address matters for auditors to consider regarding accepting or continuing audit engagements of entities in the current digital asset ecosystem. As firms seek to provide audits to entities within the ecosystem, caution and consideration must be given to unique risks and challenges in the digital asset ecosystem.

The topics in this section of the practice aid focus on auditing applications and do not address ethics or independence considerations; it is important to note, however, that these considerations remain critical to an auditor's conformity to professional standards, and engagements in the digital asset ecosystem may introduce new or different compliance risks warranting additional consideration by the auditor. For example, a member of the engagement team may hold digital assets issued by the entity subject to audit. ET section 1.200, "Independence," provides examples of relationships or circumstances that create threats to compliance with the "Independence Rule," and ET section 1.295, "Nonattest Services," addresses threats involving the provision of nonattest services to an audit client, including the following specifically:

- **Self-review threat —** Threat that a member will not appropriately evaluate the results of a previous judgment made or service the member (or colleague) performed or supervised, which the member will rely on when forming a judgment as part of an attest engagement.
- **Management participation threat —** Threat that a member will assume the role of attest client management or perform management responsibilities for an attest client.
- **Advocacy threat —** Threat that a member will promote an attest client's interests or position to the point that his or her independence is compromised.

In addition to the AICPA Code of Professional Conduct, the following standards apply to client acceptance and continuance procedures:

- QC section 10, *A Firm's System of Quality Control*, as it relates to audits
- AU-C section 200, *Overall Objectives of the Independent Auditor and the Conduct of an Audit in Accordance With Generally Accepted Auditing Standards*
- AU-C section 210, *Terms of Engagement*
- AU-C section 220, *Quality Control for an Engagement Conducted in Accordance With Generally Accepted Auditing Standards*[27]

[27] All QC and AU-C sections can be found in AICPA *Professional Standards*.

The topics covered in this section of the practice aid are divided into the following sections:

- **Section 2:** Auditor skill sets and competencies
- **Section 3:** Management skill sets and competencies
- **Section 4:** Management integrity and the entity's overall business strategy
- **Section 5:** Processes and controls, including information technology systems

Each section begins with a detailed summary of the applicable professional standards, then outlines some unique challenges to engagements in the digital asset ecosystem, and ends with practical recommendations auditors may apply to address those challenges and requirements.

2. Auditor skill sets and competencies

Relevant professional standards

QC section 10 and AU-C section 220 each contain requirements related to a firm's evaluation of its personnel's competence to perform an engagement prior to acceptance or continuance of a client relationship or specific engagement.[28]

A firm's evaluation generally encompasses competence, capabilities, resources, and availability of the engagement team. In this context, the engagement team includes the engagement partner, firm personnel assigned to the engagement (including internal specialists), and external specialists, if applicable.

The AICPA Code of Professional Conduct explains the meaning of the term *competence*, stating:

> .03 Competence is derived from a synthesis of education and experience. It begins with a mastery of the common body of knowledge required for designation as a certified public accountant. The maintenance of competence requires a commitment to learning and professional improvement that must continue throughout a member's professional life. It is a member's individual responsibility. In all engagements and in all responsibilities, each member should undertake to achieve a level of competence that will assure that the quality of the member's services meets the high level of professionalism required by these Principles.
>
> .04 Competence represents the attainment and maintenance of a level of understanding and knowledge that enables a member to render services with facility and acumen. It also establishes the limitations of a member's capabilities by dictating that consultation or referral may be required when a professional engagement exceeds the personal competence of a member or a member's firm. Each member is responsible for assessing his or her own competence of evaluating whether education, experience, and judgment are adequate for the responsibility to be assumed.
>
> [ET section 0.300.060, "Due Care"]

[28] See paragraphs .27a and .A11 of QC section 10 and paragraphs .14 and .A7 of AU-C section 220.

The purpose of the firm's evaluation is to provide the firm reasonable assurance that it will only undertake client relationships and engagements for which it can perform the audit in accordance with professional standards and applicable legal and regulatory requirements to enable the issuance of an auditor's report that is appropriate in the circumstances.

Paragraph .A11 of QC section 10 states the following:

> Consideration of whether the firm has the competence, capabilities, and resources to undertake a new engagement from a new or an existing client involves reviewing the specific requirements of the engagement and the existing partner and staff profiles at all relevant levels, including whether
>
> - firm personnel have knowledge of relevant industries or subject matters or the ability to effectively gain the necessary knowledge;
> - firm personnel have experience with relevant regulatory or reporting requirements or the ability to effectively gain the necessary competencies;
> - the firm has sufficient personnel with the necessary competence and capabilities;
> - specialists are available, if needed;
> - individuals meeting the criteria and eligibility requirements to perform an engagement quality control review are available, when applicable; and
> - the firm is able to complete the engagement within the reporting deadline.

The assessment of these items occurs before accepting or continuing an engagement and is meant to mitigate the risk that the firm accepts an engagement it is not capable of effectively performing. If a firm has an insufficient understanding of the industry and environment when it accepts a client and fails to recognize and address the need for additional resources or education, it will be difficult, and may not be possible, for that firm to perform an effective audit or comply with applicable professional standards.

An auditor's ability to obtain a robust understanding of the client and its environment (sections 3 and 4), including its system of internal control (section 5), is critical to an effective risk assessment and audit response. For example, a firm may have deep experience in the financial services industry and may be presented with a client opportunity in that industry that also involves digital assets. Consideration in evaluating the client acceptance and continuance determination include a firm's (1) current industry expertise; (2) understanding of digital assets; and (3) understanding of how digital assets are being used in the specific client situation being evaluated. Knowledge of all three components is necessary for an auditor to effectively perform an engagement, and it is important to assess the ability to perform each for a well-informed client acceptance or continuance decision.

