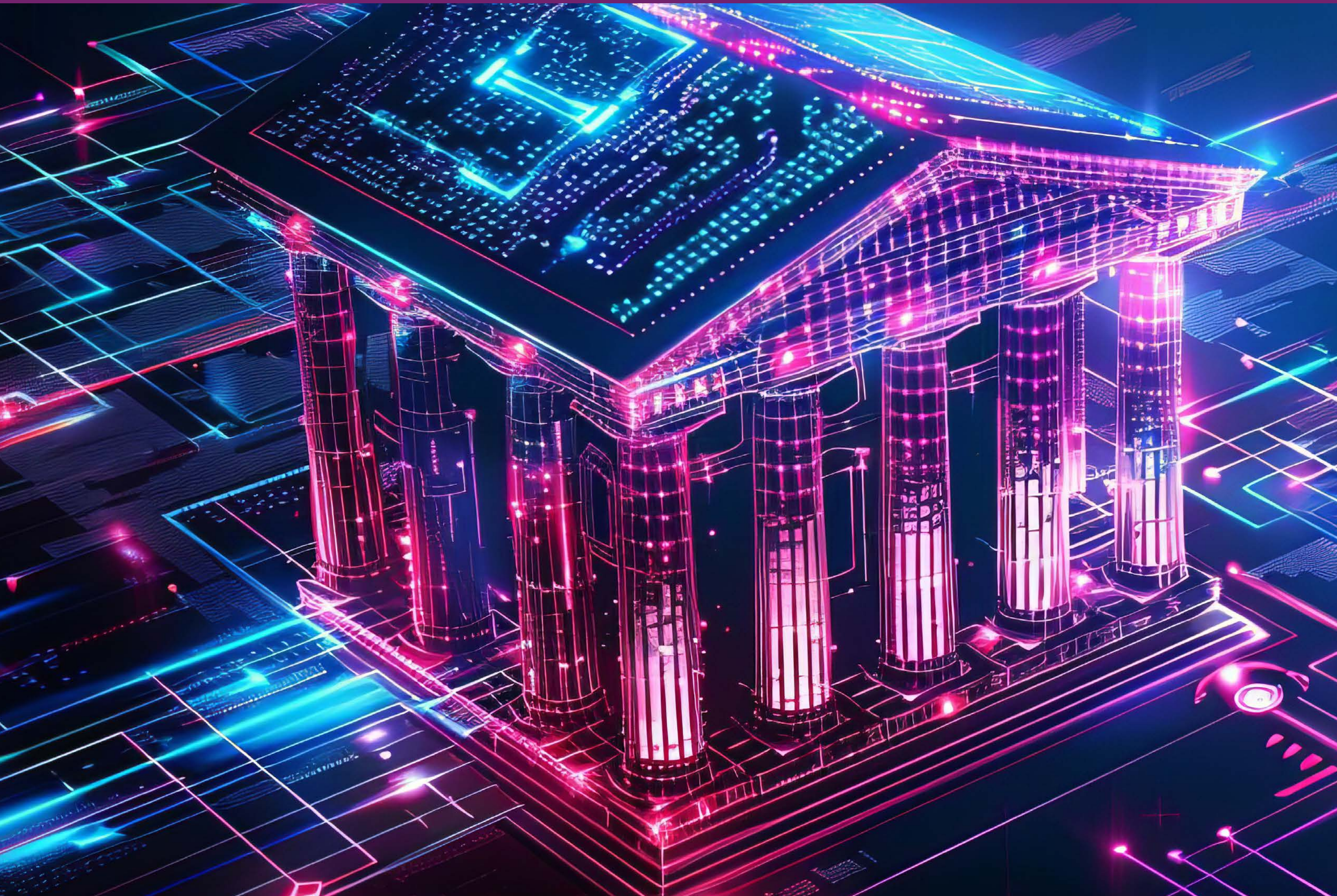
Practice aid

AICPA®

Accounting for and auditing of digital assets

as of Sept. 30, 2025



Digital Assets Working Group

Accounting Subgroup

Beth Paul, *Chair*
PwC

Monique Cole
RSM US LLP

Geoff Griffin
Ernst & Young LLP

Rahul Gupta
Grant Thornton LLP

Kevin Jackson
PwC

Jin Koo
BDO USA LLP

Jeff Megaro
Cohen & Company

Scott Muir
KPMG LLP

Amy Park
Deloitte & Touche LLP

Sean Prince
Crowe LLP

Aleks Zabreyko
Connor Group

Auditing Subgroup

Amy Steele, *Chair*
Deloitte & Touche LLP

Jennifer Alzona
Grant Thornton LLP

Damon Busse
Baker Tilly US, LLP

Michael Dellavalle
Cohen & Company

Mary Grace Davenport
PwC (Retired)

Michael Gonzales
Ernst & Young LLP

Jeremy Goss
Forvis Mazars LLP

Sara Krople
Crowe LLP

Dylan McDermott
Coinbase

Shelby Murphy
Deloitte & Touche LLP

Mark Murray
RSM US LLP

Rich Perilloux
Crowe LLP

Joey Ryan
CBIZ

Kristen Schrader
PwC

Jay Schulman
RSM US LLP

Kyle Sewell
BDO USA LLP

Robert Sledge
KPMG LLP

Jagruti Solanki
BitPay

Markus Veith
Grant Thornton LLP

Jodie Yan
KPMG LLP

AICPA®

Financial Reporting Executive Committee

Mark Crowley, *Chair*
Steve Belcher
Sally Bishop
Joe Cascio
Cathleen DeGenova
Melissa Galasso

David Gonzales
Rahul Gupta
Rich Jones
Scott Lehman
Kathy Pighini
Esther Mills

Scott Muir
Rob Nowlin
Ken Stoler
Doug Wright
Yan Zhang

Assurance Services Executive Committee

Mary Grace Davenport, *Chair*
Angela Appleby
Denny Ard
Jim Burton, *Immediate Past Chair*

Dora Burzenski
Margaret Christ
Rich Davisson
Werner Erasmus

Bridgett Gyorfi
Khadyja Johnson
Tina Kim

Auditing Standards Board

Sara Lord, *Chair*

AICPA staff

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

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

Jennifer Burns, *Chief Auditor*
Audit & Attest Standards
AICPA

Mike Glynn, *Senior Manager*
Audit & Attest Standards
AICPA

Daniel Noll, *Vice President*
Financial Reporting, Valuation &
Forensic Services
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; Matthew Schell (former chair), Angie Hipsher-Williams, Mark Shannon, and Christopher Moore of Crowe LLP; James Yamasaki of Deloitte & Touche LLP; Michael Harrington, Lan Ming, Anna Gosine, and Michael Kornstein of Ernst & Young LLP; Mike Santay and Dan Voogt of Grant Thornton; Nick Tricarichi, Brian Fields, and Ian Wildenborg of KPMG LLP; Rick Day of RSM US LLP; Jay Brodish of PwC; Bryan Martin of BDO USA LLP; Jamie Gasiorowski, Christian Randall, and Corey McLaughlin of Cohen & Company; Michael Bingham of the U.S. Government Accountability Office; Yoland Sinclair of Centri Business Consulting LLC; and the following industry reviewers: Jeremy Dillard of SingerLewak LLC; 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; Mary Kauffman of Lightspark; Rob Loban of Gemini; Aaron Jacob of TaxBit; Donna Brinton of Anchorage; Lynne Weber, Ph.D., of Kroll LLC; Muhammad Qasim Farooq of Abra; June Huang of Franklin Templeton; and Libby Schultz of Ciphercounts.

Notice to readers

The objective of this practice aid is to provide nonauthoritative guidance on how to account for digital assets under U.S. generally accepted accounting principles (GAAP) for nongovernmental entities and audit such digital assets in accordance with generally accepted auditing standards (GAAS). This guidance is intended for financial statement preparers and auditors with a fundamental knowledge of blockchain technology. For the purposes of this practice aid, a digital asset is defined broadly as a digital record that is an asset; is created or resides on a distributed ledger based on blockchain or similar technology; and is secured through cryptography. 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 is not an official pronouncement of the AICPA.

Throughout this practice aid the terms *digital assets, crypto intangible assets, in-scope crypto intangible assets,* and *out-of-scope crypto intangible assets* are used. Please refer to the Blockchain Universal Glossary for the applicable definitions of those terms used in this practice aid.

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, which did not object to its issuance.

Accounting standards and regulatory updates issued but not yet effective

This practice aid has been updated to reflect standards that have been issued and are effective as of the date of publishing. In addition, this practice aid reflects the amendments in FASB ASU No. 2023-08, *Intangibles — Goodwill and Other — Crypto Assets (Subtopic 350-60): Accounting for and Disclosure of Crypto Assets,* even though this ASU is not *mandatorily* effective until fiscal years beginning after Dec. 15, 2024.

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 another auditing publication as defined in paragraph .14 of AU-C section 200, *Overall Objectives of the Independent Auditor and the Conduct of an Audit in Accordance With Generally Accepted Auditing Standards.* 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, in accordance with paragraph .28 of AU-C section 200,[1] exercising professional judgment, assess the relevance and appropriateness of such guidance to the circumstances of the audit. The auditor may presume that other auditing publications published by the AICPA that have been reviewed by the AICPA Audit & Attest Standards staff are appropriate.

Auditing standards issued but not yet effective

This practice aid has been updated through Statement on Auditing Standards (SAS) No. 148, with the exception of SAS No. 146, *Quality Management for an Engagement Conducted in Accordance With Generally Accepted Auditing Standards,* which is not yet effective as of the date of publishing.

SAS No. 146 is effective for audits of financial statements for periods ending on or after Dec. 15, 2025.

The ASB has issued the following SAS, which is effective for audits of financial statements for periods ending on or after Dec. 15, 2026:

- SAS No.149, *Special Considerations – Audits of Group Financial Statements (Including the Work of Component Auditors and Audits of Referred-to Auditors)*

The preceding SASs are not reflected in this practice aid as they are issued but not yet effective as of the date this practice aid has been published. As these standards become effective, this practice aid will be updated.

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

Contents

Contents (continued)

AC Chapter 2: Investment companies

Questions [Published October 2020]

AC Chapter 3: Broker-dealers

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, *Financial Services — Brokers and Dealers,* and AICPA Audit and Accounting Guide *Brokers and Dealers in Securities.* 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.

AC Chapter 4: Fair value measurement

Questions [Published October 2020]

Contents (continued)

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

AC Chapter 5: Stablecoins

Questions [Published October 2020]

Contents (continued)

AC Chapter 6: Derivatives and embedded derivatives

Questions [Published January 2022]

Note: Q&A 24 is not intended for those entities that apply specialized industry guidance (for example, FASB ASC 946, *Financial Services — Investment Companies*, or FASB ASC 940, *Financial Services — Brokers and Dealers*). See Q&As 11, 12, 13, 14 and 15 for guidance related to investment companies and broker-dealers.

AC Chapter 7: Crypto intangible asset lending and borrowing

Questions [Published 2022]

Note: Q&As 25 and 26 are not intended for those entities that apply specialized industry guidance (for example, FASB ASC 946, *Financial Services — Investment Companies,* or FASB ASC 940, *Financial Services — Brokers and Dealers*). See Q&As 11, 12, 13, 14 and 15 for guidance related to investment companies and broker-dealers.

AC Chapter 8: Mining

Questions [Published January 2022]

Contents (continued)

Auditing Subgroup: Part I

Contents (continued)

Auditing Subgroup: Part II

AU Chapter 6: Considerations for valuation of digital assets

Questions [Published June 2024]

AU Chapter 7: Considerations for crypto intangible asset lending and borrowing

Questions [Published September 2025]

Appendix A

Appendix B

[2] On January 30, 2025, SEC Staff Accounting Bulletin (SAB) No. 122 was published in the Federal Register and became effective. SAB No. 122 rescinds SAB No. 121, *Accounting for Obligations to Safeguard Crypto-Assets an Entity Holds for its Platform Users*. For more information on SAB No. 122, see note at top of Appendix B, "SEC Staff Accounting Bulletin No. 121 Questions and Answers".

Introduction

What’s new?

- September 2025 added question and answers
  - AU chapter 7, “Considerations for crypto intangible asset lending and borrowing”

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 apply 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 in accordance with GAAS. Audits which are within the Public Company Accounting Oversight Board's (PCAOB) jurisdiction as defined by the Sarbanes-Oxley Act of 2002, as amended, and nonaudit 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.

In addition, see paragraph .07, "Operating Node Software on a Blockchain," in Q&A section 100, *Independence*,[1] at the following link:

pub.aicpa.org/codeofconduct/resourceseamlesslogin.aspx?prod=ethics&tdoc=et-qa&tptr=et-qa100

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, and 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.

[1] All Q&A sections can be found in *Technical Questions and Answers*

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-cima.com. 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.

In addition, see the digital assets and blockchain resource page for more blockchain resources at https://www.aicpa-cima.com/resources/landing/digital-assets-and-blockchain-resources.

Accounting Subgroup

AC Chapter 1: Classification, measurement, and recognition

Classification and measurement when an entity purchases digital assets[1]

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 digital assets for cash?[2]

Response 1:

An entity that purchases a digital asset for cash should first determine the nature of the asset based on its rights. For example:

- If the digital asset is legal tender[3] and is backed by a sovereign government, we believe it would meet the definition of *cash* or *cash equivalents* (as defined in the FASB ASC Master Glossary).
- If the digital asset provides the holder with a contractual right to receive cash or another financial instrument or an ownership interest in an entity, it would meet the definition of a *financial instrument* or *financial asset* (as defined in the FASB ASC Master Glossary). See Q&As 22 and 23 in chapter 5, "Stablecoins," of this practice aid for a discussion of accounting for stablecoin holdings.

Even if the digital asset is classified as held for sale in the ordinary course of business, it is not a tangible asset and, therefore, may not meet the definition of *inventory* (as defined in the FASB ASC Master Glossary).

Often, an entity will classify a digital asset as an intangible asset given that the FASB ASC Master Glossary defines intangible assets as assets (not including financial assets) that lack physical substance.

Digital assets that meet the definition of an intangible asset (as defined in the FASB ASC Master Glossary) are hereinafter referred to as "crypto intangible assets." Crypto intangible assets purchased for cash would initially be measured at cost. (See Q&A 2A of this chapter.)

When an entity acquires crypto intangible assets, it should determine if they are in the scope of FASB ASC 350-60, *Intangibles — Goodwill and Other — Crypto Assets* (that is, in-scope crypto intangible assets).[4]

[1] For the purposes of this practice aid, a *digital asset* is defined broadly as a digital record that is an asset; is created or resides on a distributed ledger based on blockchain or similar technology; and is secured through cryptography.

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

[3] 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.

[4] This includes entities that apply industry-specific U.S. GAAP (for example, investment companies in the scope of FASB ASC 946 and broker-dealers in the scope of FASB ASC 940). Such entities are not excluded from the scope of FASB ASC 350-60 and need to consider the financial statement presentation and disclosure requirements of that Subtopic to the extent they are incremental to those required under the entities' respective industry-specific Topics.

Crypto intangible assets meeting all the following criteria (see FASB ASC 350-60-15-1) are in-scope crypto intangible assets:

a. Meet the definition of intangible assets as defined in FASB codification

b. Do not provide the asset holder with enforceable rights to or claims on underlying goods, services, or other assets

c. Are created or reside on a distributed ledger based on blockchain or similar technology

d. Are secured through cryptography

e. Are fungible

f. Are not created or issued by the reporting entity or its related parties (as defined in the FASB ASC Master Glossary and as reproduced in the Blockchain Universal Glossary).

Holdings of in-scope crypto intangible assets are presented separately from other intangible assets on the balance sheet and subsequently measured at fair value with gains and losses from the remeasurement recorded in net income. (See Q&A 9A of this chapter).

For crypto intangible assets outside the scope of FASB ASC 350-60 (that is, out-of-scope crypto intangible assets), an entity should determine whether they have 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 out-of-scope crypto intangible asset to the entity, then it would be classified as an indefinite-lived intangible asset.

Question 1A:

Are “wrapped tokens” in the scope of FASB ASC 350-60?

Response 1A:

It depends. There is not a definition for wrapped token in U.S. GAAP nor is there a consistent industry usage of that term; therefore, a wrapped token is subject to the same FASB ASC 350-60 scoping criteria as any other digital asset.

While wrapped tokens, as “digital assets” (see Q&A 1 of this chapter), meet the criteria in FASB ASC 350-60-15-1(c) and (d), a wrapped token may fail to meet one or more of the following remaining scoping criteria in FASB ASC 350-60-15-1:

- The digital asset meets the U.S. GAAP definition of an intangible asset.
- The digital asset does not provide the asset holder with enforceable rights to or claims on underlying goods, services, or other assets.
- The digital asset is fungible.
- The digital asset is not created or issued by the entity (or its related parties).

Each wrapped token will need to be carefully evaluated against these criteria based on its specific rights, obligations, and attributes, and the conclusion as to scope may differ from one wrapped token to the next based on the facts and circumstances.

Question 1B:

Are nonfungible tokens (NFTs) in the scope of FASB ASC 350-60?

Response 1B:

No. NFTs fail the fungibility criterion in FASB ASC 350-60-15-1(e).

In addition, an NFT will often also fail one or both of the criteria in FASB ASC 350-60-15-1(a) and 15-1(b). For example, an NFT may not meet the definition of an intangible asset if it is a financial asset or may fail the enforceable right to other goods and services criterion if it conveys to the holder a license to intellectual property.

Recognition and initial measurement when an entity receives crypto intangible assets[5]

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 crypto intangible 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 crypto intangible asset in return. 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 crypto intangible asset as consideration under a revenue contract with a customer?[6]

Response 2:

Entity A would treat the receipt of the crypto intangible 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 (crypto intangible asset) at its estimated fair value[7] 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 crypto intangible 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 crypto intangible 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 or FASB ASC 350-60 as discussed in Q&As 4, 5, 6, and 7 of this chapter. (For Q&As specific to stablecoins, see AC chapter 5, "Stablecoins," of this practice aid.)

[5] Refer to the definition of *crypto intangible asset* in Q&A 1 of this chapter.

[6] 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.

[7] 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 2A:

Are transaction costs (for example, commissions, gas fees) to acquire crypto intangible assets included in the initial measurement of the acquired asset?

Response 2A:

Regardless of whether the crypto intangible asset is an in-scope[8] or out-of-scope crypto intangible asset, its initial measurement is governed by FASB ASC 350-30. Under FASB ASC 350-30-30-1, an intangible asset that is acquired either individually or with a group of other assets (but not acquired in a business combination) is initially measured in accordance with FASB ASC 805-50-30-1 through 30-2.