Performing audits in the digital asset ecosystem may require a firm to update, or include additional oversight of, its existing system of quality control. For example, if the firm intends to pursue audit work for entities participating in the ecosystem and its recruitment and training programs do not currently contemplate issues unique to that ecosystem, more thought and attention may need to be placed on assessing whether the firm has sufficient personnel with the necessary competence and capabilities in the client acceptance or continuance and other quality control processes, or the need to engage external specialists.

Paragraph .A11 of QC section 10 acknowledges that firm personnel may not have "knowledge of relevant industries or subject matter or the ability to effectively gain the necessary knowledge." A client acceptance and continuance determination, therefore, requires an assessment both of any gaps in the skill sets of the firm's personnel and of whether the firm can satisfactorily address those gaps if it chooses to accept or continue to be engaged with the client.

Notwithstanding that the standard allows for the ability to gain the necessary knowledge for emerging issues and industries, such as digital assets, for which a firm has no previous expertise, it is important to recognize the risk of overconfidence in client acceptance and continuance decision-making and implement appropriate firm quality controls or oversight to challenge those decisions. The digital asset ecosystem is evolving rapidly; it is important for the firm to understand the level of effort necessary to gain the knowledge about the ecosystem (or relevant parts thereof) needed to make a reasoned client acceptance and continuance determination and competently perform the audit.

Challenges specific to digital assets

Client acceptance and continuance procedures serve as a means of managing and mitigating the firm's own risks (including professional liability or external audit regulation) and informing its quality control strategy for an engagement. Although all industries encounter change, the digital asset ecosystem is evolving rapidly, and auditors' skill sets and competencies may be particularly strained in this environment. In designing procedures to meet the requirements of GAAS and QC section 10, firms may encounter challenges in adapting or maintaining auditors' skill sets and competencies related to the digital asset ecosystem in the following ways:

- Staying apprised of regulatory, industry, technological, or financial reporting developments affecting current or potential clients that may affect the risk assessment or other aspects of the audit
- Recruiting, developing, and retaining talent in a highly competitive market, particularly those qualified in the information technology and cybersecurity aspects of the audit
- Appropriately directing, supervising, and reviewing the work of the engagement team including staff, internal specialists, and multiple external specialists whose skill sets may not be familiar to the audit team
- Adapting to new or different risks as the ecosystem evolves or new issues are identified
- Ongoing updates of training curricula for current and future auditors to adapt to the rapidly evolving elements of the digital asset ecosystem, new digital assets, and the surrounding business and regulatory environment

When considering engagement acceptance or continuance in accordance with paragraph .27 of QC section 10, the firm takes into account the challenges to possessing appropriate competence indicated previously.

Procedures to consider specific to digital assets

Procedures specific to the digital asset ecosystem that an auditor may perform as part of the acceptance and continuance process include the following:

- Identify, in firm policy or quality control materials, the types of clients or engagements the firm is capable of accepting.
- Determine firm-wide areas of focus or criteria for client acceptance for companies within the digital asset ecosystem. For example, provided the firm's client acceptance criteria are met, some firms may decide to focus on validator entities only, given their level of experience in auditing such entities, and other firms may feel comfortable serving validator and exchange entities. If auditors are generally aware of the types of clients the firm will or will not accept, there is less risk that the firm will inadvertently accept an engagement it is not qualified to perform.

- Build general awareness among firm personnel of the risks inherent in the digital asset ecosystem, so that current auditors understand such risks and what resources are available for existing client engagements. For example, a firm's existing clients may become exposed to the digital asset ecosystem in a variety of ways, whether through vendors, customers, or the client's own strategic choices. To build awareness, a firm could develop a training program that discusses the risks described in this practice aid along with ways the firm is addressing those risks in its internal system of quality control.
- Communicate consultation resources, training, or guidance to relevant firm personnel and when necessary, re-evaluate client acceptance and continuance decisions based on changing facts and circumstances.
- Identify an individual or individuals, either internal or external to the firm, with known, demonstrated competence in auditing entities within the digital asset ecosystem to serve as the firm's subject matter expert(s) (SMEs). Note: the inability to identify such an individual may call into question the firm's ability to gain the necessary competence to perform work in this space.
- Communicate the SME name(s) to the practice for awareness.
- Require SME involvement in client acceptance and continuance decisions to make sure the considerations listed previously are made and documented appropriately.
- Implement training programs to acclimate relevant personnel to unique issues and risks discussed in other sections of this practice aid, commensurate with the needs identified in the client acceptance process; consider AICPA resources[29] or other sources to tailor training appropriately for engagement personnel and internal specialists (for example, IT, valuation, or cybersecurity).
- To the extent external specialists will be engaged, establish protocols for evaluating specialists that might not have been necessary in the past. (Paragraph .09 of AU-C section 620, Using the *Work of an Auditor's Specialist*).

If one or more engagements in the digital asset ecosystem are accepted, a firm may need to consider other potential updates to the system of quality control, including the following types of changes:

- Implement authorized lists of engagement partners and other individuals approved to be assigned to different roles on an audit in the digital asset ecosystem. (Paragraphs .33–.34 of QC section 10)
- Design, implement, and commit to maintaining guidance, practice aids, tools, training, and work programs to promote consistency and quality in engagement performance, supervision, and review, particularly in the risk assessment phase and audit strategy execution on an audit in the digital asset ecosystem. (Paragraphs .35–.36 of QC section 10)
- Establish consultation requirements for unique auditing or financial reporting issues that may be relevant in the digital asset ecosystem. (Paragraph .37 of QC section 10)
- Update the criteria for determining which engagements require an engagement quality control review, tailor review requirements to new or different risks, and assess the technical competence and qualifications of approved reviewers. (Paragraphs .38–.45 of QC section 10)
- Include new or high-risk engagements in the scope of pre- or post-issuance quality control monitoring procedures to evaluate engagement quality and the effectiveness of the quality control measures described herein. (Paragraph .52 of QC section 10)

[29] The AICPA has developed a course titled *Blockchain Fundamentals for Accounting and Finance Professionals Certificate* and also released a white paper titled *Blockchain Technology and Its Potential Impact on the Audit and Assurance Profession*.

In addition to the procedures noted previously, the following are some questions a firm may consider in the client acceptance and continuance process to evaluate its skill sets and competencies. For any negative or unknown answers, the auditor may need to perform additional procedures before accepting or agreeing to perform the audit, or ultimately decline the client or engagement. These examples are neither exhaustive nor always applicable, because facts and circumstance may vary from one engagement to the next.

- Does the firm have other similarly situated clients in the digital asset ecosystem?
- Does the auditor understand the applicable regulatory environment, and whether there is a risk an entity may not comply with laws and regulations?
- Does the auditor understand how the applicable financial reporting framework is applied to the client or its operations?
- Does the auditor understand the client's operations sufficiently to identify appropriate personnel to assign to the engagement (including partner, staff, and internal specialists) and to perform an effective risk assessment?
- Are personnel sufficiently knowledgeable? If not, can the gaps be addressed with additional training or assistance from external specialists?

  Note that these questions address the proposed engagement team's ability to understand and interact with management and its specialists on other topics, including sufficient knowledge to remain skeptical and challenge management's positions. As discussed in sections 3 through 5, a firm may identify a need for more dialogue with management prior to client acceptance and continuance, potentially including questions about the extent of digital assets in the entity's operations, the entity's system of internal control related to digital assets, what tools the entity uses, how it values and records transactions, or what custody solutions it uses. In addition, these questions may assist the auditor in evaluating appropriate audit personnel and skill sets.

- Do personnel have the time and resources needed to perform the engagement effectively?

  Note that even if external specialists will be utilized, the ethical requirements relating to due professional care (ET section 0.300.060) and GAAS require the firm have procedures in place to supervise and take responsibility for the sufficiency of the audit work.

  Additionally, in this context, "resources" may encompass investments in technology or tools needed to gather sufficient appropriate audit evidence of digital assets and transactions. Most commonly, these may include transaction validation and valuation resources.

- Does the firm have appropriate processes and resources in place to support the proposed engagement team with questions, consultations, or pre-issuance reviews?

As described previously, firms may need to adapt existing quality control practices to provide more guidance or resources for consultation or pre-issuance review procedures, including engagement quality control review. In addition to providing training and resources to the engagement team, firms may need to do so for personnel performing consultations and reviews.

3. Management skill sets and competencies

Relevant professional standards

AU-C section 210 requires the auditor to obtain the agreement of management that it acknowledges and understands its responsibility for

a. the preparation and fair presentation of the financial statements in accordance with the applicable financial reporting framework;
b. the design, implementation, and maintenance of internal control relevant to the preparation and fair presentation of financial statements that are free from material misstatement, whether due to fraud or error; and
c. providing the auditor with access to all relevant information and persons necessary to obtain audit evidence.

Further, as described in section 4, certain requirements of AU-C section 315, *Understanding the Entity and Its Environment and Assessing the Risks of Material Misstatement; and AU-C section 250, Consideration of Laws and Regulations in an Audit of Financial Statements*, are helpful to consider during acceptance and continuance procedures. As such, auditors may perform procedures to understand management's commitment to competence for particular jobs and how those levels translate into requisite skills and knowledge. The auditor should also consider attributes of those charged with governance, such as their experience and stature and whether they have sufficient skills and knowledge to fulfill their responsibilities.

Challenges specific to digital assets

Given the complexity associated with blockchain technology and digital assets, management may lack the skill sets or competencies needed to maintain the entity's books and records and secure its assets. Therefore, the assessment of whether an entity's personnel has the necessary competence and capabilities is likely an important factor related to the auditor's decision to accept or continue an audit engagement. Even if management has integrity and a sound business strategy, but does not have the appropriate skill sets or competencies, an audit may not be possible without management addressing the shortfalls. This may be because appropriate books and records were not maintained, processes and controls have not been implemented, or management over-relies on the auditor, thereby introducing the risk that the auditor is unable to fulfill their responsibility of providing an independent, objective opinion on the financial statements of the entity.

Further, when assessing the risks relative to the period being considered for acceptance or continuance, it is critical to understand *when* management obtained the necessary skill sets and competencies. For example, if an entity recently incorporated digital assets into its operations, it may be important for the auditor to consider management's ability to implement systems, processes, and controls over digital assets sufficient to produce financial statements free of material misstatement. Similarly, if certain actions are not taken when a transaction or control activity occurs, certain types of audit evidence may be difficult to obtain (for example, evidence that a control related to private key management operated effectively). Further, an entity's technical capabilities in developing digital assets technologies, although important, may not be indicative of sufficient and appropriate financial reporting capabilities or technical accounting experience.

Necessary skill sets and competencies of management include a general understanding of, and technical skill sets related to, blockchain technology and digital assets, sufficient for management to do the following:

- Identify the unique risks in the space and design and implement internal controls to respond to such risks. For example, given the pseudo-anonymity[30] associated with digital assets, management may implement internal controls to identify related parties and relationships and transactions with related parties — for example, know-your-customer (KYC) and other procedures.
- Understand the pace at which the technology could evolve and the need for additional controls or personnel.
- Have processes and controls for maintaining appropriate books and records, including maintaining appropriate support for transactions and applying the appropriate financial reporting framework. For example, an entity may maintain an independent record of digital asset transactions and reconcile such to the transaction summary provided from a custodian.
- Have competent personnel with ability to appropriately apply the financial reporting framework.
- Identify applicable laws and regulations or areas of evolving laws and regulations.
- Have access to or ability to identify the need for specialists — for example, competent legal counsel, IT specialists, or cybersecurity specialists.