Under FASB ASC 805-50-30-1 through 30-2, assets subject thereto are initially measured at their cost to the acquirer (that is, purchaser), which generally includes any transaction costs. Transaction costs is not a defined term in U.S. GAAP but is widely understood to refer to direct costs to acquire assets, and to not include indirect costs, such as general and administrative expenses.

(See Q&A 4 of this chapter for additional information on subsequent measurement.)

Question 3:

If the facts in Q&A 2 changed such that Entity A were to receive the crypto intangible 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 crypto intangible asset. In arrangements that involve the future receipt of a crypto intangible 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 crypto intangible asset in the future is a derivative or a hybrid instrument containing an embedded derivative. (For additional information on derivatives, see AC chapter 6, "Derivatives and embedded derivatives," of this practice aid.)

[8] See FASB ASC 350-30-15-4(e).

Subsequent accounting for indefinite-lived out-of-scope crypto intangible assets

Question 4:

How should an entity account for indefinite-lived out-of-scope crypto intangible assets subsequent to their acquisition?

Response 4:

An indefinite-lived out-of-scope crypto intangible asset is initially carried at the value determined in accordance with FASB ASC 350-30-30-1 and is not subject to amortization.[9] 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 not subject to amortization.

Question 5:

If an entity holds an indefinite-lived out-of-scope crypto intangible asset and identical out-of-scope crypto intangible 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 indefinite-lived out-of-scope crypto intangible asset 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 generally serve as an indicator that impairment is more likely than not. This is the case regardless of when this occurs during the reporting period and whether the price recovers before the end of the reporting period.

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, when determining whether a potential impairment is indicated.

[9] 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.

If an entity determines it is more likely than not that the indefinite-lived out-of-scope crypto intangible asset is impaired based on transactions of identical assets below its carrying value, the entity should determine the asset's fair value at that point in time even if the price that indicated impairment is an intra-day price that recovers later during the same day.

Fair value is determined in accordance with FASB ASC 820, *Fair Value Measurement*. If, based on its assessment, the entity concludes that the fair value of the indefinite-lived out-of-scope crypto intangible asset is less than its carrying value, an impairment loss should be recorded.

Question 6:

If the fair value of an indefinite-lived out-of-scope crypto intangible asset has declined below its 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 an indefinite-lived out-of-scope crypto intangible asset 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 out-of-scope crypto intangible 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 asset recovers above the original carrying value within the same accounting period.

Example: ABC Entity holds 1 million units of an indefinite-lived out-of-scope crypto intangible asset, which it purchased for cash on January 1, 20X1, for $10 per unit. During the last week of January 20X1, units of the same out-of-scope crypto intangible 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 out-of-scope crypto intangible assets were 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 out-of-scope crypto intangible asset were traded above ABC Entity's original carrying value. Although this may indicate that the fair value of the out-of-scope crypto intangible asset has increased above its 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 indefinite-lived out-of-scope crypto intangible asset holdings?

Response 7:

Entities often engage in multiple acquisitions and dispositions of out-of-scope crypto intangible assets during a period. For indefinite-lived out-of-scope crypto intangible assets, entities should determine the unit of account for purposes of testing 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 an out-of-scope crypto intangible 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 out-of-scope crypto intangible assets (or a divisible fraction of an individual unit).

When performing the impairment testing for an individual indefinite-lived out-of-scope crypto intangible 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 out-of-scope crypto intangible assets of the same type purchased at different prices.

This approach could lead to an inappropriate reduction in 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 out-of-scope crypto intangible asset units (or divisible fractions of a unit) with the same acquisition date and the same carrying value.

Determining the cost basis and carrying value of crypto intangible assets when derecognized

Question 8:

When selling a portion of an entity's crypto intangible asset holdings, how should an entity determine the cost basis and carrying value of the units sold?

Response 8:

For crypto intangible assets, entities should track the cost basis and carrying value of units (or fractional units – see Q&A 7 of this chapter) they obtain at different times and use this amount for each asset unit upon derecognition. Crypto intangible assets typically represent fungible units. It may not be possible to identify which specific units were sold or transferred in certain cases. For instance, it may be clear that the number of units held has gone down (for example, from 10 units to nine 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 this circumstance by developing a reasonable and rational methodology for identifying which units were sold and applying it consistently. For example, one reasonable and rational methodology could be the first in, first out (FIFO) method. When selecting a methodology, entities should be mindful that while the weighted average cost method would be acceptable for in-scope crypto intangible assets as referenced in FASB ASC 350-60-50-2a and, frequently, for investment companies in the scope of FASB ASC 946, that method would not be appropriate for out-of-scope crypto intangible assets because, as described in Q&A 7 of this chapter, each out-of-scope crypto intangible asset unit (or fractional unit) is its own unit of account.

Derecognition of crypto intangible assets

Question 9:

How should an entity account for the sale of crypto intangible assets?

Response 9:

An entity may transfer crypto intangible assets by exchanging them for fiat currencies (for example, crypto intangible 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 crypto intangible asset X is an output of the entity's ordinary activities), an entity should account for the sale under FASB ASC 606 and present the sale as revenue when control of the crypto intangible assets sold has transferred. If the counterparty is not a customer (that is, selling crypto intangible asset X is not an output of the entity's ordinary activities), 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 is presented net, outside of FASB ASC 606 revenue (net gain or loss as determined by subtracting the cost [or subsequent carrying value] from the measured consideration).

Question 9A:

Are gains and losses from the remeasurement and sale of in-scope crypto intangible assets presented as operating or nonoperating items in the entity's income statement?

Response 9A:

In accordance with FASB ASC 350-60-45-2, gains and losses from the remeasurement of in-scope crypto intangible assets should be included in net income and presented separately from changes in the carrying amount of other intangible assets. However, FASB ASC 350-60 does not provide guidance on operating versus nonoperating income statement classification; therefore, other U.S. GAAP applies.

In paragraph BC48 in the Basis for Conclusions to FASB ASU No. 2023-08, *Intangibles — Goodwill and Other — Crypto Assets, Accounting for and Disclosure of Crypto Assets,* FASB observed that an entity should classify gains or losses from the remeasurement of in-scope crypto intangible assets as operating or nonoperating based on the entity's facts and circumstances.[10] Therefore, this is an entity-specific determination, and one entity may not reach the same conclusion as another entity.

By contrast, any difference between the sale price of the in-scope crypto intangible asset and its FASB ASC 820 fair value immediately prior to transfer, which, for example, may arise if the entity sells the asset in a market that is not its FASB ASC 820 "principal market" should be classified as operating income (loss) items in the following situations:

- **The sale is subject to FASB ASC 606**, and therefore the sale will give rise to revenue and cost of goods sold, which are both operating income (loss) items; or
- **The sale is subject to FASB ASC 610-20**, which in FASB ASC 610-20-45-1 refers entities to the guidance in FASB ASC 360-10-45-5 when presenting gains or losses on the sale of nonfinancial (and in-substance nonfinancial) assets within its scope, including in-scope crypto intangible assets. Under FASB ASC 360-10-45-5, selling gains or losses are presented in operating income (loss).

[10] This and other paragraphs from the "Background Information and Basis for Conclusions" section of FASB ASU No. 2023-08, *Intangibles — Goodwill and Other — Crypto Assets, Accounting for and Disclosure of Crypto Assets,* were not codified in FASB ASC; however, the Digital Assets Working Group believes these paragraphs provide helpful guidance and, therefore, decided to incorporate them in this practice aid.

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),[11] 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[12] 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. 8, *Conceptual Framework for Financial Reporting—Chapter 4, 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 the 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 multi-signature wallet and, if so, what are the digital signatures that are required to execute a transaction? Who holds the private keys to the multi-signature wallet and how is ownership evidenced through any applicable account agreements?

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

[12] 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. In this circumstance, because the digital asset is recorded as its own asset, the custodian would not be subject to SAB No. 121[13] for such digital assets.

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 815.

If the custodian does not have control over the digital asset such that it does not recognize the digital asset or digital asset return liability, the custodian should recognize a safeguarding liability and accompanying safeguarding asset if the custodian is subject to SAB No. 121 and determines it has a SAB No. 121 safeguarding obligation. Refer to appendix B, "SEC Staff Accounting Bulletin No. 121 Questions and Answers," of this practice aid for more information about SAB No. 121.

[13] On January 30, 2025, SEC Staff Accounting Bulletin (SAB) No. 122 was published in the Federal Register and became effective. SAB No. 122 rescinds SAB No. 121, *Accounting for Obligations to Safeguard Crypto-Assets an Entity Holds for its Platform Users*. For more information on SAB No. 122, see note at top of Appendix B, "SEC Staff Accounting Bulletin No. 121 Questions and Answers"..

AC Chapter 2: Investment companies

Meeting the definition of an investment company when engaging in digital asset[1] 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.

[1] Refer to the definition of *digital asset* in the Blockchain Universal Glossary.

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,"[2] 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.

[2] See https://www.aicpa.org/interestareas/frc/recentlyissuedtechnicalquestionsandanswers.html.
Q&A sections can be found in AICPA *Technical Questions and Answers.*

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.

AC Chapter 3: Broker-dealers

Recognition, measurement, and presentation of digital assets[1] 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,[2] 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.[3] 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[4] the discussion of the SEC's financial responsibility rules provided in the "Joint Staff Statement on Broker-Dealer Custody of Digital Asset Securities"[5] released by the SEC Division of Trading and Markets. 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).

[1] Refer to the definition of *digital asset* in the Blockchain Universal Glossary.

[2] See EITF Abstracts Issue No. 06-12.

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

[4] 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.

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

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[6] 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. However, the need for a safeguarding liability and related asset under SAB No. 121[7] should be considered (refer to appendix B, "SEC Staff Accounting Bulletin No. 121 Questions and Answers").

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 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."[8] 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.

[6] 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.

[7] On January 30, 2025, SEC Staff Accounting Bulletin (SAB) No. 122 was published in the Federal Register and became effective. SAB No. 122 rescinds SAB No. 121, *Accounting for Obligations to Safeguard Crypto-Assets an Entity Holds for its Platform Users*. For more information on SAB No. 122, see note at top of Appendix B, "SEC Staff Accounting Bulletin No. 121 Questions and Answers".

[8] See paragraph 5.66 of chapter 5, "Accounting Standards," of AICPA Audit and Accounting Guide *Brokers and Dealers in Securities* (broker-dealer guide).

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.[9] 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 the conclusion that it is within the scope of FASB ASC 940.

[9] Paragraph 5.02 of chapter 5, "Accounting Standards," 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.

AC Chapter 4: Fair value measurement

Considerations for digital assets[1] that require fair value measurement

Question 16:

When determining the fair value for digital assets, 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 digital 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 digital 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 digital asset. For example, if an entity normally buys and sells digital 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 digital 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 digital asset transactions in nonexchange 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.

[1] Refer to the definition of *digital asset* in the Blockchain Universal Glossary.

When there is a principal market for the digital 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 digital asset being valued. The most advantageous market is the market that maximizes the amount that would be received to sell the digital 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 digital asset.

Note: Q&As 16–21 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 digital assets trade when determining the fair value of a digital asset holding?

Response 17:

Digital 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 digital asset in accordance with FASB ASC 820, an entity would need to, among other things, determine the principal (or most advantageous) market in which a digital 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 digital 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 allows 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 digital assets trade to determine the appropriate inputs or techniques for determining the fair value of a digital asset. Refer to Q&As 18–20 of this chapter for further information.

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

Question 18:

Assume the principal (or most advantageous) market for a given digital asset 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 digital asset determined in this circumstance?

Note: It is not appropriate to use a volume-weighted average price (VWAP) or other types of aggregated pricing when measuring the fair value of digital assets traded in active markets. Doing so would not be consistent with the general principles of FASB ASC 820 which gives the highest priority to quoted prices in active markets and the lowest priority to unobservable inputs. Furthermore, FASB ASC 820 defines fair value as "the price that would be received to sell an asset… in an orderly transaction between market participants at the measurement date." A weighted-average or other aggregated measurement in these circumstances may not necessarily represent a price at which a transaction would take place.

Response 18:

If there is a principal market for the digital asset, the fair value measurement of the digital 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 digital 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, midpoint 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: Q&As 16–21 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 intangible asset[2] to reflect the size of the entity's holding?

Response 19:

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

> A reporting entity shall 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 shall 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 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.

Entities will generally reach a determination that the unit of account, for a crypto intangible asset, is the individual unit (or divisible fraction of a unit.) The portfolio exception in FASB ASC 820-10-35-18D is not applicable to crypto intangible assets and, therefore, it would be inappropriate to adjust their fair value measurement to reflect the size of an entity's holding.

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

[2] Refer to the definition of *crypto intangible asset* in Q&A 1 in AC chapter 1.

Question 20:

Certain digital asset markets operate continuously, without a traditional market close. How should entities consider the impact of activity through the end of the reporting date when determining the fair value of the digital asset or assessing if potential impairment triggers exist?

Response 20:

In such circumstances, an accounting convention may establish a cut-off time for determining the fair value of the digital 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.

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

The previous notwithstanding, entities should consider transactions that take place after the cut-off time but before the end of the reporting period, to the extent those differ, similar to the guidance in FASB ASC 820-10-35-41C. For example, if an identical out-of-scope crypto intangible asset is bought and sold at a price below the entity's carrying value after the cut-off time but before the end of the reporting period, the entity should record any indicated impairment even though the impairment indicator occurred after the entity's designated cut-off time. Similarly, while explicit guidance on an entity's cut-off time does not exist, for digital assets subject to fair value measurement (for example, in-scope crypto intangible assets or any crypto intangible assets held by an investment company), the fair value measurement should generally be based on the last trading price prior to midnight of the appropriate time zone of the reporting entity.

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

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 digital asset?

Response 21:

When evaluating the relevance of transaction prices as inputs into the fair value measurement of a digital 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 AICPA Guide *Valuation of Privately-Held-Company Equity Securities Issued as Compensation*[3] and paragraph 10.34 of 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[4] 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.[5] 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.

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

[3] Please note that there is a project underway to update AICPA Accounting and Valuation Guide *Valuation of Privately-Held-Company Equity Securities Issued as Compensation.* AICPA recently released for feedback an early working draft of chapter 8, "Inferring Value From Transactions in a Private Company's Securities," and chapter 9, "Selected Accounting and Disclosure Matters" from that guide. Among other things, the above-referenced framework has been updated to better articulate the principles of FASB ASC 820, *Fair Value Measurement.* Please stay alert to further developments in this project.

[4] 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.

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

AC Chapter 5: Stablecoins

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 digital asset, or a combination of multiple different assets. Others may not be collateralized or may not be redeemable. Generally, stablecoins 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 stablecoin holding 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 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, *Financial Services — Investment Companies*, or F*ASB ASC 940, Financial Services — Brokers and Dealers).*

Response 23:

Entity A's stablecoin holding would not be a derivative[1] but does meet the definition of a financial asset under GAAP because it can be redeemed for cash. If the stablecoin also meets the definition of a security,[2] 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.

[1] 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.*

[2] As defined in definition 2 in the FASB ASC Master Glossary, a *security* is a share, participation, or other interest in property or in an entity of the issuer or an obligation of the issuer that has all of the following characteristics:

- It is either represented by an instrument issued in bearer or registered form or, if not represented by an instrument, is registered in books maintained to record transfers by or on behalf of the issuer.
- It is of a type commonly dealt in on securities exchanges or markets or, when represented by an instrument, is commonly recognized in any area in which it is issued or dealt in as a medium for investment.
- It either is one of a class or series or by its terms is divisible into a class or series of shares, participations, interests, or obligations.

AC Chapter 6: Derivatives and embedded derivatives

Note: Q&A 24 is not intended for those entities that apply specialized industry guidance (for example, FASB ASC 946, *Financial Services — Investment Companies*, or FASB ASC 940, *Financial Services — Brokers and Dealers*). See Q&As 11, 12, 13, 14, and 15 for guidance related to investment companies and broker-dealers.

Contracts involving derivatives and embedded derivatives

Question 24:

Entity A provides a good to Entity B in exchange for a promise to receive a fixed quantity of crypto intangible assets.[1] Entity A recognizes a right to receive crypto intangible assets that will be settled in 30 days and revenue for the sale of the good. How should Entity A evaluate whether the asset representing the right to receive a fixed quantity of crypto intangible assets contains an embedded derivative?[2]

Response 24:

A right to receive crypto intangible assets may result from a variety of transactions, such as the sale of goods or services subject to FASB ASC 606, *Revenues from Contracts with Customers*. The evaluation of contracts involving the future delivery of crypto intangible assets would generally first consider FASB ASC 815, *Derivatives and Hedging*, at contract inception, to determine whether the contract is or contains a derivative that should be accounted for separately from the right to receive crypto intangible assets.

To determine if the right to receive crypto intangible assets represents a derivative in its entirety, Entity A evaluates the definition of a *derivative* in FASB ASC 815-10-15-83. The transaction is a result of an exchange of a good for a right to receive crypto intangible assets of equivalent value. As such, in this fact pattern, it does not represent a derivative contract in its entirety because it would not meet the initial net investment criterion in FASB ASC 815-10-15-83(b).[3] That is, in this case, Entity A's initial net investment (that is, the value of the good) is not less than, by more than a nominal amount, the initial net investment that would be required to acquire the crypto intangible asset. However, further evaluation should be performed to determine if the right to receive crypto intangible assets contains an embedded derivative that should be bifurcated and accounted for separately.

FASB ASC 815-15-25-1 provides guidance for evaluating whether a feature in a hybrid instrument is an embedded derivative subject to bifurcation. If the embedded derivative meets all the requirements of FASB ASC 815-15-25-1, then (1) the embedded derivative would need to be separately accounted for as a derivative, and (2) the host contract would be accounted for based on other applicable GAAP.[4]

[1] Refer to the definition of *crypto intangible asset* in Q&A 1 in AC chapter 1, "Classification, measurement, and recognition."

[2] This Q&A focuses on the evaluation of embedded features in a crypto intangible asset–denominated receivable. Although many elements of the analysis may be similar, this Q&A does not address how to evaluate an executory contract (such as an agreement to deliver goods or services in the future) for embedded features pursuant to FASB *Accounting Standards Codification* (ASC) 815, *Derivatives and Hedging.*

[3] Refer also to paragraphs 94–98 of FASB ASC 815-10-15 for additional details.

[4] Refer to FASB ASC 815-15-25-54.

Entity A should first assess the embedded feature to be evaluated. In this example, we believe the host contract should be viewed as the receivable denominated in the entity's functional currency, and the embedded feature is a forward contract that swaps the entity's functional currency for a fixed quantity of a crypto intangible asset. Entity A should evaluate the guidance in FASB ASC 815-15-25-1(a) to determine if the characteristics and risks of the embedded derivative (that is, the forward right to receive crypto intangible assets in the future) are clearly and closely related to the economic characteristics and risks of the host contract (a simple receivable that represents a debt host under FASB ASC 815). We believe Entity A would conclude that an embedded crypto intangible asset forward contract is not clearly and closely related to its host arrangement (a functional currency receivable for goods provided) because a forward contract on FASB ASC 350 intangible assets is not typically present in fiat financing arrangements.