Procedures to consider specific to digital assets

Given the challenges described previously, evaluating the skill sets and competencies of management in the client acceptance or continuance process may be more involved than typically performed for other new or continuing clients. Client acceptance and continuance procedures may include an evaluation of whether management has the requisite understanding of the risks, necessary controls, and understanding of the applicable financial reporting framework. This includes assessing the entity's ability to identify and address risks within the underlying technology that may introduce risks of material misstatement due to errors or fraud.

The following are some inquiries an auditor may consider incorporating into the acceptance and continuance process to evaluate management's skill sets and competencies.

- Does management have experience in the digital asset ecosystem such that it can identify the unique risks in the space and design and implement internal controls to respond to such risks (for example, risks surrounding private key management, related party transactions and disclosures or other fraud risks)?
- Does management understand the applicable regulatory environment and areas of evolving laws and regulations?
- Does management either (1) maintain books and records that are independent from the blockchain or third party or (2) derive the entity's records of balances and transactions solely from the blockchain or from statements provided by a third party? If the latter, the auditor may want to further understand, as part of the acceptance and continuance process, management's processes and controls over the quality of this information.

[30] In blockchain environments, digital assets are exchanged between blockchain addresses and private keys are used for authorization. However, the specific names and identities of those parties transacting are not explicitly identified with those addresses and keys. While it is possible to determine the identity through various de-anonymizing methods, this offers a level of disguised identity by transacting without publicly providing any personally identifiable information.

- Does management engage appropriate and qualified specialists or accounting consultants as needed when management does not have sufficient knowledge or expertise (for example, in house or external legal counsel or IT specialists, including cryptography and cybersecurity specialists) and perform effective reviews of the work performed by such specialists?
- Does management understand how the applicable financial reporting framework is applied to its operations? (See the "Accounting Subgroup" section of this practice aid.)

In addition to the previous inquiries, reading the accounting policy memorandums prepared by the entity (or performing detailed inquiries with management) assists the auditor in determining whether the entity appears to be sufficiently knowledgeable to assess the applicability of accounting standards, in addition to determining whether the entity has adequately applied the accounting standards. The entity should have competent members of the finance and accounting teams to determine appropriate accounting treatment of digital assets. Digital assets may carry different properties warranting varying classifications in the financial statements. Processes should be in place to assess the proper recognition, derecognition, measurement, classification, and tracking of new digital .new digital assets (See "Accounting Subgroup" section of this practice aid.)

Depending on the results of these inquiries and procedures, auditors may need to further expand inquiries or seek additional information. In addition to evaluating management's skill sets and competencies, the auditor also considers management's integrity and overall business strategy regarding digital assets as a part of the client acceptance and continuance process.

4. Management integrity and overall business strategy

Relevant professional standards

In accordance with paragraph .27 of QC section 10, a firm should establish policies and procedures for the acceptance and continuance of client relationships and specific engagements, designed to provide the firm with reasonable assurance that it will undertake or continue relationships and engagements only when, among other things, the firm has considered the integrity of the client and does not have information that would lead it to conclude that the client lacks integrity.

Matters to consider regarding the integrity of a client may include the following:

- The identity and business reputation of the client's principal owners, key management, and those charged with governance
- The nature of the client's operations, including its business practices
- Information concerning the attitude of the client's principal owners, key management, and those charged with governance toward such matters as internal control or aggressive interpretation of accounting standards
- Indications of an inappropriate limitation in the scope of the work
- Indications that the client might be involved in money laundering or other criminal activities
- The reasons for the proposed appointment of the firm and non-reappointment of the previous firm (Paragraph .A12 of QC section 10).

When performing acceptance and continuance procedures, it may also be helpful for the auditor to consider certain requirements in other AU-C sections addressing activities that may occur after client acceptance and continuance, such as AU-C section 315 and AU-C section 250. For example, paragraph .12 of AU-C section 315 requires the auditor to obtain an understanding of the entity's objectives and strategies and those related business risks that may result in risks of material misstatement. Paragraph .15 of AU-C section 315 further requires that the auditor should obtain an understanding of the control environment, including evaluating whether

- management, with the oversight of those charged with governance, has created and maintained a culture of honesty and ethical behavior, and
- the strengths in the control environment elements collectively provide an appropriate foundation for the other components of internal control and whether those other components are not undermined by deficiencies in the control environment.

Elements of the control environment that may be relevant when obtaining this understanding include management's communication and enforcement of integrity and ethical values and commitment to competence, as well as attributes of those charged with governance, such as their experience and stature (paragraph .A79 of AU-C section 315).

The auditors may also consider the requirements in AU-C section 250, which highlights aspects of the legal and regulatory environment. Paragraph .12 of AU-C section 250 requires that the auditor obtain a general understanding of the following:

a. The legal and regulatory framework applicable to the entity and the industry or sector in which the entity operates
b. How the entity is complying with that framework

Challenges specific to digital assets

The digital asset ecosystem presents unique considerations for auditors in the client acceptance and continuance process, which relate to both management's integrity and commitment to compliance with laws and regulations and its strategic objectives; for example, the following:

- The pseudo-anonymous nature of the digital asset transactions may present an opportunity for illegal activities such as money laundering or other illegal activities. Noncompliance with KYC procedures, anti-money laundering (AML) procedures, and other regulations could present considerable reputation and business risks to the entity in the form of fines and penalties, both criminal and civil.
- The anonymity of participants in public blockchain transactions may make it difficult to identify transactions with related parties or "bad actors" who may have illegal or fraudulent intentions. It may also provide opportunities to engage in fraud schemes such as roundtrip transactions.

- Ease of entry to the market (that is, anyone can market or create a digital asset) may attract those who lack integrity or a commitment to competence into the digital asset ecosystem.
- Management may not have a sufficient understanding of digital assets, the underlying technology and protocols, or the evolving regulatory environment to identify the risks related to fraud or noncompliance with laws and regulations. Furthermore, although management may assert that activities related to digital assets may not be significant or material to the financial statements, it is important for the auditor to consider noncompliance with laws and regulations (for example, failing to meet the regulatory requirements governing the issuance of a token that might be a "security") regardless of materiality, when completing client acceptance and continuance evaluations.