Entity A would next consider whether the embedded derivative meets the definition of a *derivative* on a stand-alone basis in accordance with FASB ASC 815-15-25-1(c), as follows:

- FASB ASC 815-10-15-83(a): The forward element has a notional (that is, a fixed quantity of crypto intangible assets) and an underlying (that is, the price of the crypto intangible asset).
- FASB ASC 815-10-15-83(b): As noted previously, the hybrid contract requires a significant initial net investment. However, when evaluating whether the embedded derivative meets the definition of a *derivative* on a stand-alone basis, FASB ASC 815-15-25-1(c) states that the initial net investment for the hybrid instrument should not be considered to be the initial net investment for the embedded derivative. Because the embedded feature is an at-the-market forward arrangement, there is not more than an insignificant initial net investment.
- FASB ASC 815-10-15-83(c): The embedded feature will result in a fixed quantity of crypto intangible assets delivered. Assuming that there are no other features associated with the hybrid contract that would require or permit net settlement (that is, through the delivery of cash) and a market mechanism does not exist to net settle the contract, Entity A would need to evaluate (at inception and on an ongoing basis) whether the underlying crypto intangible assets to be delivered are readily convertible to cash. In instances when the underlying assets delivered are readily convertible to cash, the contract is effectively net settled and would meet the definition of a *derivative*.
- Assets are readily convertible to cash when they have both (1) interchangeable (fungible) units and (2) quoted prices available in an active market that can rapidly absorb the quantity held by the entity without significantly affecting the price.[5] Indicators for assessing whether crypto intangible assets are readily convertible to cash, include, but are not limited to (1) evidence that an *active market*[6] (as defined in FASB ASC 820) exists for the crypto intangible asset, (2) the conversion costs[7] associated with converting the crypto intangible assets to cash, including consideration of costs to access active markets and other factors, are not significant and (3) the market identified can rapidly absorb the contract quantity of crypto intangible assets to be delivered without affecting the price.[8]

Finally, Entity A should evaluate whether any FASB ASC 815 scope exceptions are applicable.

If Entity A determines that the embedded derivative should be bifurcated (that is, it meets all the criteria of FASB ASC 815-15-25-1), Entity A will bifurcate the forward arrangement at an initial fair value of zero, pursuant to FASB ASC 815-15-30-4 and subsequently measure the derivative at fair value. In accordance with FASB ASC 815-10, changes in fair value each period associated with the embedded feature (the forward contract) should be recognized in net income. If the embedded derivative is not bifurcated, Entity A may need to further consider impairment and other subsequent measurement concerns as well as the appropriate characterization of its right to receive the fixed quantity of crypto intangible assets.

[5] Refer to FASB ASC Master Glossary for the definition of *readily convertible to cash*.

[6] Per the FASB ASC Master Glossary, an *active market* is "a market in which transactions for the asset or liability take place with sufficient frequency and volume to provide pricing information on an ongoing basis."

[7] See paragraphs 125–127 of FASB ASC 815-10-15 for additional information on the effect of conversion costs.

[8] The spot market should be evaluated by comparing the crypto intangible asset contract quantity to the daily transaction volume to determine if and how the market price could be affected by the contract. If the price would not be significantly affected, then the market can rapidly absorb the contract.

AC Chapter 7: Crypto intangible asset lending and borrowing

Note: Q&As 25 and 26 are not intended for those entities that apply specialized industry guidance (for example, FASB ASC 946, *Financial Services — Investment Companies* or FASB ASC 940, *Financial Services — Brokers and Dealers*). See Q&As 11, 12, 13, 14, and 15 for guidance related to investment companies and broker-dealers.

Crypto intangible asset[1] lending

Question 25:

Assume a lender lends 100 units of a crypto intangible asset (Crypto Intangible Asset ABC) for a term of six months to a borrower.

The borrower will pay a fee in total of six units of Crypto Intangible Asset ABC for borrowing Crypto Intangible Asset ABC during the six-month loan period, paying one unit of Crypto Intangible Asset ABC each month in arrears during the term (this is typically referred to as an *interest payment* in the agreement). At the end of six months, the borrower is required to deliver 100 units of Crypto Intangible Asset ABC back to the lender. For purposes of the Q&A, assume that:

- Crypto Intangible Asset ABC is an intangible asset under FASB ASC 350.
- The ownership of loaned Crypto Intangible Asset ABC is transferred to the borrower upon the transfer, and the borrower has the right to transfer, encumber, or pledge the crypto intangible asset in any way it chooses.
- The borrower is not required to post collateral to the lender in the arrangement.
- The borrower has identified its functional currency as the U.S. dollar under FASB ASC 830, *Foreign Currency Matters*.

How should the lender account for the loan?

Response 25:

This response is based, in part, on comments made by the SEC staff at the AICPA & CIMA Conference on Current SEC and PCAOB Developments in Washington, D.C., in December 2022 and SEC staff discussions with the AICPA Digital Assets Accounting Working Group regarding the SEC staff view on the accounting for crypto intangible asset lending arrangements.

U.S. GAAP does not provide explicit guidance specific to the lending of crypto intangible assets and accordingly we understand the SEC staff considered all relevant guidance in U.S. GAAP but did not base its accounting conclusions solely on a single FASB ASC Topic. We understand that the SEC staff believes it would be appropriate, in this specific fact pattern, to conclude that the lender transferred control of the crypto intangible asset such that the asset should be derecognized by the lender. While this fact pattern did not require the borrower to post collateral, the posting of collateral would not impact the derecognition conclusion.

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

In assessing whether the crypto intangible assets lent should be derecognized in this fact pattern, various indicators of control and elements of asset derecognition would be considered, including, but not limited to, the following:

- The lender has transferred the present rights to the economic benefits associated with the crypto intangible asset for a different right to receive crypto intangible assets in the future;
- The lender cannot sell, pledge, loan, or otherwise use the lent crypto intangible assets while the loan is outstanding, as those rights have been transferred to the borrower;
- Inherent in the realization of the economic benefits associated with the crypto intangible asset loan receivable is exposure to credit risk of the borrower; and
- The borrower of the crypto intangible assets can deploy those assets at its discretion for the duration of the lending arrangement and bears the risk of loss or theft of those assets and otherwise has the ability to direct the use of the assets transferred.

Upon derecognition of the lent crypto intangible asset, we understand the SEC staff would not object to a conclusion that the lender would recognize an asset that is reflective of its right to receive the crypto intangible assets from the borrower at the end of the loan period (herein referred to as a crypto intangible asset loan receivable).

The crypto intangible asset loan receivable would be measured at the fair value of the lent crypto intangible assets both initially and at subsequent reporting dates, assuming the lender is not otherwise required to apply specialized industry measurement guidance for the loan, such as that required by investment companies. Any difference between the carrying amount of the derecognized crypto intangible assets and the initial measurement of the crypto intangible asset loan receivable would be presented in the income statement as other gains and losses and not as revenue. Further, because the crypto intangible asset loan receivable exposes the lender to the credit risk of the borrower, the lender should recognize an allowance for expected credit losses that incorporates forecasts reflecting the lender's expectation of credit losses related to the crypto intangible asset loan receivable utilizing the principles in FASB ASC 326, *Financial Instruments – Credit Losses.*

The SEC staff would not object to the application of this model being applied as the adoption of a new accounting principle under FASB ASC 250, *Accounting Changes and Error Corrections.* Therefore, such change in accounting principle would be reflected on a retrospective basis for all periods presented unless impracticable to do so.

While not an all-inclusive list, as other disclosures may be applicable based on the facts and circumstances, the lender's financial statements should include disclosures regarding the terms, risks, and nature of the arrangements, including how management monitors its exposure to credit risk from these arrangements. If collateral is required, disclosures should include, but are not limited to, the type and amount of collateral held for crypto intangible asset loans; the terms of the collateral (including any requirement to pledge additional collateral during the term of the loan); and how management monitors its ability to liquidate the collateral and recover the crypto intangible assets in case of borrower default.

The financial statements should include relevant disclosures using the principles of FASB ASC 326 regarding factors used to develop expected credit loss at inception and on an ongoing basis including, but not limited to, quantitative and qualitative information about the credit risk characteristics of the borrowers and lending arrangements; changes in the allowance for expected credit losses, including current period provisions and write-offs and recoveries of previous write-offs; and crypto intangible asset loan receivables past due and how such status is determined.

Disclosures should also address, if applicable, vulnerability from concentrations disclosures using the principle of FASB ASC 275, *Risks and Uncertainties,* related party disclosures under FASB ASC 850, *Related Party Disclosures,* and fair value measurement disclosures required by FASB ASC 820, *Fair Value Measurement.*

We understand the SEC staff would not object to similar conclusions under IFRS, including application of the principles in IFRS 9, *Financial Instruments* regarding the allowance for credit losses.

Entities considering applying alternative models should consider consulting with their professional adviser or the SEC staff.

Crypto intangible asset borrowing

Question 26:

Assume identical facts to question 25. How should the borrower account for the loan?

Response 26:

Crypto intangible asset lending transactions can be complex, and the accounting for a particular transaction depends on the facts and circumstances. In this example, it is assumed that the borrower has obtained control because it has the right to transfer, encumber, or pledge the crypto intangible asset in any way it chooses. The borrower should recognize the units of Crypto Intangible Asset ABC received at fair value on its balance sheet at the date it obtains control of the crypto intangible asset. See Q&A 10 in AC chapter 1, "Classification, measurement, and recognition" for additional guidance on making the judgment about whether the borrower has obtained control of the units of Crypto Intangible Asset ABC.

If it is determined the borrower obtained control of the crypto intangible asset, the borrower also should record an offsetting obligation to return Crypto Intangible Asset ABC to the lender, which should be recognized at the fair value of Crypto Intangible Asset ABC on the date the borrower obtains control. Subsequently, the borrowed Crypto Intangible Asset ABC should be accounted for at fair value or at cost less impairment, depending on whether Crypto Intangible Asset ABC is an in-scope or out-of-scope crypto intangible asset, respectively. (See Q&A 1 in AC chapter 1 of this practice aid for additional guidance on the characteristics to determine an in-scope or out-of-scope crypto intangible asset) The obligation to return Crypto Intangible Asset ABC should be accounted for as a liability.

Pursuant to FASB ASC 815, *Derivatives and Hedging*, the obligation to return should be viewed as a hybrid instrument with a debt host contract and embedded derivatives linked to the fair value of Crypto Intangible Assets ABC loaned. Because the obligation is denominated in units of Crypto Intangible Asset ABC, the borrower will generally identify Crypto Intangible Asset ABC as indexed embedded features in the hybrid instrument that may need to be bifurcated and subsequently measured at fair value pursuant to the provisions of FASB ASC 815. This analysis of the obligation to deliver a fixed number of crypto intangible assets in satisfaction of the obligation is similar to the example in FASB ASC 815-10-55-76, in which an obligation to deliver shares in the future is viewed as a hybrid instrument with a debt host and embedded forward derivative feature.

The borrower identifies the host contract as a dollar-denominated debt obligation with a fixed interest rate following the principles in FASB ASC 815-15-25-24. Consistent with that judgment, the Crypto Intangible Asset ABC indexed elements of the obligation are viewed as embedded features with an initial fair value of zero pursuant to FASB ASC 815-15-30-4. Specifically, if the host contract is a fixed rate debt instrument, the embedded features represent pay crypto, receive dollar forward contract elements that should be evaluated for bifurcation. The bifurcation analysis under FASB ASC 815 depends on a number of factors, including whether the embedded feature can be net settled. In contracts that require gross settlement, the net settlement criterion may be met, for instance, if delivery of Crypto Intangible Asset ABC would be readily convertible to cash under that standard (refer to Q&A 24 for details). If the forward embedded features are required to be bifurcated, the features would be remeasured to fair value through net income each period as a derivative in accordance with FASB ASC 815-10.

When the related asset is not otherwise measured at fair value (for example, borrower's holding of Crypto Intangible Asset ABC is an out-of-scope crypto intangible asset), the bifurcated embedded feature (crypto ABC derivative) related to the liability may be considered a hedging instrument in a fair value hedging relationship of the Crypto Intangible Asset ABC if designated, documented, and found to qualify for hedge accounting under the provisions of FASB ASC 815.

AC Chapter 8: Mining

Transaction fees and block rewards

Question 27:

If an entity operates as a miner, how should the entity recognize, and measure, transaction fees and block rewards earned in connection with its mining efforts?

For purposes of this Q&A, assume the following:

- The miner does not apply any specialized industry accounting (for example, FASB ASC 946, *Financial Services — Investment Companies*).
- The digital assets earned as transaction fees and block rewards are crypto intangible assets.

Blockchain networks that use Proof-of-Work protocols rely on miners that compete to validate and add blocks of transactions to the distributed ledger. To incentivize these miners to compete in processing the transactions for the next block, the winning miner is entitled to transaction fees, a block reward, or both. Transaction fees are specified in each transaction request and are paid by the participant who requested the transaction (the requester) in the native crypto intangible asset of the blockchain (for example, bitcoin). Block rewards are newly created crypto intangible asset units granted to the winning miner by the network under the blockchain's consensus protocol.

Response 27:

Transaction fees

Transaction fees earned by a miner should be recognized as revenue from customers in accordance with FASB ASC 606, *Revenues from Contracts with Customers*.

The transaction fees are specified in each transaction request and paid by the requester to the successful miner in exchange for the successful processing of the transaction. The requester meets the definition of a *customer* in FASB ASC 606 because it has contracted with the miner to obtain a service (successful mining) that is an output of the miner's ordinary activities in exchange for consideration.

A contract with a customer exists at the point when the miner successfully validates a requesting customer's transaction to the distributed ledger. At this point, the performance obligation has been satisfied in accordance with FASB ASC 606-10-25-30. Because of this, the additional criteria in FASB ASC 606-10-25-1 would be met as follows:

- Both the requester (a customer) and the miner have approved the contract and are committed to the transaction at the point of successfully validating and adding the transaction to the distributed ledger.
- Each party's rights, the consideration to be transferred, and the payment terms are clear.
- The transaction has commercial substance (that is, the risk, timing, or amount of the miner's future cash flows is expected to change as a result of the contract).
- Collection of the fees is probable because it is completed as part of closing a successful block.

By successfully mining a block, the miner satisfies its performance obligation to the requester and, thus, should recognize revenue at that point in time.

The payment of transaction fees in crypto intangible assets constitutes noncash consideration under FASB ASC 606-10-32-21. This noncash consideration is measured at its estimated fair value at contract inception — that is, the date that the criteria in FASB ASC 606-10-25-1 are met. If fair value cannot be reasonably estimated in accordance with FASB ASC 606-10-32-22, the consideration should be measured indirectly by reference to the stand-alone selling price of the miner's services.

Miners should disclose, if not presented separately in the statement of comprehensive income (statement of activities), transaction fees as *revenue recognized from contracts with customers* in accordance with FASB ASC 606-10-50-4.

Block rewards

Block rewards earned by a miner are generally recognized as revenue, but an evaluation is required to determine if the block rewards earned should be recognized as revenue from contracts with customers under FASB ASC 606 or as other revenue.

Entity A should first evaluate whether its mining activities represent a contract with a customer to provide services and, if so, whether it should recognize block rewards it receives from the network as revenue from a customer under FASB ASC 606. All relevant facts and circumstances, including the network's protocols, should be considered in determining (1) whether Entity A has a contract with a customer under FASB ASC 606-10-25-2 and (2) whether its mining activities on the network meet all the criteria in FASB ASC 606-10-25-1.

If the miner concludes that the block rewards aren't revenue from contracts with customers under FASB ASC 606, it should consider other relevant guidance.

The inflow of crypto intangible assets as a result of the block reward would meet the definition of *revenue* in the concepts statements because it gives rise to economic benefits to the miner from rendering services or carrying out activities. Therefore, miners may account for the block reward as revenue. Because there is no specific guidance that applies to revenues from block rewards, a miner could apply by analogy the revenue recognition guidance in FASB ASC 606 to recognize and measure the revenue from block rewards.

If analogizing to FASB ASC 606, the revenue from block rewards would be presented separately from FASB ASC 606 revenues from contracts with customers on the statement of comprehensive income or separately disclosed in the notes to the financial statements. This is because FASB ASC 606-10-50-4(a) requires an entity to disclose, unless separately presented in the statement of comprehensive income, the amount of revenue recognized from contracts with customers under FASB ASC 606 separately from other sources of revenue.

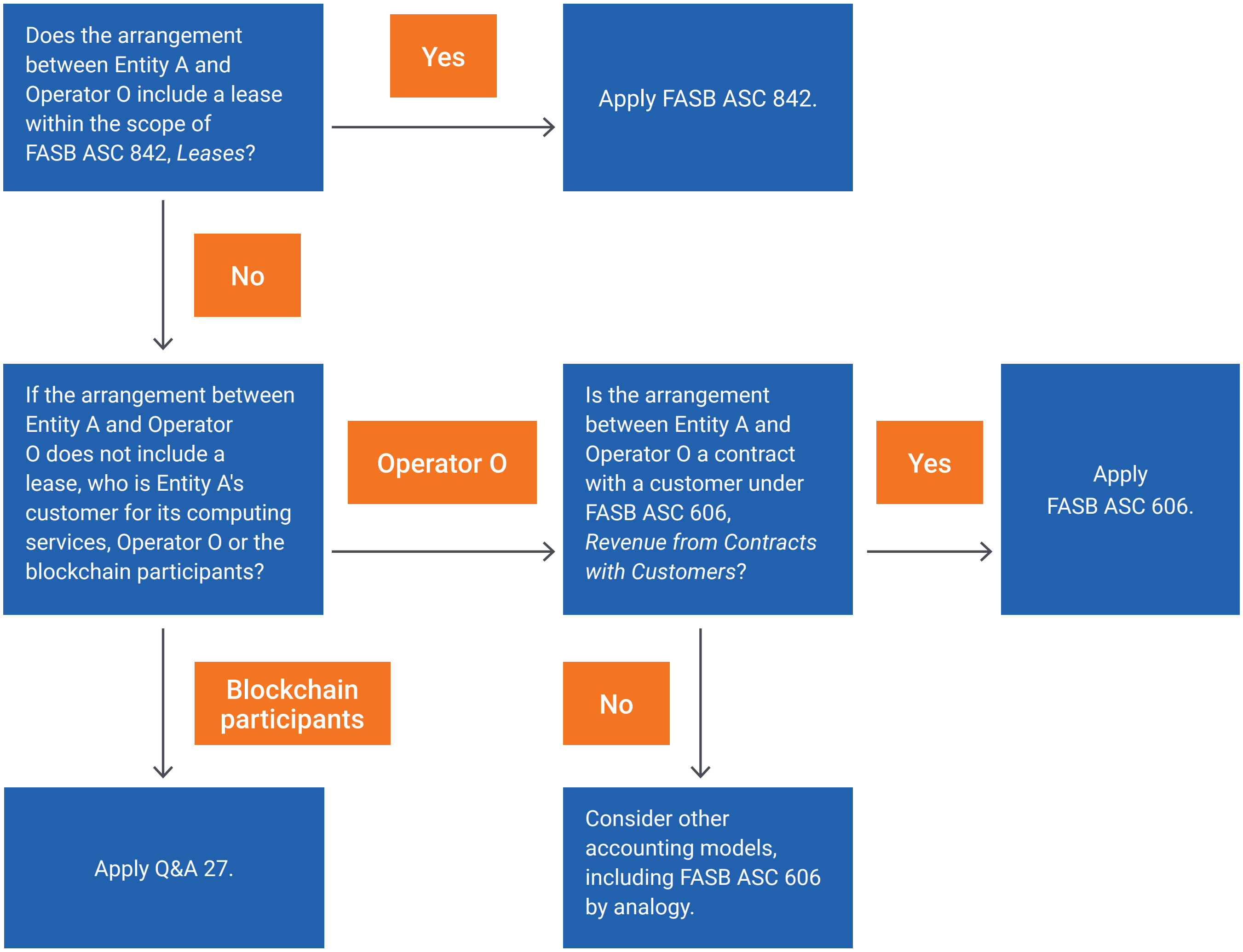
Mining pools

Question 28:

Entity A shares its computing infrastructure as part of a mining pool run by Operator O. The computing infrastructure from participants (including Entity A) is used for the mining activities of the pool. Each participant operates their own computing infrastructure. The block rewards received from the network upon successfully mining a block are collected by Operator O and then transferred to the mining pool participants in accordance with an agreed-upon formula.

How does Entity A account for the arrangement?

Response 28:



Does the arrangement between Entity A and Operator O include a lease within the scope of FASB ASC 842, *Leases*?

Yes

Apply FASB ASC 842.

No

If the arrangement between Entity A and Operator O does not include a lease, who is Entity A's customer for its computing services, Operator O or the blockchain participants?

Operator O

Is the arrangement between Entity A and Operator O a contract with a customer under FASB ASC 606, *Revenue from Contracts with Customers*?

Yes

Apply FASB ASC 606.

Blockchain participants

Apply Q&A 27.

No

Consider other accounting models, including FASB ASC 606 by analogy.

Entity A should apply the following steps to determine the appropriate accounting for its arrangement with Operator O.

- **Step 1: Does the arrangement between Entity A and Operator O include a lease within the scope of FASB ASC 842, *Leases*?**

  The guidance in FASB ASC 842 applies to contracts that convey the right to control the use of identified property, plant, and equipment for a period of time in exchange for consideration. For a lease to exist under FASB ASC 842, a customer should have both the right to obtain substantially all the economic benefits from using an identified asset and the right to direct its use. This determination should be based on all the facts and circumstances, including the terms and conditions of the contract. If Operator O can dictate when Entity A makes use of its computing infrastructure assets, this may indicate that Entity A is leasing those assets to Operator O.

  If the arrangement between Entity A and Operator O includes a lease, Entity A should apply the lessor accounting guidance in FASB ASC 842. Entity A should also consider whether it is providing a nonlease component service to Operator O of operating and maintaining the computing infrastructure assets.

  If Operator O is leasing Entity A's computing infrastructure, Entity A's customer for that lease and any operations and maintenance services will generally be Operator O. This means that, in general, Operator O is the principal to the mining activities undertaken using Entity A's computing infrastructure.

- **Step 2: If the arrangement does not include a lease, the next step is for Entity A to assess for which party it is providing computing services. Depending on the facts and circumstances, Entity A may be providing those services either for Operator O or the blockchain participants.**

  To make this determination, it would typically be appropriate for Entity A to consider whether it or Operator O is the principal for the mining activities performed on the blockchain, using the principal versus agent guidance in FASB ASC 606, *Revenues from Contracts with Customers.* If Entity A is the principal for providing mining services to the blockchain participants, Operator O is an agent arranging for Entity A to provide those services. If, instead, Operator O is the principal performing the mining activities on the blockchain, Entity A is providing computing services to Operator O, assisting Operator O with its provision of mining services to the blockchain participants.

  Determining the principal for performing the mining service may involve judgment. An entity should consider all the relevant guidance in FASB ASC 606 on principal versus agent considerations when making this determination.

  Some questions that may be relevant to applying that guidance in the context of mining pool arrangements include the following:

  - Does Operator O direct (that is, assign) to the mining pool participants (including Entity A) the mining activities they undertake as part of the pool?
  - Is Entity A or Operator O primarily responsible for selecting the transactions to be mined, the activities to be performed, placing the mined block on the blockchain, and collecting the block reward?
  - Does Entity A bear the risks and rewards associated with the mining activities? For example, is Entity A compensated on a fixed basis per unit of computing power delivered or, instead, allocated a percentage only of the actual rewards earned based on the results of the mining activities?

  If Entity A concludes that it is engaging in mining activities directly on the blockchain, rather than providing computing services to Operator O, the mining pool arrangement may represent a sharing of transaction fees and block reward between pool participants that is some form of joint arrangement under FASB ASC 808, *Collaborative Arrangements.* In that case, Entity A should apply Q&A 27 to account for its share of the transaction fees and block reward.

- **Step 3: Once Entity A determines to which party it is providing computing services, it should consider if those services are being provided pursuant to a contract with a customer under FASB ASC 606.**

  Refer to Q&A 27 if Entity A concludes it is providing computing services to the blockchain participants, that is, engaging in mining activities directly on the blockchain.

  If Entity A concludes it is providing computing services to Operator O, Entity A should evaluate whether its mining pool arrangement with Operator O is a contract with a customer. This evaluation should consider the definitions of both *contract* and *customer* in FASB ASC 606 as well as the following questions:

  - Do the terms and conditions of the mining pool arrangement create enforceable rights and obligations for Operator O and Entity A as described in FASB ASC 606-10-25-2?
  - Does the arrangement meet all the criteria in FASB ASC 606-10-25-1?
  - Is providing computing services of this nature an output of Entity A's ordinary activities pursuant to FASB ASC 606-10-15-3?

  If Entity A's computing services to Operator O are provided pursuant to a contract with a customer, Entity A should apply the guidance in FASB ASC 606 to recognize revenue from that contract.

  If Entity A determines that its computing services are not being provided pursuant to a contract with a customer, they are outside the scope of FASB ASC 606. Entity A should determine the appropriate accounting and presentation model to apply, including whether it is appropriate to apply FASB ASC 606 by analogy.

Auditing Subgroup

Part I: Overview

Part I of this practice aid addresses, in narrative format, the relevant professional standards, unique challenges to engagements in the digital asset ecosystem, and practical recommendations auditors may apply to address those challenges and requirements. In addition, Part I provides an overview of related processes and controls unique to the digital asset ecosystem and identifies some risk assessment considerations that auditors may need to take into account as part of their audits.

Part I includes the following chapters:

Note:

Independence and ethics — The topics in this section of the practice aid focus on auditing applications and do not address ethics considerations, including those related to independence. It is important to note, however, that these considerations remain critical to an auditor's performance of the engagement in conformity with professional standards, and engagements in the digital asset ecosystem may introduce new or different compliance risks warranting additional consideration by the auditor.

For information regarding independence requirements and ethics responsibilities, see the AICPA Code of Professional Conduct at pub.aicpa.org/codeofconduct/Ethics.aspx.

In addition, see paragraph .07, "Operating Node Software on a Blockchain," in Q&A section 100, *Independence,* at the following link:

pub.aicpa.org/codeofconduct/resourceseamlesslogin.aspx?prod=ethics&tdoc=et-qa&tptr=et-qa100

Risk of material misstatement due to fraud — For entities in the digital asset ecosystem, the Q&As herein do not contemplate all potential risks of material misstatement, including all potential fraud risks. AU-C section 240, *Consideration of Fraud in a Financial Statement Audit*, includes further requirements regarding procedures to identify and respond to fraud risks.

Risks of material misstatement due to fraud may be present, and the auditor should identify and assess such risks at the financial statement level and at the assertion level for classes of transactions, account balances, and disclosures.[1,2] See AU chapter 2 of this practice aid for factors to consider when identifying and assessing risks of material misstatement, including those risks that may be significant risks due to error or fraud.

[1] Paragraph .26 of AU-C section 315, *Understanding the Entity and Its Environment and Assessing the Risks of Material Misstatement.*

[2] Paragraph .25 of AU-C section 240, *Consideration of Fraud in a Financial Statement Audit.*

AU Chapter 1: Client acceptance and continuance

1. Introduction

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 is 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 considerations, including those related to independence; it is important to note, however, that these considerations remain critical to an auditor's performance of the engagement in conformity with 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:

- QM section 10A, *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*
- If the audit is of group financial statements, AU-C section 600A, *Special Considerations – Audits of Group Financial Statements (Including the Work of Component Auditors)*
- AU-C section 220A, *Quality Control for an Engagement Conducted in Accordance With Generally Accepted Auditing Standards*[1]

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

The topics covered in this chapter of the practice aid are divided as follows:

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.

Note: For engagements involving digital assets, there may be a potential for an increase in instances of scope limitations given the potential for challenges in obtaining sufficient appropriate audit evidence.

2. Auditor skill sets and competencies

Relevant professional standards

QM section 10A and AU-C section 220A 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.[2]

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"]

[2] See paragraphs .27a and .A11 of QM section 10A and paragraphs .14 and .A7 of AU-C section 220A.

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 QM section 10A 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 QM section 10A 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 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 QM section 10A, 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
- Updating 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 QM section 10A, 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 entities 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[3] 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 whether the auditor's specialists have the necessary competence, capabilities, and objectivity for the auditor's purposes (paragraph .09 of AU-C section 620, *Using the Work of an Auditor's Specialist*).

[3] 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.*

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 QM section 10A).
- 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 QM section 10A).
- Establish consultation requirements for unique auditing or financial reporting issues that may be relevant in the digital asset ecosystem (paragraph .37 of QM section 10A).
- 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 QM section 10A).
- 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 QM section 10A).

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

Pursuant to paragraph .06b of AU-C section 210, to establish whether the preconditions for an audit are present, the auditor should obtain the agreement of management that it acknowledges and understands its responsibility

a. for the preparation and fair presentation of the financial statements in accordance with the applicable financial reporting framework;

b. for 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. to provide the auditor with

   i. access to all information of which management is aware that is relevant to the preparation and fair presentation of the financial statements, such as records, documentation, and other matters;

   ii. additional information that the auditor may request from management for the purpose of the audit; and

   iii. unrestricted access to persons within the entity from whom the auditor determines it 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 the levels of those jobs translate into requisite skills and knowledge. This also may include consideration of 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[4] 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.

[4] 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.

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.
- 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 assets. (See AC chapter 1, "Classification, measurement, and recognition," 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 .27c of QM section 10A, the 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 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.

According to paragraph .A12 of QM section 10A, 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

The extent of knowledge that a firm will have regarding the integrity of a client will generally grow within the context of an ongoing relationship with that client

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 .19*a*(i) of AU-C section 315 requires the auditor to obtain an understanding of the entity's organizational structure, ownership and governance, and its business model. Understanding the entity’s objectives, strategy, and business model helps the auditor to understand the entity at a strategic level and to understand the business risks the entity takes and faces.[5] Paragraph .21 of AU-C section 315 further requires the auditor, through performing risk assessment procedures, to obtain an understanding of the control environment relevant to the preparation of the financial statements. As the auditor obtains this understanding, the auditor should obtain an understanding of the set of controls, processes, and structures that address the following:

- How management’s oversight responsibilities are carried out, such as the entity’s culture and management’s commitment to integrity and ethical values
- When those charged with governance are separate from management, the independence of and oversight over the entity’s system of internal control by those charged with governance
- The entity’s assignment of authority and responsibility
- How the entity attracts, develops, and retains competent individuals
- How the entity holds individuals accountable for their responsibilities in the pursuit of the objectives of the system of internal control

[5] Paragraph .A70 of AU-C section 315, *Understanding the Entity and Its Environment and Assessing the Risks of Material Misstatement.*

Based on the auditor's understanding of the control environment, the auditor should evaluate whether

- management, with the oversight of those charged with governance, has created and maintained a culture of honesty and ethical behavior;
- the control environment provides an appropriate foundation for the other components of the entity's system of internal control considering the nature and complexity of the entity; and
- control deficiencies identified in the control environment undermine the other components of the entity's system of internal control.

[Paragraph .21*b* of AU-C section 315]

The auditor's evaluation of how the entity demonstrates behavior consistent with the entity's commitment to integrity and ethical values; whether the control environment provides an appropriate foundation for the other components of the entity's system of internal control; and whether identified control deficiencies undermine the other components of the system of internal control assists the auditor in identifying potential control deficiencies in the other components of the system of internal control. [Paragraph .A118 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 assets, and validators) may present unique considerations.

When a predecessor auditor exists, the auditor should request management to authorize the predecessor auditor to respond fully to the auditor's inquiries regarding matters that will assist the auditor in determining whether to accept the engagement. If management authorizes the predecessor auditor to respond to the auditor's inquiries, the auditor should inquire of the predecessor auditor about matters that will assist the auditor in determining whether to accept the engagement, in accordance with paragraph .12 of AU-C section 210. If management refuses to authorize the predecessor auditor to respond, or limits the response, the auditor should inquire about the reasons and consider the implications of that refusal or limitation in deciding whether to accept the engagement.

In addition, 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 client acceptance procedures by including some or all 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 know-your-customer (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 management to understand whether management uses third parties (for example, custodians or exchanges) and whether an appropriate SOC report is available. If the services provided by a service organization (and subservice organizations, 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 entities 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 entities 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,[6] 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.

[6] 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

Pursuant to paragraph .05 of AU-C section 200, *Overall Objectives of the Independent Auditor and the Conduct of an Audit in Accordance With Generally Accepted Auditing Standards,* an audit in accordance with GAAS is conducted on the premise that management and, when appropriate, those charged with governance, have acknowledged certain responsibilities that are fundamental to the conduct of an audit. Pursuant to paragraph .06 of AU-C section 210, in order to establish whether the preconditions for an audit are present, the auditor should, among other things, obtain the agreement of management that it acknowledges and understands its responsibility for the preparation and fair presentation of the financial statements in accordance with the applicable financial reporting framework, and for 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. 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.

Note: Paragraph .A25 of AU-C section 330, *Performing Audit Procedures in Response to Assessed Risks and Evaluating the Audit Evidence Obtained*, states that the auditor may find it impossible to design effective substantive procedures that, by themselves, provide sufficient appropriate audit evidence at the relevant assertion level. This may occur when an entity conducts its business using IT, and no documentation of transactions is produced or maintained, other than through the IT system. In such cases, paragraph .08*b* of AU-C section 330 requires the auditor to perform tests of controls that address the risk for which substantive procedures alone cannot provide sufficient appropriate audit evidence.

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 asset 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, information to be used as 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.

Pursuant to paragraphs .27–.28 of AU-C section 315, the auditor should identify controls that address risks of material misstatement at the relevant assertion level, and then, based on those controls identified, the auditor should identify the IT applications and other aspects of the entity's IT environment that are subject to risks arising from IT. Consequently, more detailed inquiries or a 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 asset 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 asset 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 asset 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 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 automated processes. The volume of transactions 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 general IT 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 entities 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 public 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 its own digital assets or holds assets on behalf of others, 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 rights and obligations assertion of the digital assets. In some instances, management may assert that the entity's ability to sign messages demonstrates the entity's control of those digital assets and, therefore, can provide information to be used as audit evidence of the rights and obligations assertion. In certain instances, operational limitations may prohibit the entity from signing messages using the entity's private keys, which further reduces available substantive evidence to support the rights and obligations assertion. Although control of a digital asset is one consideration in the evaluation of the rights and obligations 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 rights and obligations assertion.

If an entity holds digital assets on behalf of others, the auditor may need to consider how the entity will demonstrate its fulfillment of its obligation to safeguard assets and the presence of any potential loss events. In such circumstances, the auditor may determine that substantive procedures alone are not adequate to provide sufficient audit evidence to address risks of material misstatements identified.

Digital assets held by a third-party custodian

If an entity relies on a third-party custodian to store digital assets, including assets held on behalf of others, 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 when 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 general IT controls, application controls, and the 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. 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 service organizations (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 mechanism, 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 multi-signature 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).

AU Chapter 2: Risk assessment and processes and controls

1. Introduction

A. Overview

As previously stated in AU chapter 1, "Client Acceptance and Continuance," the digital asset ecosystem is constantly evolving, which presents unique risks and challenges. It is especially important for the auditor to understand these unique risks and challenges when performing procedures in response to the requirements to identify and assess the risks of material misstatements, whether due to fraud or error.

This section of the practice aid is organized into the following topics:

2. Understanding the Entity and Its Environment

3. Understanding and Evaluating the Entity's Risk Assessment Process

4. Understanding the Entity's Processes and Controls

5. Identify and Assess Risks of Material Misstatement and Design Further Audit Procedures

Each of these sections describes the unique considerations that may be important when performing risk assessment procedures, including the types of procedures that auditors may perform, or are required to perform, to identify and assess risks of material misstatement in audits of entities engaged in the digital asset ecosystem.[1]

B. Relevant professional standards

AU-C section 315, *Understanding the Entity and Its Environment and Assessing the Risks of Material Misstatement,* as well as AU-C section 240, *Consideration of Fraud in a Financial Statement Audit,* are relevant to the discussion in this chapter. The following provides details of some paragraphs of these standards that are especially relevant.

Paragraph .11 of AU-C section 315, states that the objective of the auditor is to identify and assess the risks of material misstatement, whether due to fraud or error, at the financial statement and assertion levels, thereby providing a basis for designing and implementing responses to the assessed risks of material misstatement.

Paragraph .14 of AU-C section 315 states that risk assessment procedures should include the following:

a. Inquiries of management and of other appropriate individuals within the entity, including individuals within the internal audit function (if the function exists);

b. Analytical procedures; and

c. Observation and inspection.

During the client acceptance and continuance process, the auditor gains some understanding of the entity and its environment. In obtaining audit evidence with respect to risk assessment procedures, paragraph .15a of AU-C section 315 states that the auditor should consider information from the auditor's procedures regarding acceptance or continuance of the client relationship or the audit engagement, and when applicable other engagements performed by the engagement partner.