Procedures to consider specific to digital assets

When making client acceptance and continuance decisions for audits of entities in the digital asset ecosystem, auditors will likely find it important to obtain information necessary to understand the entity's business strategy, planned operations, and role the entity serves or intends to serve in the overall digital asset ecosystem.

Obtaining an understanding of the entity's business purpose in its initial involvement or significant changes in its involvement with digital assets is a key aspect in assessing management's integrity. If a new engagement is accepted or an existing engagement is continued, such understanding will be a critical starting point for identifying and assessing risks of material misstatement associated with those areas where special audit consideration may be necessary (for example, related party transactions).

In addition, each role within the digital asset ecosystem (for example, entities that hold the digital assets, custodians or wallet companies, exchanges, funds that invest in digital assets, vendors accepting digital currency, and validators) may present unique considerations.

Given the challenges described, auditors considering accepting new engagements or continuing existing engagements for clients in the digital asset ecosystem will ordinarily find it appropriate to augment their usual procedures by including some or all of the following. (The examples provided are nonexhaustive, and the nature and extent of these example procedures may vary depending on the entity's role in the ecosystem and the type of digital assets held by the entity.)

- Inquire with management to understand its business purpose related to the entity's current and future anticipated involvement with digital assets. The depth and breadth of these inquiries may vary depending on the nature and significance of the entity's involvement in digital assets (for example, whether entities own, invest, trade, have custodial responsibilities for, or otherwise transact digital assets). For example, if an entity accepts payment in digital assets but immediately converts it to U.S. dollars, the auditor's consideration of the business purpose of the involvement with digital assets may be less complex compared to an exchange offering multiple types of digital assets.
- Inquire with management to understand the control environment and the tone at the top, including management's philosophy, operating style, and level of tolerance for risk. These inquiries may focus on obtaining an understanding of how the entity's involvement in digital assets has been considered as a part of management's risk assessment and the level of risk they are willing to accept in the context of their overall risk appetite.

- Inquire with management to understand the nature of digital assets held or intended to be held and significance of such assets to the business. Inquiries may focus on obtaining an understanding of the type of digital assets held by the entity and the materiality of such assets.
- Inquire with management to understand their policies and procedures to onboard new customers or enter into relationships with other players in the digital asset ecosystem. These may include KYC procedures, AML procedures, and other due diligence procedures to understand the identity and integrity of the counterparty. These procedures may also assist in obtaining an understanding of management's process for identifying related parties and relationships and related party transactions. Inquiry may go beyond the chief executive officer, chief financial officer and chief accounting officer and include discussions with chief compliance officers, the entity's risk management or legal departments, or chief anti-money laundering officers, when applicable.
- Inquire with management to understand their processes and procedures to monitor transactions for illegal or suspicious activity subsequent to new customer onboarding or entering into a new business relationship. This may also include inquiry to understand third parties that may be used to facilitate digital asset transactions (for example, exchanges).
- Inquire with management to obtain an understanding of the legal and regulatory framework applicable to digital asset transactions, including regulations in other jurisdictions in which the entity is engaged, changes in this environment, and management's process for maintaining compliance with legal and regulatory requirements.
- Inquire with management regarding Bank Secrecy Act (BSA), or AML law, reports prepared by a third party or process documentation prepared by the entity. The auditor may inquire whether any known instances of noncompliance with these laws and regulations have occurred, or whether the entity has received communication from regulatory bodies concerning the entity's compliance or noncompliance with these types of laws and regulations.
- Inquire with management to understand policies and procedures, including due diligence procedures, performed when evaluating potential digital assets to transact with. The depth and breadth of these inquiries may vary depending on the role in the ecosystem and the type of digital asset (for example, a more established digital asset may have different risks compared to a lesser known or less liquid digital asset).
- Inquire with management to understand their policies and procedures to identify related parties and relationships and transactions with related parties. Given the pseudo-anonymous nature of the blockchain, the risk of material misstatements associated with related party transactions and disclosures as well as the risk of engaging in fraudulent activity (for example, engaging in transactions with related parties to inflate revenue) may increase. Gaining an understanding of management's policies and procedures to identify related parties and relationships and transactions with related parties, may assist the auditor in evaluating the entity's commitment to developing an ethical culture through the implementation of processes and controls.
- Inquire with management to understand the considerations for maintaining adequate books and records related to the particular digital assets that the entity currently transacts in, including any planned or potential additions to the digital assets currently held. Examples of such considerations include the identification and monitoring of related parties and the ability to prove ownership. The nature and extent of the books and records to support the assertions of management in the financial statements may depend on the particular digital assets.