[1] Note that this section of the practice aid specifically excludes engagements related to decentralized finance.

In addition, in accordance with paragraph .36 of AU-C section 315, the auditor should determine whether any of the assessed risks of material misstatement are significant risks.

AU-C section 240 includes further requirements regarding procedures to identify and respond to fraud risks. Paragraph .12 of AU-C section 240 states that the auditor should maintain professional skepticism throughout the audit, recognizing the possibility that a material misstatement due to fraud could exist, notwithstanding the auditor's past experience of the honesty and integrity of the entity's management and those charged with governance. Pursuant to paragraph .15 of AU-C section 240, the required discussion among the key engagement team members should include an exchange of ideas or brainstorming among the engagement team members about how and where the entity's financial statements might be susceptible to material misstatement due to fraud, how management could perpetrate and conceal fraudulent financial reporting, and how assets of the entity could be misappropriated. Paragraph .27 of AU-C section 240 states that the auditor should treat the assessed risks of material misstatement due to fraud as significant risks and, accordingly, to the extent not already done so, the auditor should identify the entity's controls that address such risks, and evaluate their design and determine whether they have been implemented.

2. Understanding the entity and its environment

Auditors are required to gather information about a wide range of matters to enable them to understand the entities they audit. Some of these matters relate directly to the financial reporting process, whereas others relate to the broader business issues, such as the current status of the industry in which the entity operates as well as the entity's business objectives and strategies.

The facts and circumstances of each entity differ depending on the nature of their activities in the digital asset ecosystem. When obtaining an understanding the entity and its environment, the auditor gathers information that pertains to the entity's strategy, operations, internal controls and its role in the digital asset ecosystem, among other things. The level of effort necessary to obtain a sufficient understanding of the entity and its environment and the auditor's risk assessment procedures will likely vary based on the entity's business purpose, the entity's role in the digital asset ecosystem, management's competencies and skill set, and the involvement of service organizations, among other things. (See AU chapter 1 of this practice aid for additional information on factors an auditor may need to consider when assessing the competencies and capabilities of management.)

The following table provides examples of questions the auditor may consider inquiring of management, those charged with governance, or others within the entity who may have information that is likely to assist in identifying risks of material misstatement due to fraud or error as part of the risk assessment process to gain an understanding of the entity and its environment. The list is not intended to be all-inclusive, and the example questions should only be viewed as a starting point. Additional follow-up inquiries will likely be needed depending on the entity's facts and circumstances. In addition, the auditor may have obtained a preliminary understanding of some of these topics as part of the client acceptance and continuance process. In those cases, the auditor enhances the understanding obtained during client acceptance and continuance throughout the risk assessment process.

General — Nature of the entity	
1	What is the entity’s business purpose related to current and future anticipated holding or transacting in digital assets, and what is the entity’s role in the digital asset ecosystem?
Digital assets held and custody considerations	
2	What types of digital assets does the entity hold? How did the entity acquire these digital assets? What are the entity’s controls around safeguarding of assets, including the protection of private keys?
3a	How does the entity maintain custody of its digital assets? Does it use a third party (for example, to secure private keys)?
3b	If a third party is used to maintain custody of digital assets • are the digital assets stored in segregated or commingled wallets? • does the service organization have adequate controls in place, how is management assessing the controls in place, and will the auditor be able to obtain sufficient evidence of the effectiveness of relevant controls either by performing direct testing of third-party controls or by obtaining a service auditor's report? • does management have complementary user entity controls? • what type of analysis has the entity performed to determine whether the entity or the third party is the owner of the digital assets? • does the custodian have the right to sell, transfer, loan, encumber, or pledge the digital assets for its purposes without the depositor’s consent or notice, or both?
4a	Does the entity hold digital assets on behalf of others (for example, customers) or only on the entity’s behalf? If digital assets are held on behalf of others, how does the entity safeguard such assets (for example, self-custody or use of a third party)?
4b	What are the entity’s policies and controls for determining which entity (the depositor or the custodian) has control of the digital asset based on the specific facts and circumstances of the agreement between the depositor and custodian and applicable laws and regulations? Does the entity have a process in place to perform appropriate legal analysis to evaluate the aspects of the agreement between the depositor and custodian, including legal ownership?
4c	If digital assets are held on behalf of others, how does the entity track customer assets separately from the entity’s assets?
5	What is the entity’s policy for claiming, recording, and valuing forked digital assets and air-dropped digital assets received by the entity? If the entity has unclaimed or unrecorded digital assets, or both, how does the entity evaluate the potential effect on the financial statements?
6	Does the entity hold digital assets that are illiquid or thinly traded? If so, what are the entity’s policies to determine whether these assets are illiquid or thinly traded and the policies for accounting for such assets? How does the entity value these digital assets, and what are the sources that the entity uses to measure and determine the value? What are the entity’s accounting policies for recording these digital assets?

7 What types of wallets does the entity (or the third party that holds the entity’s digital assets) use to store the digital assets? For example, a hot wallet that is connected to the internet, cold storage that is offline, single signature vs. multi-signature wallets? What are the controls that management has in place for wallet management, access, and other wallet control-related attributes? What is the entity’s process for a key generation?

8 Does the entity have controls and policies in place at the entity and any entities holding assets on its behalf to evaluate whether the appropriate insurance coverage exists to cover potential digital asset losses? If so, do these policies cover the entirety of the digital assets held or only a portion? What types of losses are covered by the policies, and what evidence exists to prove ownership?

Digital assets transactions

9 What is the nature, frequency, types, volume, and value of the entity’s digital asset transactions?

- What types of counterparties (for example, exchanges, custodians, validators) are involved with the entity’s digital asset transactions?
- Does the entity exchange digital assets for cash, other digital assets or other goods and services (for example, to pay vendors, employees, contractors)?

10 Are digital asset transactions recorded on the blockchain? What is the entity’s method of maintaining its books and records and reconciling it to the external blockchain to support its books and records? If there are off-chain transactions, how are they managed, recorded and reconciled?

11 Does the entity engage in digital asset-based derivatives, or has it made investments in digital assets or other entities, or ventures related to digital assets? If so,

- are there aspects of the entity’s operations that might present risks that are hedged using derivatives?
- are there any anticipated changes to the entity’s investment activities? If so, how will the changes affect its financial reporting processes?
- what are the entity’s due diligence policies on reviewing investments in new digital assets, including evaluating the integrity of the underlying blockchains and the software used to interact with the blockchains?

12 What process has management put in place to evaluate the reliability of the information obtained from underlying blockchains where digital assets and digital asset transactions are recorded? (Refer to Q&A 1: “Evaluating the reliability of information obtained from a blockchain” in chapter 5, “Existence, rights, and obligations,” for factors that may be relevant to consider when evaluating the reliability of a blockchain.)

Industry, regulatory, and other external factors

13 Are there any legal, regulatory, tax, or reporting requirements that apply to the entity given its involvement with digital assets? How does the entity comply with the requirements, and have there been any instances of noncompliance (for example, with money transmitter licenses) or communications with regulators (for example, SEC inquiries, Office of Foreign Assets Control [OFAC] sanctions, and so on) about the entity’s digital asset activities?

14 What are the entity’s policies for complying with applicable regulations such as the following:

- International regulations if the entity has foreign operations;
- Know your customer (KYC); and
- Anti-money laundering (AML) requirements to prevent criminal activity.

15 What are the entity’s views related to the potential market risks affecting valuation of the digital asset (for example, considerations such as volatility and level of maturity of the entity’s digital asset market)?

16 If the entity transacts or is otherwise involved in effecting transactions in digital asset securities for customers or its own account, has the entity complied with applicable registration requirements? If so, what are the entity’s policies to comply with the appropriate regulatory requirements?

17 What potential financial statement risks related to unexpected technology has the entity considered that may affect its operations or those of its clients, vendors, or other partners?

Financing

18 How does the entity finance its activities, and what are its plans for raising funds (for example, working capital loans, crowdfunding, token sale, security offerings, equity)?

Financial reporting

19 What are the entity’s significant accounting policies for its digital assets and/or digital assets held on behalf of others? Refer to the “Accounting Subgroup” section of this practice aid for examples of accounting considerations.

In addition to inquiries, the auditor’s risk assessment procedures should include analytical procedures as well as observation and inspection. In accordance with paragraph .A34 of AU-C section 315, analytical procedures performed as risk assessment procedures may assist in identifying and assessing the risks of material misstatement by identifying aspects of the entity of which the auditor was unaware or understanding how inherent risk factors, such as change, affect susceptibility of assertions to misstatements. For example, the auditor may consider using information obtained from a blockchain to perform analytics related to transaction volumes to identify unusual transactions. (See AU chapter 3, "Laws and regulations and related parties," of this practice aid for other procedures the auditor may perform to identify unusual transactions.) In accordance with paragraph .22 of AU-C section 240, based on analytical procedures performed as part of risk assessment procedures, the auditor should evaluate whether unusual or unexpected relationships that have been identified indicate risks of material misstatement due to fraud. To the extent not already included, the analytical procedures, and evaluation thereof, should include procedures relating to revenue accounts.

Paragraph .A38 of AU-C section 315 states that observation and inspection may support, corroborate, or contradict inquiries of management and others and may also provide information about the entity and its environment.

3. Understanding and evaluating the entity's risk assessment process

The digital asset ecosystem presents challenges that may threaten an entity's ability to achieve its objectives of maintaining reliable financial reporting, effective and efficient operations, and compliance with applicable laws and regulations. Paragraphs .22–.23 of AU-C section 315 address the auditor's responsibility, through performing risk assessment procedures, to obtain an understanding of the entity's risk assessment process. In particular, the auditor is required to, among other things, obtain an understanding of the entity's process for identifying business risks, including the potential for fraud, relevant to financial reporting objectives, and evaluating whether the entity's risk assessment process is appropriate to the entity's circumstances considering the nature and complexity of the entity. Paragraph .17 of AU-C section 240 also requires the auditor to make inquiries of management, among other things, regarding management's process for identifying, responding to, and monitoring the risks of fraud in the entity.

The auditor may look to applicable internal control frameworks, such as the *Internal Control — Integrated Framework (2013)* published by the Committee of Sponsoring Organizations of the Treadway Commission (COSO), to understand and evaluate the entity's risk assessment process.

The auditor may consider performing the following in understanding and evaluating the entity's risk assessment process:

- Review management's governing documents to understand policies, procedures, and other information relevant to digital assets (for example, valuation policies, processes for onboarding new digital assets, evaluating the reliability of information obtained from relevant blockchains and performing due diligence over exchanges, custodians, or other service organizations).
- Inquire of management or those charged with governance about the entity's risk assessment process for identifying objectives and risks related to digital assets, including the process for identifying, assessing, and mitigating those risks.
- Evaluate whether the entity's risk assessment process enables the entity to identify new risks in a timely manner related to, for example, changes in applicable laws and regulations that affect compliance, changes in GAAP that affect accounting policies, and changes in blockchain-related technology that affect the safeguarding of digital assets.
- Evaluate how the entity assesses risks related to changes in management or key personnel, including consideration of appropriate skill sets and competencies to fulfill their responsibilities related to, for example, safeguarding of digital assets, establishing digital asset accounting policies that are appropriate under existing GAAP, providing oversight of service organizations, and understanding the applicable regulatory environment and changes in laws and regulations.
- Inquiring of management or those charged with governance about identified business risks, and along with the unique financial reporting risks related to digital assets, including those related to the identification of transactions with related parties, the existence of digital assets, and the rights to digital assets. (See AU chapter 3 of this practice aid.)
- If the auditor identifies risks of material misstatement that management failed to identify, paragraph .23 of AU-C section 315 requires the auditor to determine whether any such risks are of a kind that the auditor expects would have been identified by the entity's risk assessment process and, if so, obtain an understanding of why the entity's risk assessment process failed to identify such risks of material misstatement. Additionally, the auditor would be required to consider the implications on the auditor's evaluation whether the entity's risk assessment process is appropriate to the entity's circumstances considering the nature and complexity of the entity.

In addition, because many entities in the digital asset ecosystem are emerging entities, a formal risk assessment may not have been performed by management. In accordance with paragraph .A23 of AU-C section 315, some entities may not have established structured processes and systems (for example, a risk assessment process) or may have established processes or systems with limited documentation. When such systems and processes lack formality, the auditor may still be able to perform risk assessment procedures through observation and inquiry.

4. Understanding the entity's processes and controls

The characteristics, complexity, and evolving nature of digital assets and the underlying technologies create the need for tailored processes and controls that are important for the auditor to consider when identifying and assessing the risks of material misstatement, whether due to fraud or error. As previously stated in AU chapter 1, a client acceptance and continuance determination includes an assessment of any gaps in the skill sets of the firm's personnel and whether the firm can satisfactorily address those gaps. For example, some of the concepts discussed in this section are highly technical in nature and may require specialized skills that are not found in the common IT audit practitioner.

This section does not include specific auditor responses; however, substantive procedures alone may not provide sufficient appropriate audit evidence (for example, ownership of digital assets). When this is the case, the auditor is required to evaluate the design, determine implementation, and test operating effectiveness of an entity's relevant controls over digital assets.

This section provides an overview of the following concepts, and the related processes and controls unique to the digital asset ecosystem, and identifies some risk assessment considerations, including potential fraud risks, that auditors may need to take into account as part of their audits:

A. **Digital asset safeguarding**

B. **Transacting in digital assets**

C. **Digital asset transaction monitoring and reporting**

D. **Digital asset valuation**

E. **Digital assets held by third parties**

F. **Digital assets held on behalf of others**

A. Digital asset safeguarding

1. Overview of concepts, processes, and controls

One of the essential elements of asserting ownership of digital assets is demonstrating control of the digital assets (for example, through access to the private key associated with the public address where the digital assets reside). Developing processes and controls that mitigate the risk of inappropriate access to this private key also presents challenges.

The concepts, processes, and controls relating to digital asset safeguarding are most relevant to the existence and rights, and obligations assertions. Given the extensive efforts entities often take to safeguard private keys, challenges may arise in evaluating whether the storage environment is properly controlled. Methods of safeguarding private keys may include the following:

- Security procedures surrounding the key generation;
- Physical security of the facilities and infrastructure storing the private keys;
- Encryption or splitting (also known as *sharding*) of private keys; and
- Multi-signature addresses.

Key generation

Many digital asset blockchains, including the largest blockchains such as Bitcoin and Ethereum, consist of public addresses analogous to bank account numbers. The public and private keys needed to access digital assets in the public address, referred to as *key pairs,* are generated using cryptographic algorithms beginning with a “seed” phrase, which may be generated randomly or by other means. The underlying cryptographic technology makes it virtually impossible (with currently available computing power) to determine the private key using the public key or public address. Possession of the private key, or the “seed” inputs to the generation of the private key, is required to access the digital assets held and to transfer digital assets from an address. Thus, generating a sufficiently robust private key and maintaining security of private keys or the “seed” inputs to the generation of the private key is essential to mitigating the risk of misappropriation or loss of digital assets.

Entities that have ownership and control of their private keys may generate the key pair themselves using off-the-shelf or customized hardware and software. This hardware or software may include random number generators, computers, hardware security modules, and physical storage. Access to the aforementioned hardware, software, or key pairs that enable the movement of digital assets should be limited to authorized personnel. Additional risk factors, including fraud risk factors, exist when personnel involved in the key-generation process are also involved in financial or technology roles.

As the key-generation process results in the information needed to initiate transactions on the blockchain (that is, the private keys), access at each stage of the key-generation process should be properly controlled. Personnel with access to private keys created during the key-generation process should be monitored to verify that duties are compatible with their other responsibilities. For example, it may be inappropriate for individuals with financial reporting responsibilities to have access to private keys, giving them the ability to execute unauthorized transfers of digital assets held by the entity.

Physical security

Although digital assets are virtual in nature and do not exist in a physical sense, private keys may be generated and stored on a physical device. Private keys may be stored in the entity's facilities either digitally, physically in the form of physical printouts, or both, and they can also be stored off-site or in a cloud storage infrastructure not owned by the entity, such as within third-party cloud data centers. Typically, an entity will store multiple copies of this data to prevent the entity from losing access to the data if one of the copies is lost or damaged. Controls over the entity's ability to hold, copy, or transmit private keys should be considered in developing and maintaining physical security. For example, access to physical locations where private keys are stored may be controlled through the following measures:

- Limiting approved access to personnel with compatible duties;
- Logging of individuals visiting the site;
- Use of badges, physical keys, or other measures to verify appropriate segregation of duties; and
- Utilization of third parties (for example, data centers or other secure facilities).

Encryption or "sharding" of private keys

An entity may encrypt its private keys to provide additional security of the private keys. An entity may use hardware or software, or a combination of the two, to encrypt the private keys, and require a pass phrase or other information to decipher the private key, so that it can be used to authorize a transaction.

To provide additional security, entities may also separate their private keys into multiple components, which is known as *sharding*. Sharding of private keys means using cryptographic techniques to split the private key into multiple parts. Because a transaction cannot be initiated without a private key, splitting up and separately storing the pieces of private keys requires an additional step, the "reassembling" of the private key, to occur prior to using the private key to initiate a transaction. These "shards" can be distributed to various physical or virtual locations and maintained under the control of different individuals. For example, shards of the private keys may be held in various safety deposit boxes geographically isolated, with access to those safety deposit boxes monitored and logged. The cryptographic parameters determine the number of shards required to reassemble the private keys.

Distributing these shards to multiple individuals requires these individuals to work together to reassemble the private keys. Misappropriation of digital assets using private keys that are sharded and held by multiple individuals would likely require collusion between these individuals or an external cyberattack. The security surrounding these private keys can be further enhanced by encryption of the individual shards.

Multi-signature addresses

The entity may also rely on multi-signature wallets or addresses to require consensus of multiple parties to initiate a transaction. These multi-signature addresses are similar to sharded private keys in that they require multiple pieces of information (for example, multiple private keys) to initiate the transaction. Multi-signature transactions require a minimum number of signatures to authorize a transaction. For example, a "3 of 5" multi-signature address would require three distinct private keys to initiate a transaction, of the five total private keys associated with that multi-signature address.

2. Auditor risk assessment considerations

Note:

Examples of risks

An inherent risk exists that the private keys could be lost, destroyed, stolen, or misused by either internal or external parties. The financial statement implications of this risk may include the following:

- If the private key has been stolen or inappropriately accessed, the entity's digital assets likely will have been lost or moved to an address the entity does not control (that is, the assets no longer exist in the entity's addresses).
- If the private key has been lost or destroyed, the entity may no longer have the ability to access its digital assets (that is, the entity no longer has rights to the assets).

Auditors may also consider risks of material misstatement due to fraud resulting from private key loss or theft. Examples include the following:

- The loss or theft of the private key may be intentionally hidden to mask financial losses.
- Management asserts to the loss of private keys, records those losses in the books and records, and misappropriates assets from the related public addresses.

Additionally, if an entity enlists a third party to hold its digital assets on the entity's behalf, the third party may fail to effectively safeguard the digital assets. This may be by not safeguarding the digital assets from hacking and not maintaining access to the private key, or by the third party using the customer assets outside the terms of service.

Lastly, if multiple parties have access to the private keys, the risk exists that each party could claim to "control" the digital assets. This may result in the recognition of an asset for which the entity does not have rights to the asset.

Examples of risk assessment procedures

An initial step in identifying and assessing risks of material misstatement relating to the entity's rights and ownership of digital assets or an entity's obligation to safeguard digital assets held on behalf of others is understanding how the risk of loss or theft of the private keys is mitigated through storage and access controls.

Obtaining an understanding of how digital assets are stored includes understanding whether the assets are held in "self-custody" or by a third party, whether the assets are stored in segregated or commingled public addresses, and to what extent private keys are stored offline (cold storage) or online (hot storage). Entities may have different methods of storage for different digital assets, may use a combination of storage methods, and may change methods from time to time. This understanding may be obtained via observation and inquiry of appropriate personnel and inspection of internal control documentation.

When obtaining an understanding of the internal controls that the entity has implemented to safeguard digital assets, the auditor will likely determine it is important to obtain an understanding of controls that address the following:

- Hardware and software procurement & deployment (including management's due diligence over the technology);
- Initial generation of private key;
- Ongoing safeguarding of the private key;
- Backups or other recovery mechanisms;
- Access to perform digital asset transactions;
- Segregation of incompatible duties;
- General IT controls with respect to the digital wallet software; and
- Cybersecurity.

It is important for the auditor to understand these controls regardless of whether the digital assets are held in self-custody or by a third party. If the digital assets are held by a third party and an adequate service auditor's report is not available, and the controls are relevant to the audit, in accordance with paragraphs .12b–d of AU-C section 402, *Audit Considerations Relating to an Entity Using a Service Organization,* the auditor should perform additional procedures to obtain an understanding of the controls, such as making inquiries of the third party and observing control activities taking place. In accordance with paragraph .05 of AU-C section 705, *Modifications to the Opinion in the Independent Auditor's Report*, the auditor is required to express clearly an appropriately modified opinion (such as a scope limitation) when the auditor is unable to obtain sufficient appropriate evidence to conclude that the financial statements as a whole are free from material misstatement. Refer to section E, "Digital assets held by third parties," for further discussion.

Understanding of the following factors, usually through a combination of inquiry of management or those charged with governance, observation of control performance, and inspection of documentation produced by the entity, assists the auditor in understanding management's controls over private keys:

- Which personnel are involved in the key-generation process and what their roles are within the entity and within the key-generation process. The auditor, including a member of the engagement team with adequate skills and understanding of the technical configuration of the systems used, may need to observe the key-generation process to determine the role of those individuals involved in the key generation.
- The entity's onboarding and offboarding processes for employees with access to private keys, including whether background checks are performed.
- How the entity transfers private keys after they are generated into storage, and who can view or obtain the private keys during transfer.

- Where the entity's private keys are stored, including the safeguards that exist at each location. The auditor may consider observing the physical storage locations, which may involve the following:
  - Inquiring of security personnel to determine who has access to the media the keys are stored on, how an employee's access is managed upon hiring or termination, whether access to private key databases is logged, and whether logs are reviewed. The auditor may consider inspecting the logs for evidence of the reviews.
  - Observing the physical security in place, such as access badges or key codes, including determining how long those controls have been implemented and what evidence is available for inspecting historical access (for example, logs).
- The encryption process, including procedures used when those procedures are performed, the encryption methods used, and who is responsible for the encryption. The encryption procedures may be performed soon after the process of generating the private keys to prevent the keys from being accessible in an unencrypted format.
- Whether the information needed to decrypt the private keys is appropriately controlled, including where and how the tools and information used to decrypt the private keys are stored. For example, if a private key is encrypted and an employee has access to the tools needed to decrypt the private key, the auditor may consider management's process for determining what information the employee could retain if the employee was terminated or if the employee's duties no longer require the ability to decrypt the private key.
- The controls in place to verify proper segregation of duties with respect to access and recording of digital assets, considering the competency and background of the individuals involved.
- If private keys are sharded, management's process and controls related to the following:
  - Who has access to the sharded private keys;
  - The number of individuals necessary to reassemble the private keys;
  - Whether these shards are encrypted and where they are stored;
  - The process of initiating the reassembly of the private keys and how the sharded information is reassembled.
- The entity may rely on specific IT systems to manage this process.
- Control over multi-signature addresses, considering similar factors as for sharded private keys because the security procedures often share similar attributes regarding the dissemination of information needed to acquire the relevant data to authorize transactions using private keys.

Effective risk assessment procedures may include consideration of the potential for loss or theft of the private key after the balance sheet date, so that the auditor can design appropriate subsequent events procedures.

B. Transacting in digital assets

1. Overview of concepts, processes, and controls

An entity may transact in digital assets through several means and for a variety of purposes. Different means of transacting in digital assets may reflect differences in intended uses of the assets and result in different accounting considerations and risks. Although some methods of transacting in digital assets are similar to transacting in securities and financial instruments, such as acquiring assets on an exchange or through an over the counter (OTC) desk, some means of transacting in digital assets, especially in the acquisition of digital assets, are unique to digital assets. Methods of transacting in digital assets may include the following:

- Acquiring or transferring digital assets using a third-party exchange or OTC desk;
- Acquiring digital assets as payment for selling products or services to customers;
- Transferring digital assets for payments to vendors or employees;
- Acquiring from a token issuer;
- Acquiring through forks and air drops (discussed later) from existing digital assets owned by the entity; and
- Acquiring through validating activities, such as mining and staking.

Effective and timely communication among software engineering, security, accounting, operations, and any applicable service organizations is necessary for an entity to sufficiently design a control environment responsive to each transaction method.

The concepts, processes, and controls relating to transacting in digital assets are often most relevant to the rights and obligations, occurrence, and completeness assertions. It is important for the entity to establish specific processes and controls focused on key aspects of digital asset transactions, including the following:

- Verifying that transactions are authorized by appropriate individuals, including reviewing the intended address of the transaction;
- Considering the use of manual approvals prior to authorizing transactions above certain monetary values, similar to controls that may be in place over fiat disbursements; and
- Understanding the identities of the counterparties, including whether a particular counterparty subjects the entity to additional regulations.

This section provides additional details on some methods of acquiring assets that are unique to the digital asset industry: forks, airdrops, and mining and staking activities. The next section (Section C, "Digital asset transaction monitoring and reporting") provides an overview of controls related to monitoring and reporting digital asset transactions, which is applicable for each type of transaction method.

Acquisition through forks and airdrops

Two acquisition methods unique to the digital asset ecosystem are *forks* and *airdrops*. The blockchains on which digital assets exist can be "forked" by other entities and developers. Forks occur when changes are made to the blockchain's software, but not all network participants adopt the changes. These forks are classified as either *hard forks* or *soft forks*. Soft forks do not require network participants to adopt the new software to continue to participate in the network, whereas hard forks cause the updated software to be incompatible with the previous version of the software, resulting in two types of digital assets that are incompatible with one another's respective blockchain. Technical changes in the underlying infrastructure may result in incompatibility with an entity's means of tracking or transferring the digital asset. Therefore, it is important for the entity to have qualified individuals with the requisite technical means of understanding and implementing changes to the digital asset's infrastructure, including responding to changes made to the blockchain network.

Airdrops occur when blockchain developers distribute digital assets, often for free, to blockchain addresses. Airdrops are commonly used to promote a particular digital asset and spur a greater user base or increase trading volume.

Both forks and airdrops may result in new digital assets owned by the entity or its customers for no consideration paid. Internal systems and processes must be designed to capture instances of forks and airdrops to determine completeness and accuracy of digital assets held by the entity as well as determine appropriate accounting treatments.

Validating activities

Another acquisition method unique to digital assets is the concept of *validating*. Certain blockchains use models such as "proof-of-work" or "proof-of-stake" to validate transactions on the blockchain and reward the validators with digital assets as compensation for their participation in the network. Validators participating on blockchains with a "proof-of-work" model compete to successfully complete complex computations needed to validate blockchain transactions and earn mining fees in the form of digital assets. A validator's ability to earn mining fees in a "proof-of-stake" model depends less on computing power and more on the validator's designated holdings (or "stake") of digital assets on a particular blockchain. This determines how rewards will be allocated for participation in the cryptographic processes to maintain integrity of the blockchain network and its transactions.

Similar to forks and airdrops, validating activities result in digital assets acquired, the primary evidence of which is the blockchain activity itself. Because of the importance of technical capabilities in appropriately identifying and monitoring digital asset acquisitions from these and other similar methods, an entity may need to involve several departments, including accounting, legal, engineering, and compliance, to appropriately design its controls.

2. Auditor risk assessment considerations

Because digital assets may have different properties than those of other assets, it is important for the auditor to consider the manner in which management and those charged with governance have adapted the entity's controls. The controls need to be responsive to potential additional risks and considerations relating to these digital assets. It is necessary to gain an understanding of the processes and controls related to digital asset transactions, which may include the following:

- The entity's process to assess the risks posed from the acquisition and transacting in digital assets;
- The ongoing monitoring of the entity's controls as new digital assets with new properties are added, including the potential effect of forks, airdrops, and other means of acquiring digital assets; and
- The extent of formal documentation of the entity's processes and controls surrounding the acquisition and transacting of digital assets, including understanding of the counterparty to the transaction and evaluating related party relationships and transactions.

In addition, the acquisition of new digital assets may require the auditor to gain an understanding of the entity's process and controls that have been tailored to address the related unique risks. Understanding of the following assists the auditor in understanding management's controls over the acquisition of new digital assets:

- Classification of the digital asset under the relevant regulatory framework (for example, whether the asset is considered a security);
- Whether there are regulatory restrictions on the purchase and sale of the digital asset;
- Whether there are related parties involved in the development or governance of the digital asset;
- The means of providing consideration to pay for the digital asset (for example, through fiat via the banking system or through other digital assets); and
- Accessibility and capability of the digital assets network, including whether the blockchain is visible to the public or to the entity.

The auditor may also determine it is appropriate to understand management's policies for recognizing digital assets received resulting from hard forks, airdrops, or validating activities.

C. Digital asset transaction monitoring and reporting

1. Overview of concepts, processes, and controls

Reporting digital asset transactions involves the following processes, each of which is described in this section:

- Monitoring digital asset transactions on the blockchain;
- Evaluating the reliability of blockchain data and methods used to extract blockchain data;
- Determining the appropriate classification and measurement of digital asset transactions; and
- Determining the appropriate cut-off of digital asset transactions.

The concepts, processes, and controls relating to digital asset transaction monitoring and reporting are most relevant to the occurrence, completeness, accuracy, existence, classification, valuation, and cut-off assertions.

Monitoring digital assets on the blockchain

Blockchains typically provide a level of anonymity that is not present in transactions via fiat currencies through traditional financial institutions. Digital assets and the blockchains they operate on inherently do not provide account statements in the conventional sense. Instead, blockchains typically provide a publicly observable history of all transactions on the blockchain, albeit without personally identifiable information. Specific considerations relating to transacting in digital assets should be considered by the entity.

Some types of digital assets, known as *privacy coins*, may use blockchains in which transaction data such as sending or receiving addresses, balances, or other transactional information are not publicly observable, which may require additional considerations when recording and accounting for transactions involving these digital asset types. It is important for the auditor to consider the potential implications and risks associated with privacy coins if held or used by the entity.

Due to the degree of pseudo-anonymity and immutability of transactions on blockchains, it is important for the entity to establish specific processes and controls focused on key aspects of digital assets transaction monitoring and reporting, including the following:

- Identifying and evaluating digital asset transactions on the blockchains, considering the appropriateness of the entity's general IT controls when the entity has automated processes in place;
- Considering AML, KYC, and other regulations for exchanges and other entities subject to such regulations (also see section F, "Digital assets held on behalf of others");
- Identifying related party transactions on the blockchains, including considering the entity's capabilities and controls surrounding the capturing of relevant information about blockchain addresses it is transacting with;
- Performing timely reconciliations of blockchain transactions to the entity's accounting records and other relevant off-chain information (for example, bank statements, contracts); and
- Identifying in a timely manner security breaches that could potentially result in the entity's private keys being compromised.

An entity's control in these areas is often designed to detect situations in which private keys have been stolen or misused by either internal or external parties.

Evaluating the reliability of blockchain data and methods used to extract blockchain data

For digital asset transactions that are processed on a blockchain, the completeness, occurrence, and cut-off of the transactions are largely dependent on the reliability of the blockchain itself as well as any methods used to extract the information from the blockchain. Therefore, it is important that management consider the reliability, accuracy, and completeness of information it obtains from blockchains.

A blockchain's technological parameters determine what methods are available for an entity to produce a balance of digital assets from the blockchain at a point in time. For example, many blockchains consist of ledgers of transactions (ins and outs) in public addresses, the sum of which is the spendable balance at a given point in time. Blockchains often provide software applications that query the blockchain to obtain balance data for a given public address. Further, third-party online block explorers also provide similar data. An entity may also host its own "node" (or copy) of the blockchain and build its technology infrastructure to obtain information from the blockchain. Regardless of the method used, entities should develop processes and controls to validate the reliability of the source and completeness and accuracy of the data obtained from the blockchain.

Further, reliability of the blockchain itself can pose additional risks. Certain blockchains may not provide transparency in governance or in transactions. These blockchain technologies may introduce additional risks requiring further risk assessment procedures to identify and respond to the assessed risks. For example, newer blockchains with untested or unverified properties or capabilities may represent an increased risk that the information in the blockchain is not reliable and that the blockchain can be manipulated by other parties, either within or external to the entity. In addition, while a blockchain may work effectively, the technology does not alleviate the risk that transactions recorded therein could be unauthorized, fraudulent, or illegal and, hence, render the information subject to new or different risks the auditor would consider. Management should have processes and controls in place to assess the reliability of the blockchain and potential risks associated with manipulation of the blockchain data. Having processes and controls in place to reconcile blockchain data to entity records may support the accuracy and completeness of transactions and balances. For digital assets new to the entity, management may consider reviewing the underlying technical documentation of the blockchain and the extent of the decentralization of the validators in the network.

Refer to Q&A 1: "Evaluating the reliability of information obtained from a blockchain," in chapter 5 of this practice aid, for factors that may be relevant to consider when evaluating the reliability of a blockchain.

Determining the appropriate classification of digital asset transactions

Many accounting systems are not designed to accommodate digital asset transactions. As part of management's reconciliation of digital assets from the related blockchains to the entity's internal records, management is responsible for determining the appropriate classification of transactions in the entity's accounting systems. Therefore, incremental processes may be necessary to properly record these transactions in the entity's accounting system, for example, distinguishing entity-owned assets from those held on behalf of customers. These incremental processes may introduce additional risks. Understanding the substance of the transaction is necessary for the entity to determine the accounting treatment. The entity should also design and implement policies and procedures to address how or whether digital assets are recorded in the entity's financial records.

An entity should have competent members of the finance and accounting teams to determine appropriate accounting treatment of its digital assets or assets held on behalf of others. Different digital assets may have different properties warranting varying classifications in the financial statements and disclosure in the notes to the financial statements. Processes should be in place to assess the proper classification and tracking of digital assets. Additionally, the nature of the transaction may affect how the transaction is recorded. For example, if the entity's primary activities include facilitating customer exchanges of digital assets in an agency capacity, the entity may determine it is not appropriate to record the gross settlement of digital assets but, rather, to record the transaction fees associated with that digital asset transaction as revenue. Understanding the business purpose of the entity's primary activities and transactions in assessing the proper classification of digital assets can often present unique challenges. (See AC chapter 1, "Classification, measurement, and recognition," of this practice aid for guidance related to classification of digital assets.)

Determining the appropriate cut-off of digital asset transactions

Due to the decentralized nature of blockchains and digital assets, transactions may occur at any time and are not restricted to normal business hours. In addition, blockchains may vary significantly in the speed with which they process transactions, which could result in cut-off issues if there are significant delays. It is important for the entity to have formal policies in place to determine the period in which transactions occur and that controls be implemented to determine that these policies are consistently applied. If the entity has operations spanning multiple time zones, using one time zone when recording transactions across the entire entity may help prevent errors that result in inaccurate or incomplete cut-off in the period-end recording of digital asset transactions and balances.

2. Auditor risk assessment considerations

As part of the auditor's risk assessment process, it is important for the auditor to understand how management records transactions for an entity's digital assets or digital assets it holds on behalf of others and balances in its books and records, including how it determines that the information being recorded is complete, accurate, appropriately classified, and recorded in the appropriate period. As part of obtaining this understanding, the auditor would consider the methods used to extract the information from the blockchain, including the risk that the methods used to extract the information do not function as expected.

When digital asset transactions are not processed on a blockchain (for example, processed off-chain by an exchange), it is important for auditors to consider the risk that information obtained from a third party (for example, an exchange) is not reliable. Refer to section E, "Digital assets held by third parties," for further discussion.

As part of understanding whether the entity is consistently applying its accounting policies, it also may be relevant for the auditor to understand who drafts and approves accounting documentation and who posts and reviews journal entries. The auditor considers the types of disclosures related to the entity's digital asset activities, including the entity's obligation to safeguard digital assets on behalf of others, if applicable, that may be appropriate to include in the financial statements and may make inquiries of management or those charged with governance about its planned disclosures that may be appropriate or required.

Management's processes and controls over digital asset transactions and reporting may differ depending on the characteristics of a particular blockchain. In accordance with ET section 0.300.060, an auditor should possess the necessary knowledge and technical capabilities to identify and assess the risks related to each relevant blockchain and digital asset. These capabilities include understanding the technical parameters of the data output by the blockchain, such as the definition of various fields and components of amounts presented in transaction data.

Management inquiries to aid in the auditor's understanding may include the following:

- What technical analysis, including the assessment of reliability, integrity, and availability of information obtained from the blockchain, does the entity perform prior to acquiring a new digital asset?
- What tools are used to extract transaction and balance data from each relevant blockchain?
- How does management consider reliability of each relevant blockchain and tools used to extract data from the blockchain?
- Do the parameters of the blockchain obscure digital assets transactions or cause complexities in determining a point in time balance (for example, privacy coins)?
- How does management validate that cut-off times for digital asset balances have been appropriately established and are consistently applied?
- How does management confirm accuracy in preparation of digital asset reconciliations?
- What controls are in place over completeness and accuracy of information used in the reconciliations?
- What volume of public addresses does the entity control for each digital asset, and how are digital asset balances dispersed among the public addresses?
- How does management validate that all digital asset transactions are authorized by appropriate individuals?
- How does management identify related party transactions on the blockchain?
- How would management know if a security breach occurred that did (or could) compromise the entity's private keys?
- How does management record digital asset transactions and balances in its books and records?
- How does management assess the reliability of information obtained from a third party when digital asset transactions are not processed on a blockchain?
- How does the entity segregate its own assets from assets it holds on behalf of others?
- How does the entity determine that its accounting policies are consistently applied?