- Inquire with predecessor auditor, if applicable, regarding matters that will assist the auditor in determining whether to accept the engagement, in accordance with paragraph .11 of AU-C section 210.
- Inquire with management to understand whether management uses third parties (for example, custodians or exchanges) and whether an appropriate SOC[31] report is available. If the services provided by a service organization (and sub-service providers, if applicable) are relevant to the audit of a user entity's financial statements, obtaining an understanding of management's processes and controls in addition to obtaining and evaluating the SOC report will also be relevant. If a SOC report is not likely to be available, inquire with management regarding alternative procedures that could be performed. For example, if the entity uses a third party to maintain custody of its digital assets, inquire with management to understand whether the third party commingles the entity's digital assets in a public address that also includes the digital assets of other depositors. When custodians commingle digital assets, a customer might see its individual account balances for each digital asset through the third party's web interface, but it may not be transparent to the customer whether those digital assets exist in the blockchain. Further, if the transactions (buy/sell or send/receive) are between two customers both using this same entity as the custodian, the custodian might decide to transfer funds only within their internal systems rather than using the public blockchain. When assets are commingled, it might be more challenging for management to maintain adequate books and records and for auditors to obtain sufficient appropriate audit evidence. In situations where there is commingling, it is important for auditors to understand management's processes and controls to validate the existence of, and the entity's rights to, the digital assets prior to acceptance or continuance. This will likely involve understanding whether an appropriate SOC report is available for the third party that maintains custody of the entity's digital assets and the complementary user entity controls, or whether alternate procedures can be performed if a SOC report is not available.
- For companies that have or plan to have initial coin offerings or similar mechanisms to create and distribute digital assets to others, understand the business purpose of the offering (for example, tokenizing a limited partnership interest in a venture capital fund or raising capital to develop a utility platform) and assess management's commitment to, and process for, identifying, staying current with, and complying with applicable laws and regulations (for example, state, local, federal, and international). Consider expanding inquiries to the entity's legal counsel and inspecting additional documentation or correspondence.
- For companies seeking to invest in an initial coin offering or similar offering, understand management's process to evaluate whether the digital asset is considered a security,[32] including the use of management's experts; the due diligence procedures the entity performed on the counterparty; the business rationale for investing in the initial coin offering; and the counterparty's business purpose of the initial coin offering.
- Consider contradictory information obtained by performing media searches and from other sources, including information from background checks on management and indicators that management may not be ethical.

[31] System and organization controls (SOC) is a suite of service offerings CPAs may provide in connection with system-level controls of a service organization or entity-level controls of other organizations. SOC 1® reports focus the controls at a service organization relevant to user entities' internal control over financial reporting and SOC 2® reports focus on controls at a service organization relevant to security, availability, processing integrity, confidentiality, and privacy.

[32] The SEC FinHub staff's "Framework for 'Investment Contract' Analysis of Digital Assets" (April 3, 2019) provides a framework for analyzing whether a digital asset offered or sold as an investment contract is a security.

5. Processes and controls, including information technology

Relevant professional standards

As described in paragraph .06 of AU-C section 210, a precondition for an audit is management's ability to prepare and take responsibility for the fair presentation of the financial statements, and the design, implementation, and maintenance of effective internal controls over financial reporting. The degree to which an auditor evaluates these preconditions in the client acceptance and continuance process may vary significantly. Engagements in the digital asset ecosystem often warrant rigorous inquiries in the client acceptance and continuance process to evaluate these preconditions. This is largely due to the complexity of the underlying technology and the unique risks and the related audit challenges in gathering sufficient appropriate audit evidence. Internal controls, including controls over information technology, have a direct effect on the auditability of the underlying financial activity, and auditors may need to expand traditional acceptance or continuance procedures to understand these challenges. For example, understanding how the entity is dependent on or enabled by IT and the manner in which information systems are used to record and maintain financial information may be more critical in the client acceptance or continuance process for entities engaged in newer technology.

Challenges specific to digital assets

Overview

Obtaining an understanding of how the entity uses digital assets, the underlying IT environment, and the controls implemented by the entity over digital assets is likely to be relevant to the auditor in deciding whether to accept or continue an engagement. In some cases, an auditor may encounter circumstances after the initial acceptance or continuance decision that may be cause for reassessment of the decision, such as instances where the auditor has determined that management has not or is unable to fulfill its responsibilities for the preparation and fair presentation of financial statements. For example, if the entity has entered into material digital assets transactions for the first time or strategically entered into a business that leverages digital assets in everyday operations, management may not have proper skill set and understanding, supporting books and records, or internal controls implemented to effectively account for and fairly present digital assets or associated transactions within the financial statements.

Certain applications of blockchain technology can eliminate the need for a central intermediary (for example, banks) for the completion of transactions. Correspondingly, audit evidence traditionally obtained from these intermediaries surrounding the existence and rights and obligations of assets may not be available. If an entity loses access to the private key, or another party inappropriately accesses the private key and transfers the digital assets to another public address where the entity does not have knowledge of the private key, then the entity may lose control of or access to the digital assets. Due to these characteristics, the knowledge of the private key represents control of the digital assets. Although procedures (for example, sending signed messages or moving assets) may be performed to evidence control of a digital asset, additional procedures may often need to be performed to obtain sufficient appropriate audit evidence of the entity's ownership of digital assets (for example, testing the operating effectiveness of controls over private key management).

Although it is sometimes claimed that blockchain technology eliminates the need for trust among transaction participants, the underlying technology does not make the information contained within it inherently trustworthy. Events recorded on the blockchain are not necessarily accurate and complete, and the reliability of data obtained from a blockchain is highly dependent upon the reliability of underlying complex blockchain technology. In addition, entities may implement new IT applications that interface between the blockchain and financial reporting system. The introduction of an interface system may further increase the complexity of an entity's IT environment.

The pseudo-anonymous nature of a public blockchain often increases risks related to undisclosed related party transactions or transactions with entities subject to sanctions or other regulations. There may be no record of which transactions relate to one another, such as may be the case if there is a side arrangement to an initial contract. Moreover, although the blockchain ledger may provide the public address of the transacting parties and the amount of value exchanged, and transactions can be tracked using a transaction identification number or an address, the technology does not provide any information concerning the identity of the counterparty or the appropriate recognition or classification in the financial statements.

As a result of these factors, the auditor may need to test the effectiveness of certain processes and controls around digital assets because substantive procedures alone may not be sufficient to obtain sufficient appropriate audit evidence.[33] (Note: if the auditor plans on relying on controls, the auditor is required to test those controls.[34]) Consequently, more detailed inquiries or review of relevant documentation surrounding the entity's internal control and IT environment may be appropriate in the client acceptance and continuance process. Such inquiry and review may focus on the following areas:

- The blockchain technology and technology used by and relied on by the entity to track, aggregate, reconcile, and report digital assets balances and transactions
- The entity's method and controls implemented to hold and secure digital assets and to authorize and track digital asset transactions
- The entity's controls established to identify, authorize, and approve related parties and relationships and transactions with related parties

Each of these areas is discussed in more detail in the following subsections.