In addition, the entity may develop its own IT infrastructure systems, databases, and applications for tracking and reporting digital assets held by the entity, or it may purchase third-party software to perform some or all the functions needed by the entity. Evaluating general IT controls and application controls relating to these systems may be relevant to the audit.

Depending on the results of the auditor's risk assessment, consideration of management's controls over completeness of digital asset addresses may be relevant, including understanding how key pairs are generated and the controls in place to determine that the address listing is complete. The auditor may also consider management's controls over maintaining an inventory of addresses, such as roll-forwards performed by the entity or comparing the address population at year-end with prior periods, to understanding additions or removals to the address population. In addition, it is important for auditors to consider whether there is a risk of material misstatement because an entity did not record all its digital assets, including those that resulted from hard forks or airdrops and validation rewards. The existence of a wallet not previously accounted that comes to the attention of the auditor during the course of the audit may be an indication that its existence was deliberately hidden. This may be indicative of a fraud risk, including the risk of management override of controls regarding digital asset wallets.

D. Digital asset valuation

1. Overview of concepts, processes, and controls

Fair value measurements of digital assets are necessary when an entity measures digital assets at fair value or for an impairment analysis. See FASB ASC 820, which provides guidance that applies to all entities, transactions, and instruments that require or permit fair value measurements. Also, see Q&As 16–21 in AC chapter 4, "Fair value measurement," of this practice aid for more detailed discussion of the fair value accounting considerations related to digital assets.

The digital asset ecosystem consists of a large number of marketplaces with operations that may not have been fully developed, institutionalized, or regulated. This exposes entities to challenges in valuing digital assets. Digital assets are commonly traded on multiple exchanges, which may result in inconsistent pricing across the various marketplaces, and not all marketplaces may be designed to prohibit self-dealing. Processes and controls should be in place to make sure that the valuation of digital assets is consistently and appropriately applied in accordance with GAAP and the entity's accounting policies.

This section provides an overview of the following unique attributes of digital assets, which often make valuation (including the identification of impairment indicators, when applicable) more complex:

- The lack of intrinsic value of many types of digital assets;
- Challenges in identifying and accessing the principal (or most advantageous) market for digital assets given that multiple marketplaces often exist globally for the same assets;
- The decentralized nature of blockchain and the ability for transactions to occur between parties at any time; and
- Variation in levels of regulation in digital asset marketplaces.

Lack of intrinsic value

Most traditional asset classes have clearly defined benefits or underlying cash flows that provide a basis for assessing fair value when market data is limited. For example, financial assets often carry defined cash flow streams, which can be discounted at appropriate discount rates to estimate fair value. Digital assets often lack even unobservable inputs from which fair values can be independently measured aside from market transactions. This lack of intrinsic value can pose challenges when estimating fair value for thinly traded digital assets. These factors likely result in higher inherent risk that these types of assets are misstated because they are not appropriately valued. This may be indicative of a fraud risk factor whereby management uses biased assumptions in order to manage earnings.

Lack of a clear principal (or most advantageous) market

The valuation of digital assets requires entities to determine which sources of the value or pricing of the digital assets should be used. Fair value of digital assets determined in accordance with FASB ASC 820 should reflect the price at which a transaction would take place between marketplace participants in the principal (or, in its absence, the most advantageous) market. The *principal market* is defined as the market with the greatest volume and level of activity for the asset or liability. In the absence of a principal market, an entity should determine the *most advantageous market* that an asset could be sold in, which is defined as the market that maximizes the amount that would be received to sell the asset or minimizes the amount that would be paid to transfer the liability, after taking into account transaction costs and transportation costs. FASB ASC 820-10-35-5A states that in the absence of evidence to the contrary, the market in which the reporting entity normally would enter into a transaction to sell the asset or transfer the liability is presumed to be the principal market or, in the absence of a principal market, the most advantageous market.

In circumstances in which a market is immature, the following characteristics can make the principal (or most advantageous) market for digital assets difficult to substantiate or identify:

- Pricing information reported to an entity may not be representative of orderly transactions (for example, when related party considerations are present).
- Volume data reported by sources may be unreliable (for example, pricing sources may engage in wash trading to inflate volume).
- The principal (or most advantageous) market can change frequently due to current market fragmentation and the ability to transfer assets across marketplaces instantly, in many cases.

These characteristics increase the risk that an entity is unable to properly identify the principal (or most advantageous) market, whether erroneously or intentionally (that is, "cherry-picking" pricing sources).

Valuation measurement date and time

Unlike traditional markets, the market for digital assets does not close, and an entity may inappropriately measure its digital assets at times of the day that are not consistent across reporting periods (for digital assets measured at fair value on a recurring basis under applicable GAAP) and not in accordance with its valuation policies. This, in combination with the significant intra-day volatility of digital assets, could result in a material misstatement of valuation.

Regulation

The regulatory framework of a marketplace can influence the efficacy and transparency of underlying transactions and reporting in that market. Because the same digital assets trade in disparate markets around the world with varying levels of regulation and oversight, determining the level of pricing reliability requires diligence on the part of the entity.

2. Auditor risk assessment considerations

It is important for the auditor to understand management's process for pricing digital assets to evaluate whether accounting and disclosure requirements were appropriately considered and addressed. When gaining an understanding of processes and controls surrounding the valuation of digital assets, it is important for the auditor to consider the facts and circumstances of the entity.

This understanding may be obtained by inspecting management's valuation policies and documentation and making inquiries of management or those charged with governance that address various considerations, including the following:

- How the entity identifies the principal (or most advantageous) market for each digital asset, including how it considers the reliability of information about the volume and level of activity in various markets;
- How the entity considers the reliability of pricing information obtained;
- Whether, and if so, how, the entity evaluates variances between prices used and other available third-party price data, including the precision of any variance thresholds;
- The time of day used as the balance sheet cut-off for measuring digital assets (for example, at fair value or at cost less any impairment, depending on applicable GAAP);
- Whether any changes have been made to valuation policies and the reasons for any changes;
- How the entity measures illiquid investments in digital assets, including how it determines the amount of weight placed on observable trades for the digital asset and how it identifies digital assets that are similar (if pricing of similar digital assets is used as part of the valuation);
- Whether the entity uses a specialist to measure the value of digital assets, and if so, the competency and objectivity of management's specialist; and
- If the entity applies an accounting policy that requires evaluation of asset impairment (for example, digital assets accounted for as intangible assets), how the entity identifies and assesses impairment indicators in accordance with GAAP and the entity's accounting policies.

E. Digital assets held by third parties

1. Overview of concepts, processes, and controls

Entities may use a third party to maintain custody of their digital assets or the digital assets held on behalf of others. In such circumstances, the entity is responsible for making sure that the third party has designed appropriate controls related to digital asset safeguarding and any other relevant processes that exist at the third party (for example, transaction monitoring and reporting). One way to do this is to obtain and review an appropriate SOC report from the third party that provides assurance about the effectiveness of the controls in place at the third party to address the relevant risks.

The concepts, processes, and controls relating to digital assets held by third parties are most relevant to the existence, completeness, accuracy, and rights and obligations assertions.

Commingling of digital assets

For operational and security purposes, entities holding digital assets in custody for customers often pool customer digital assets into consolidated addresses on the blockchain. Thus, each customer's digital assets are not determinable simply by viewing publicly available blockchain activity. Likewise, not all digital asset transactions result in transactions recorded on blockchains. These third parties maintain a customer database separate from the blockchain to track and monitor individual customer activity and balances with batched transaction activity being broadcasted to the blockchain when necessary.

For example, an exchange, acting as a custodian on behalf of its customers, may purchase digital assets directly from customers wishing to sell their digital assets. In this situation, the net position of the entity's digital assets remains unchanged, and no blockchain transactions are necessary to fulfill these transactions. In this scenario, the only changes are the amount of digital assets held on behalf of its customers and the amount held by the entity and to which it has rights. These transactions are recorded only on the third party's internal ledger. Alternatively, if the entity has assigned addresses to its individual customers, this transaction may result in a blockchain event (for example, sending the digital asset from the address assigned to the customer to an address assigned to the entity).

2. Auditor risk assessment considerations

It is important for the auditor to inquire of management or those charged with governance whether any digital assets recognized by the entity and, if applicable, digital assets held on behalf of others, are held on other platforms outside of the entity's control. In accordance with paragraph .09 of AU-C section 402, *Audit Considerations Relating to an Entity Using a Service Organization,* the auditor should obtain an understanding of how the user entity uses the services of a service organization in its operations, including the following:

- The nature of the services provided by the service organization and the significance of those services to the user entity, including their effect on the user entity's internal control;
- The nature and materiality of the transactions processed or accounts or financial reporting processes affected by the service organization;
- The degree of interaction between the activities of the service organization and those of the user entity; and
- The nature of the relationship between the user entity and the service organization, including the relevant contractual terms for the activities undertaken by the service organization.

If the services provided by a service organization are relevant to the audit of an entity's financial statements, obtaining an understanding of management's processes and controls, as well as the controls established by the service organization (and subservice organizations, if applicable) will be relevant. In obtaining an understanding of controls implemented by the entity over service organizations, used in relation to digital assets and digital asset transactions, the auditor may consider the following:

- Who initiates and authorizes transactions with the third party and what processes the entity has in place over the initiation of transactions with the third party;
- How transactions with the third party are recorded and reconciled in the entity's accounting records;
- How the entity validates that the third party maintains control of the digital assets in its custody, particularly when digital assets are commingled by the custodian;
- How the entity monitors the effectiveness of the third party's internal controls (for example, review of SOC reports); and
- How the entity validates the effective design and implementation of relevant complementary user entity controls.

An understanding of the controls implemented by the service organizations may be obtained through review of a SOC report. However, it is important for the auditor to determine what reliance can be placed on the SOC reports. If the auditor is unable to obtain sufficient understanding of the nature and significance of the services provided by the service organization from the user entity or through review of SOC or other attestation reports (for example, due to unavailability or unreliability), the auditor will likely need to perform additional procedures to assess the risk of material misstatement related to the transactions and balances. Paragraph .12 of AU-C section 402 provides additional procedures that may be performed in such cases, including the following:

- Contacting the service organization, through the user entity, to obtain specific information;
- Visiting the service organization and performing procedures that will provide the necessary information about the controls at the service organization that address risks of material misstatements at the assertion level in accordance with AU-C section 315; and
- Using another auditor to perform procedures that will provide the necessary information about the controls at the service organization that address risks of material misstatement at the assertion level in accordance with AU-C section 315.

In the event that sufficient understanding of the nature and significance of the services provided by the service organization and their effect on the audit cannot be obtained at the third party, the auditor may need to consider the impact on the audit report (for example, a scope limitation).

F. Digital assets held on behalf of others

1. Overview of concepts, processes, and controls

Entities that hold digital assets on behalf of others need to have processes and controls in place to track customer balances separately from entity balances, onboard new customers, and authorize and monitor digital asset transactions.

Tracking customer balances separately from entity balances

As explained in the previous section on commingling of digital assets, digital asset custodians and exchanges often maintain a customer database separate from the blockchain to track and monitor individual customer activity and balances. Some of these entities may also combine customer and entity digital assets into the same consolidated addresses. The digital assets held by the entity are periodically reconciled to the digital assets held on the blockchain. Because the reconciliation process only validates that total (customer and entity) digital assets in the database agree to the blockchain, entities should effectively design and implement controls over the IT applications and databases to verify accurate segregation of customer and entity digital assets as well as individual customers' digital assets.

Customer onboarding and due diligence

Storing assets on behalf of customers introduces additional legal and regulatory risks and responsibilities for the entity, including the entity's responsibility to validate that their customers' identities are properly verified as part of customer onboarding.

The jurisdictions in which the entity, its subsidiaries, and its customers are located may have regulations in place requiring the entity to perform customer due diligence (CDD) procedures as part of the customer onboarding process. These procedures verify that the entity knows the true identity of the customer and that the customer is not subject to sanctions or other situations that may restrict the customer from transacting with the entity or its products.

When this is the case, it is important for the entity to have formalized CDD policies with sufficiently designed and operating controls in place. Differences in jurisdictions, whether local, state, federal, or international, require the entity to have robust processes in place prior to expanding its operations into new jurisdictions as well as existing processes in place to continuously monitor changes to existing customers or customer base. An entity may be subject to civil or criminal penalties for not complying with these policies, resulting in increased financial statement risks.

Transaction authorization and monitoring

Entities will need to implement appropriate systems, processes and controls to validate that transactions executed in relation to digital assets held on behalf of others have been appropriately authorized. Entities may also implement monitoring controls, to identify unusual activity associated with digital assets held on behalf of others.

2. Auditor risk assessment considerations

If an entity is holding digital assets on behalf of others as well as for their own purposes, it is generally important for the auditor to understand the following:

- How the digital assets are segregated and what procedures are performed by the entity to determine whether the segregation of the digital assets is appropriate
- If digital assets held on behalf of others and for the entity are held within commingled addresses, the reconciliation procedures performed (Note: The commingling of digital assets held on behalf of others with the digital assets of the entity may give rise to additional fraud risk factors; for example, inappropriate use of customer assets for the entity's benefit.)
- Whether the entity has controls in place surrounding transaction authorization and monitoring of digital assets held on behalf of others
- Whether the entity has controls in place to verify that enough digital assets are available to meet customer obligations
- The legal and regulatory framework the entity operates under (See AU chapter 3 of this practice aid.)

The following considerations assist the auditor in understanding the processes and controls surrounding customer onboarding and due diligence:

- ***Obtaining an understanding of applicable laws and regulations. (See AU chapter 3 of this practice aid and how the entity's processes and controls are tailored to each jurisdiction in which they operate as well as to the unique characteristics of their customer base.)*** For example, an entity transacting with institutions will likely require different background verification than those required for individual users. The auditor may reperform the review of KYC information provided to the entity as part of the auditor's onboarding procedures. For example, certain types of KYC information may include drivers' licenses or banking information from individual users and entity documents and other forms from institutional customers.
- ***Whether transactions between related parties have been appropriately recorded and disclosed.*** In accordance with paragraph .04 of AU-C section 550, *Related Parties,* the auditor has a responsibility to perform audit procedures to identify, assess, and respond to the risks of material misstatement arising from the entity's failure to appropriately account for or disclose related party relationships, transactions, or balances. This includes whether the transactions reported in the financial statements include related party transactions and whether the financial statements include disclosures required by GAAP. Transactions between related parties may give rise to additional fraud risks because the transactions often lack an arms-length nature. The pseudo-anonymity of blockchain addresses and pseudo-anonymous digital asset transactions heighten this risk. (See AU chapter 3 of this practice aid.)

5. Identify and assess risks of material misstatement and design further audit procedures

1. Identify and assess risks of material misstatement

Risks of material misstatement are identified and assessed by the auditor in order to determine the nature, timing, and extent of further audit procedures necessary to obtain sufficient appropriate audit evidence. This evidence enables the auditor to express an opinion on the financial statements at an acceptably low level of audit risk. Paragraph .32 of AU-C section 315 states the auditor should identify the risks of material misstatement and determine whether they exist at the financial statement level or the assertion level for classes of transactions, account balances, and disclosures.

In addition, paragraph .36 of AU-C section 315 states that the auditor should determine whether any of the assessed risks of material misstatement are significant risks. The determination of which of the assessed risks of material misstatement are close to the upper end of the spectrum of inherent risk and, therefore, are significant risks, is a matter of professional judgment, unless the risk is of a type specified to be treated as a significant risk in accordance with the requirements of another AU-C section. AU-C section 240 and AU-C section 550 provide further requirements and guidance in relation to the identification and assessment of the risks of material misstatement due to fraud and related party relationships and transactions. Significant risks often relate to significant unusual transactions and matters that require significant judgment.

As stated in paragraph .A251 of AU-C section 315, risks of material misstatement that may be assessed as having higher inherent risk and, therefore, may be determined to be a significant risk, may arise from matters such as the following:

- Transactions for which there are multiple acceptable accounting treatments such that subjectivity is involved
- Accounting estimates that have high estimation uncertainty or complex models
- Accounting for unusual or complex transactions (for example, accounting for revenue with multiple performance obligations that are difficult to value)
- Emerging areas (for example, accounting for digital assets)
- Complexity in data collection and processing to support account balances
- Account balances or quantitative disclosures that involve complex calculations
- Accounting principles that may be subject to differing interpretation
- Changes in the entity's business that involve changes in accounting, for example, mergers and acquisitions

Risks of material misstatement may be greater for significant unusual transactions arising from matters such as the following example:

An entity uses a third party (a custodian or an exchange) to hold its digital assets and the digital assets are held in a segregated address. A risk of material misstatement was identified by the auditor that the private keys held by the third party could be lost or destroyed (that is, the inability to access its digital assets raises a risk related to the existence assertion) or are not appropriately safeguarded (that is, unauthorized access to the private keys such that multiple parties could access and claim rights to the assets raises a risk to the rights and obligations assertion).

Based on consideration of this information, as well as consideration of other relevant risk factors (for example, the nature and materiality of the transactions, nature of the relationship between and the services provided by the user entity and the third party, understanding of the relevant controls at the third party, consideration of fraud risk factors) and evidence obtained from the risk assessment procedures, the auditor may determine that the risk of material misstatement is a significant risk.

2. Design further audit procedures

In accordance with paragraph .06 of AU-C section 330, *Performing Audit Procedures in Response to Assessed Risks and Evaluating the Audit Evidence Obtained,* the auditor is required to design and perform further audit procedures whose nature, timing, and extent are based on, and are responsive to, the assessed risks of material misstatement. As the assessed risk of material misstatement increases, the more persuasive the audit evidence needs to be in order to be sufficient and appropriate and to support the audit conclusions. What constitutes sufficient and appropriate audit evidence is a matter of professional judgment based on the characteristics of the identified risk. Therefore, auditor judgments about the evidence needed will influence how auditors design the nature, timing, and extent of the further audit procedures.