The blockchain technology and technology used by and relied on by the entity to track, aggregate, reconcile, and report digital assets balances and transactions

During the client acceptance and continuance process, obtaining an understanding of the nature of blockchain technology and the technology used to track, aggregate, reconcile, and report digital assets balances and transactions helps the auditor assess the extent of audit procedures that may be required. The nature and extent of procedures performed to obtain an understanding of the technology used by the entity will vary depending on the entity's role in the digital asset ecosystem.

It will be important for the auditor to obtain an understanding of the underlying blockchain technology related to the digital asset transactions. If an entity derives its books and records of balances and transactions solely from the blockchain or from statements provided by a third party, the auditor may want to further understand, as part of the acceptance and continuance process, management's processes and controls over the quality of this information. In certain instances, audit evidence obtained from the blockchain or such third parties may not constitute sufficient appropriate audit evidence, and further procedures may be warranted.

As noted, entities may have separate financial reporting systems apart from the blockchain or from a third party to evaluate whether digital asset transactions have been appropriately recorded with their financial records. For example, reconciliation of digital asset balances and transactions from accounting records to the relevant blockchain or a third party may be accomplished through manual processes or through automated processes. The volume of transactions

[33] Paragraph .31 of AU-C section 315.

[34] Paragraph .07 of AU-C section 330.

and addresses processed by the entity and how the entity processes these balances and transactions, including whether the entity maintains a copy of the blockchain to independently reconcile transactions and whether the systems were developed in house or purchased from third parties may also be important to determine the extent of audit procedures necessary to obtain sufficient appropriate audit evidence.

Additionally, the extent to which balances and transactions are recorded internally by the entity and not transmitted to the blockchain (off-chain transactions) may also be relevant. Some entities, primarily entities operating as digital asset exchanges, may record their customers' transactions on an internal ledger and send transactions to be recorded on the blockchain (on-chain transactions) only if the transaction is taking place between an address controlled by the entity and an address not controlled by the entity. Off-chain transactions may present additional challenges in obtaining audit evidence as compared to a transaction recorded on the blockchain.

Transacting and safeguarding digital assets typically requires a number of IT systems to process and record digital asset activity. As such, the auditor may consider assessing whether substantive procedures alone will provide sufficient appropriate audit evidence. In the instances where substantive procedures alone may not provide sufficient appropriate audit evidence, obtaining an understanding of the design, implementation, and operating effectiveness of IT general controls and application controls may be relevant in the client acceptance or continuance process.

Finally, due to the evolving nature of the industry and the technology used by companies within the digital asset ecosystem, it is important for management and the auditor to stay apprised of current and anticipated changes in the underlying technology used by the entity.

The entity's method and controls implemented to hold and secure digital assets and to authorize and track digital asset transactions

Blockchain transactions are designed to be difficult or impossible to reverse. Although the same could be said for any double-entry bookkeeping application, the peer-to-peer nature of blockchains means that once an entity sends a transaction to a particular wallet address, there is no adjusting blockchain entry that can be made unless the counterparty is actively involved. As such, erroneous or inappropriate digital assets transfers may result in the permanent loss of digital assets. Consequently, controls over initiation and authorization of transactions are critical.

Similarly, given that digital assets are secured using cryptography that results in "private keys" that provide control (that is, the ability to transfer) of the associated digital assets, there is an inherent risk that the private keys could be stolen, lost, or misused by either internal or external parties. One example of misuse could be sharing private keys to facilitate an intentional misreporting of assets through a fraud. Private key security and understanding how private keys are controlled is paramount, because anyone with access to the private keys of the entity's assets can use or send those assets, and thus obtaining an understanding of the entity's methods of storing and safeguarding the private key (for example, hot/cold self-storage or through a third-party custodian) is important.

Digital assets held by the entity

If the entity stores digital assets itself (also referred to as *self-custody*), it may be important for the auditor to consider the entity's related technical capabilities, including the entity's ability to verify existence of the digital asset as well as safeguards in place to prevent digital asset loss due to fraud or error. In most public blockchains, the underlying digital assets are bearer instruments and private keys that are lost or stolen represent irreversible, and typically uninsured, losses for the entity, with no recourse due to the decentralized nature of the blockchain.

Obtaining an understanding of the entity's safeguards related to the storage and transaction initiation/authorization of digital assets, may include, but is not limited to, inquiring about the policies, processes and controls around the following:

- The security of the physical location of the private keys
- The processes surrounding key lifecycle management, including the key generation process (hardware, software, and algorithms associated with generation)
- The security of the entity's data centers
- Access to private keys, including redundant private keys
- The number of users required to process a transaction, whether through encrypting and splitting of keys or multisignature address signing requirements
- Segregation of duties in the authorization of digital asset transactions

The auditor will need to obtain an understanding of how management intends to provide evidence related to the ownership assertion of the digital assets. In some instances, management may assert that the entity's ability to sign messages demonstrates their control of those digital assets and therefore can provide audit evidence of the ownership assertion. In certain instances, operational limitations may prohibit the entity from signing messages using their private keys, which further reduces available substantive evidence to support the ownership assertion. Although control of a digital asset is one consideration in the evaluation of the ownership assertion, the auditor will need to determine whether the demonstration of control in this manner constitutes sufficient evidence of ownership of the related digital assets or whether other considerations or procedures are necessary, such as testing the effectiveness of internal controls. The auditor may determine that substantive procedures alone are not adequate to provide sufficient audit evidence of the ownership assertion.

Digital assets held by a third-party custodian

If an entity relies on a third-party custodian to store its digital assets, the auditor considers additional risks both at the entity and the custodian. Determining the level of interaction between the entity and the custodian, including who has the ability to initiate transactions, may be critical to determining whether the preconditions for an audit are present. For example, audit procedures to test digital asset ownership by obtaining signed messages may require interaction with the custodian. If so, understanding whether the custodian is willing and technically capable to assist in the audit process helps the auditor evaluate whether the preconditions for an audit are present. As noted, professional judgment may be needed for the auditor to determine whether sufficient appropriate audit evidence can be obtained to prove ownership of the related digital asset.

For security, efficiency, or other reasons, the custodian may commingle assets of many customers into the same addresses and maintain the custodian's own off-chain ledger. Commingling and off-chain ledgers can complicate the auditor's verification of the entity's specific assets held by the custodian, because the blockchain is no longer representative of the entity's holdings alone. In these instances, the auditor may need to consider procedures to confirm balances with the custodian. Confirmation procedures require the auditor to determine whether the custodian's confirmation is reliable as audit evidence, which may require additional procedures. As of this writing, there is no widely accepted confirmation form or process for digital asset custodians or exchanges, similar to what exists for cash balances held at financial institutions.

Management is responsible for designing, implementing, and maintaining internal control relevant to the preparation and fair presentation of financial statements, including establishing controls over information received from service organizations such as an exchange or controls over the safeguarding of assets that may occur at a custodian. As a part of the acceptance and continuance process, the auditor may seek to understand controls implemented by management to monitor service organizations. Management's controls may include performing appropriate reviews of SOC reports by personnel with the relevant competency and skill set and implementing complementary user entity controls. In the event SOC reports are not available, understanding alternative controls implemented by management (for example reconciliations of third-party data to the entity's independent books and records) will be important. The auditor may wish to obtain the SOC report to consider whether the auditor can rely on the SOC report, as a part of the acceptance and continuance process. If the auditor is unable to determine whether the auditor can rely on the SOC report or that the scope of the report is not relevant for audit purposes, inquiring of the client about the auditor's ability to perform audit procedures at the service organization will help the auditor assess the sufficiency of audit evidence that can be obtained. Often custodians will offer a SOC 2® report in lieu of SOC 1® reports. Although SOC 2 reports may offer greater insights on controls implemented to address trust service principles, they do not necessarily provide insights on the controls over processing of transactions for financial statement reporting. Additionally, SOC 1 reports may not contain control objectives relating to generation, security, and monitoring of the keys used in these transactions, and the lack of this information may affect obtaining a thorough understanding of the relevant controls related to financial reporting. If a SOC report is unavailable, it is important for the auditor to consider whether additional procedures will be necessary and feasible to obtain sufficient appropriate audit evidence for reliance on information produced by the service organization.

Additionally, due to the pseudo-anonymous nature of blockchain transactions, obtaining an understanding of whether customer onboarding and due diligence procedures are performed by the custodian assists the auditor in determining whether business risks at the custodian could result in legal or other risks associated with noncompliance with BSA, AML, or other regulations.

The entity's controls established to identify, authorize, and approve related parties and relationships and transactions with related parties

The pseudo-anonymous nature of blockchain transactions may create challenges in determining the identity of the parties with which the entity transacts, hence increasing the risk associated with the completeness of related party relationships, transactions, and disclosures. Understanding the policies, processes, and controls performed by the entity assists the auditor in assessing the risk that a counterparty to the entity's transactions is a potentially undisclosed related party.

The auditor's inquiry surrounding compliance with KYC, AML, and other regulations as discussed in section 4 in tandem with other processes may assist in the identification of related parties and relationships, as well as transactions with related parties.

Procedures to consider specific to digital assets

The preceding section addressed challenges as well as some inquiries or procedures auditors may consider addressing the underlying challenges. Some additional procedures specific to the digital asset ecosystem to consider as part of the acceptance and continuance process may include the following:

- Inquire with management, specifically those from the IT department, to understand the nature of the IT general controls, application controls, processes in place to track, aggregate, and reconcile digital assets as well as mitigate IT risks associated with the underlying blockchain technology and any known deficiencies.
- Evaluate the competence of the entity's personnel involved with the controls and processes and understand the technology used to transact with digital assets.
- Understand the entity's use of IT specialists (internal or external) and whether plans exist to implement new technology to allow for the processing of digital asset transactions. New digital assets that are created and supported by new technologies require management to be able to implement processes to read and process digital asset transactions and account for them.
- Understand the entity's use of service organizations (for example, to secure private keys) and the availability of SOC reports. Obtain and read any SOC reports (including SOC 2 reports) that are available and obtain an understanding of whether management has controls in place to review SOC 1 reports and appropriate complementary user entity controls. The auditor should focus on the responsiveness of the controls in the SOC report to the financial reporting risks.
- Inquire with management to understand their due diligence procedures performed on third-party service providers (for example, custodians), including gaining an understanding of the processes and controls performed by the third party related to customer onboarding and due diligence.
- Understand the entity's due diligence process for transacting in new digital assets, such as how it assesses the consensus protocol, and the governance model and process for evaluating available wallet software that may be needed to transact. Consider whether certain assets that are specifically designed to further increase individual privacy may affect the auditor's ability to obtain sufficient appropriate audit evidence.
- Understand the entity's protection of private keys and other customer information, including the following:
  - The infrastructure used to generate and store private keys, including how private keys are stored (for example, hot wallets and cold wallets)
  - Segregation of duties in the authorization of digital asset transactions
  - The number of users required to process a transaction, whether through encrypting and splitting of keys or multisig address signing requirements
  - Monitoring of addresses for any unauthorized activity
- Understand the entity's process for identifying, accounting for, and disclosing related parties and relationships, as well as related party transactions.
- Understand the existence of cybercrime or fidelity insurance from reputable carriers.
- Understand the wallet software and wallet backup (for example, whether encrypted private key information is backed up to provide the entity with continued access to the private key in case of system failure).

Association of International Certified Professional Accountants™

AICPA® CIMA®

The Association of International Certified Professional Accountants, powering leaders in accounting and finance around the globe