The auditor may find it impossible to design effective substantive procedures that, by themselves, provide sufficient appropriate audit evidence at the relevant assertion level.[2] In such cases, in addition to substantive procedures, in accordance with paragraph .08b of AU-C section 330, the auditor should design and perform tests of controls (for example, testing private key management controls over digital asset safeguarding and access to private keys) to obtain sufficient appropriate audit evidence about the operating effectiveness of controls associated with digital assets. This may particularly be the case when the digital assets are commingled or when there is an assessed risk of material misstatement related to circumstances in which multiple parties have access to private keys and could potentially demonstrate “control” of the digital asset.

[2] Paragraph .A25 of AU-C section 330, *Performing Audit Procedures in Response to Assessed Risks and Evaluating the Audit Evidence Obtained.*

AU Chapter 3: Laws and regulations and related parties

Introduction

AU-C section 250, *Consideration of Laws and Regulations in an Audit of Financial Statements,* addresses the auditor's responsibility to consider laws and regulations in an audit of financial statements. The requirements in AU-C section 250 are designed to assist the auditor in identifying material misstatement of the financial statements due to noncompliance with laws and regulations. It is the responsibility of management, with the oversight of those charged with governance, to ensure that the entity's operations are conducted in accordance with the provisions of laws and regulations, including compliance with the provisions of laws and regulations that determine the reported amounts and disclosures in an entity's financial statements.

AU-C section 550, *Related Parties,* addresses the auditor's responsibilities relating to related party relationships and transactions in an audit of financial statements. Paragraph .04 of AU-C section 550 states that the auditor has the responsibility to perform audit procedures to identify, assess, and respond to the risks of material misstatement arising from the entity's failure to appropriately account for or disclose related party relationships, transactions, or balances.

This section of the practice aid addresses the unique challenges and potential procedures to consider surrounding both laws and regulations as well as related parties when auditing an entity that holds or transacts with digital assets. Because related party transactions may reflect a risk of material misstatement due to noncompliance, these topics are considered in the same section.

Laws and regulations

Relevant professional standards

Paragraph .10 of AU-C section 250 states that the objectives of the auditor are to

> a. obtain sufficient appropriate audit evidence regarding material amounts and disclosures in the financial statements that are determined by the provisions of those laws and regulations generally recognized to have a direct effect on their determination;
>
> b. perform specified audit procedures that may identify instances of noncompliance with other laws and regulations that may have a material effect on the financial statements; and
>
> c. respond appropriately to noncompliance or suspected noncompliance with laws and regulations identified during the audit.

Challenges specific to digital assets

The auditor is required to obtain a general understanding of how the entity is complying with the legal and regulatory framework applicable to the entity and the industry or sector in which the entity operates. Given the evolving nature of the regulation of digital assets, it is important to understand the entity's identification, monitoring, and adherence to existing laws and regulations that apply in the digital asset ecosystem, which may require significant judgment and expertise. Inherent in the design of most digital asset ecosystems is the potential for the pseudo-anonymity of the transacting participants. Although pseudo-anonymity may have benefits to certain elements of the ecosystem, it increases the risk that participants are seeking to conceal illegal activities, such as money laundering.

Some of the challenges of meeting the requirements or objectives of GAAS, specific to the digital asset ecosystem, may include the following:

- The maturity of the legal and regulatory environments related to digital assets differs across jurisdictions. These differences may make it difficult for the auditor to obtain an understanding of the legal and regulatory framework applicable to the entity, which may include compliance with regulatory requirements, including those addressing internal control, market surveillance, custody, financial statement disclosures, tax, securities law, and investor or consumer protection. Additional difficulty arises from the evolving nature of the legal and regulatory environment related to digital assets (for example, regulations may change, previously unregulated activity may become regulated, and so on).
- The pseudo-anonymity of participants in public blockchain transactions may make it difficult for the auditor to identify transactions with related parties or with entities who have or may have illegal intentions.
- For entities that facilitate customer transactions of digital assets (for example, custodians and exchanges), the pseudo-anonymity of parties involved in public blockchain transactions may make it difficult for the auditor to understand the business purpose of the transactions (or lack thereof).

Procedures to consider specific to digital assets

Procedures to address the risk of material misstatement of the financial statement due to noncompliance with laws and regulations include the following:

- Inquire with management to understand its processes (and controls, as applicable) to identify, stay current with, comply with, and monitor compliance with laws and regulations.
- Inquire with management to understand the applicable laws and regulations, including understanding whether management has obtained regulatory licenses, as applicable.
- Inquire with management to understand and evaluate its business purpose related to transactions involving digital assets, including considering whether there are any indicators of fraud, asset concealment, or money laundering.
- Understand the entity's business strategy and intentions (for example, acquiring a broker-dealer to transact in the digital asset ecosystem or investment in an initial coin offering [ICO]) and understand the nature and extent of management's communications or formal agreements with appropriate regulators (for example, the Financial Industry Regulatory Authority [FINRA], SEC, Commodity Futures Trading Commission [CFTC], state money transmitter authorities, and states attorney general).
- Inquire with management, legal counsel (internal and external), and those charged with governance concerning the entity's compliance with laws and regulations and knowledge of noncompliance (potential or actual).
- Inquire with management to understand its policies and procedures to onboard new customers or enter into relationships with other players in the digital asset ecosystem. These may include performing know your customer (KYC), anti-money laundering, and other due diligence procedures to understand the identity and integrity of the counterparty.
- Inquire with management to understand how the entity identifies transactions with entities who have or may have illegal intentions. For entities that facilitate customer transactions of digital assets, auditors may also inquire with management to understand how the entity evaluates the integrity of trading, including procedures to identify and investigate
  - fraud and market manipulation;
  - compliance with applicable laws and regulations (including security regulations); and
  - suspicious transactions, which may be subject to monitoring and reporting regulatory requirements.

- Evaluate underlying transactions, for example, identifying whether there are patterns that may be indicative of legal violations, either by the entity or by others, which the entity may be required to identify and report.
- Consider whether the laws and regulations permit or prohibit self-dealing.
- Read external sources of information (for example, through media searches and other sources) and remain alert for any contradictory information.
- Evaluate legal letters (internal or external) and determine whether it is necessary to obtain specific legal representations.
- Inquire with management regarding any regulatory inquiries or other similar matters and related responses or communications. Inspect correspondence, if any, with the relevant licensing or regulatory authorities.
- Evaluate whether recorded accruals or the disclosure of possible loss contingencies arising from digital asset activities, including those related to pending or threatened litigation and noncompliance with laws and regulations, are appropriate.
- Read minutes of board of director and audit committee meetings.
- Obtain written representation from management specific to the circumstances.
- Engage legal or other specialists when needed. For example, in some cases, a legal specialist may be engaged to assist with a required procedure.

Certain of these procedures may have been performed during the client or engagement acceptance and continuance process and may also be used to satisfy the requirements of AU-C section 250.

In addition, the auditor is required to respond appropriately to noncompliance or suspected noncompliance with laws and regulations identified during the audit in accordance with AU-C section 250.

Related parties

Relevant professional standards

Paragraph .09 of AU-C section 550 states that the objectives of the auditor are to

a. obtain an understanding of related party relationships and transactions sufficient to be able to

   i. recognize fraud risk factors, if any, arising from related party relationships and transactions that are relevant to the identification and assessment of the risks of material misstatement due to fraud.

   ii. conclude, based on the audit evidence obtained, whether the financial statements, insofar as they are affected by those relationships and transactions, achieve fair presentation.

b. obtain sufficient appropriate audit evidence about whether related party relationships and transactions have been appropriately identified, accounted for, and disclosed in the financial statements.

Challenges specific to digital assets

Not only does the pseudo-anonymity of participants in digital asset transactions create challenges for considerations related to AU-C section 250, but it also creates unique challenges when considering the requirements of AU-C section 550. The pseudo-anonymity creates challenges in obtaining sufficient appropriate audit evidence about whether related party relationships and transactions have been appropriately identified, accounted for, and disclosed in the financial statements. Related party relationships and transactions may present risk of error, illegal acts, or fraud. For example, an auditor may identify a risk of material misstatement related to the entity conducting market activities to manipulate the value of a thinly traded digital asset issued by the entity. As another example, management may seek to materially misstate its financial position or results of operations by concealing related party transactions or "double-counting" by asserting ownership of the same digital assets across entities (for example, in a fund complex).

Some of the challenges of meeting the requirements or objectives of GAAS, specific to the digital asset ecosystem, may include the following:

- The pseudo-anonymity of participants in public blockchain transactions may make it difficult to identify transactions with related parties. For example, an auditor may be unable to determine if a digital asset transaction is also a related party transaction if an entity does not perform KYC or other procedures that assist with determining the specific names and identities of counterparties.
- Management may not have the ability or the related processes and controls to properly identify, account for, and disclose transactions with related parties.
- Sufficient appropriate evidence may not be available to demonstrate that a transaction management asserts to be arms-length is, in fact, arms-length. Potential risks may exist around self-dealing or "round trip transactions."
- For entities that facilitate customer transactions of digital assets (for example, custodians and exchanges), management may not have the ability or the related processes and controls to
  - distinguish between transactions on the entity's behalf and those that are on the customer's behalf;
  - identify employee or platform trading (for example, conflicts of interest, self-dealing).

Procedures to consider specific to digital assets

Procedures to obtain sufficient appropriate audit evidence about whether related party relationships and transactions have been identified, accounted for, and disclosed in the financial statements specific to the digital asset ecosystem include the following:

- Consider the results of client or engagement acceptance or continuance.
- Inquire with management to understand and evaluate its business purpose related to the transactions involving digital assets, including possible related party considerations.
- Evaluate management's policies and procedures for identifying, recording, summarizing, and disclosing related party transactions related to digital assets and perform additional procedures, including testing relevant controls, as necessary.
- Evaluate management's policies and procedures for obtaining appropriate knowledge of the parties with whom the entity is entering into digital asset transactions and perform additional procedures, including testing relevant controls, as necessary.
- Evaluate management's policies and procedures for identifying those transactions that are self-dealing or potential conflicts of interest and perform additional procedures, including testing relevant controls, as necessary.
- Examine the entity's digital asset transactions and consider whether management has appropriately identified all related party transactions. This may include substantive procedures related to the completeness of related party transactions identified by management. For example, obtain a listing of all entity-owned wallets and search for transactions with entity-owned wallets, obtain evidence of the counterparty to digital asset transactions by examining off-chain evidence (for example, digital asset transaction agreements and contracts) and determine whether the counterparty is a related party.
- Test management's controls for identifying, recording, summarizing, and disclosing related party transactions related to digital assets, if substantive procedures alone cannot provide sufficient appropriate audit evidence at the assertion level.

Note:

Paragraph .A25 of AU-C section 330 states that the auditor may find it impossible to design effective substantive procedures that, by themselves, provide sufficient appropriate audit evidence at the relevant assertion level. This may occur when an entity conducts its business using IT, and no documentation of transactions is produced or maintained, other than through the IT system. In such cases, paragraph .08b of AU-C section 330 requires the auditor to perform tests of controls that address the risk for which substantive procedures alone cannot provide sufficient appropriate audit evidence.

- Consider related disclosures.

AU Chapter 4: Consideration of an entity's use of a service organization

Background

Processing digital asset transactions and safeguarding digital assets often requires sophisticated technologies and platforms as well as specialized knowledge of blockchain and related technologies within the digital asset ecosystem. In many cases, entities may use third parties that have the technological capabilities and competencies to transact in, safeguard, or account for digital assets, including digital assets entities hold on behalf of others. A user entity[1] in this circumstance, having a responsibility to maintain effective internal control over financial reporting (ICFR), needs to design and implement complementary user entity controls (CUECs) as well as controls to monitor third-party services.

AU-C section 402, *Audit Considerations Relating to an Entity Using a Service Organization*[2] identifies such third parties as service organizations[3] if the services they provide to user entities are relevant to the user entity's ICFR. AU-C section 402 also states the following:

- Services provided by a service organization are relevant to the audit of a user entity's financial statements when those services and the controls over them affect the user entity's information system, relevant to the preparation of the financial statements.
- Other related controls, beyond those that are part of the user entity's information system relevant to the preparation of the financial statements, also may be relevant to the audit, such as controls over the safeguarding of assets.

Paragraph .11 of AU-C section 402 requires the user auditor[4] to determine whether a sufficient understanding of the nature and significance of the services provided by the service organization and their effect on the user entity's system of internal control has been obtained to provide an appropriate basis for the identification and assessment of the risks of material misstatement.

If the services provided by a service organization are relevant to the user entity's ICFR, AU-C section 402 requires the user auditor to do the following:

- Obtain an understanding of the nature and significance of the services provided by the service organization, and their effect on the user entity's system of internal control sufficient to provide an appropriate basis for the identification and assessment of the risks of material misstatement.
- Design and perform further audit procedures that are responsive to those risks.

[1] A user entity is an entity that uses a service organization and whose financial statements are being audited.

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

[3] A *service organization* is an organization, or segment of an organization, that provides services to user entities (that is, entities that use a service organization). For additional information on what constitutes a service organization and when controls at a service organization are relevant to a user entity's audit, see AICPA Guide Reporting on an Examination of Controls at a Service Organization Relevant to User Entities' Internal Control Over Financial Reporting (SOC 1®) (SOC 1 guide) and AICPA Guide *SOC 2® Reporting on an Examination of Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy* (SOC 2 guide).

[4] A *user auditor* is an auditor who audits and reports on the financial statements of a user entity.

In applying AU-C section 315, *Understanding the Entity and Its Environment and Assessing the Risks of Material Misstatement,* when obtaining an understanding of the entity's system of internal control, the user auditor should identify controls in the control activities component at the user entity from those that relate to the services provided by the service organization, including those that are applied to the transactions processed by the service organization, and evaluate their design and determine whether they have been implemented.[5] AU-C section 402 identifies the aspects of a user entity's information system that may be affected by a service organization's services. One aspect is how transactions of the user entity are initiated and how information about them is recorded, processed, corrected as necessary, and incorporated in the financial statements. In addition, how information about events or conditions, other than transactions, is captured, processed, and disclosed by the user entity in the financial statements. In the context of digital assets, it is important that the user auditor understand the procedures related to safeguarding and transferring digital assets (for example, reconciliations, online digital wallets, trading services, custodian storage methods, and private key management). The user auditor will need a sufficient understanding of services provided by subservice organizations[6] to enable the user auditor to evaluate the effect of those services on the audit.

Inquiry alone is not sufficient to obtain audit evidence about the design and implementation of identified controls.[7] When obtaining an understanding of the user entity in accordance with AU-C section 315, the user auditor should obtain an understanding of how the user entity uses the services of a service organization in the user entity's operations, including the following:[8]

a. The nature of the services provided by the service organization and the significance of those services to the user entity, including their effect on the user entity's internal control.

b. The nature and materiality of the transactions processed or accounts or financial reporting processes affected by the service organization.

c. The degree of interaction between the activities of the service organization and those of the user entity.

d. The nature of the relationship between the user entity and the service organization, including the relevant contractual terms for the activities undertaken by the service organization.

Such understanding may also assist the user auditor in determining whether the service organization represents a related party, which may affect the identification and assessment of the risks of material misstatement. (See the section "The entity's controls established to identify, authorize, and approve related parties and relationships, and transactions with related parties" under item 5, in AU chapter 1, "Client acceptance and continuance" of this practice aid.)

If the user auditor is unable to obtain a sufficient understanding of the services provided by the service organization from the user entity, in accordance with paragraph .12 of AU-C section 402 the user auditor should obtain that understanding from one or more of the following procedures:

- If available, obtaining and reading a type 1 or type 2 system and organization controls (SOC) 1 report. In certain instances, a type 1 or type 2 SOC 2 report may provide some relevant information. (See Interpretation No. 1, "Considerations Related to the Use of a SOC 2® Report in an Audit of a User Entity's Financial Statements," of AU-C section 402.) The "Different Types of SOC Reports" section of this chapter includes information on the different types of SOC reports and what each report covers. No matter which SOC report is obtained, the user auditor is required to perform certain procedures to evaluate the SOC report as audit evidence. These procedures generally address whether the SOC report is sufficient to meet the user auditor's objectives by considering, for example, its type and its relevance to the audit (such as whether the SOC report addresses controls related to the reliability of data, including the timeliness, accuracy, and completeness of the data obtained from the blockchain).

[5] See paragraph .10 of AU-C section 402, *Audit Considerations Relating to an Entity Using a Service Organization.*

[6] A *subservice organization* is a service organization used by another service organization to perform some of the services provided to user entities that are relevant to those user entities' internal control over financial reporting.

[7] See paragraph .A203 of AU-C section 315, *Understanding the Entity and Its Environment and Assessing the Risks of Material Misstatement.*

[8] See paragraph .09 of AU-C section 402.

- Contacting the service organization, through the user entity, to obtain specific information. Specific information may include information related to the design and implementation of relevant controls at the service organization.
- Visiting the service organization and performing procedures that will provide the necessary information about the controls at the service organization that address risks of material misstatement at the assertion level in accordance with AU-C section 315. For example, the user auditor may test controls at a service organization or perform procedures related to a user entity's transactions or balances maintained by the service organization.
- Using another auditor to perform procedures that will provide the necessary information about the controls at the service organization that address risks of material misstatement at the assertion level in accordance with AU-C section 315. For example, a user auditor may request, through the user entity, that a service auditor perform agreed-upon procedures, such as testing controls at a service organization or performing procedures related to a user entity's transactions or balances maintained by the service organization.[9]

Different types of SOC reports

User auditors may be able to obtain the necessary understanding of the controls at the service organization and whether they have been implemented by obtaining and reading SOC reports that address controls at the service organization relevant to user entities' ICFR. For both SOC 1® and SOC 2® engagements, type 1 and type 2 reports are available. A type 1 report provides evidence about the design and implementation of controls at a point in time; a type 2 report[10] provides evidence of the design, implementation, and operating effectiveness of the controls over a defined period covered by the report.

User auditors use SOC 1 reports, which focus on ICFR, to evaluate the effect of the service organization's controls on the user entity's internal control relevant to the audit. In addition to SOC 1 reports, many entities participating or involved with digital asset transactions obtain SOC 2 reports. These latter reports focus on the service organization's controls relevant to one or more of the categories of trust services criteria related, for example, to the security, availability, and processing integrity of the systems used to process data or to the confidentiality and privacy of data). See Interpretation No. 1 of AU-C section 402.

Challenges specific to auditing digital assets affected by the services performed by service organizations

The following areas may present specific challenges to the user auditor when performing audit procedures related to digital assets relevant to services provided by a service organization. The following examples are not exhaustive — other facts and circumstances may need to be considered:

- **Risks for which substantive procedures alone may not provide sufficient appropriate audit evidence**

  As discussed further in AU chapter 2, "Risk assessment and processes and controls," of this practice aid, substantive procedures alone may not provide sufficient appropriate audit evidence for certain risks of material misstatement (for example, ownership of digital assets). Thus, for risks of material misstatement for which substantive procedures alone do not provide sufficient appropriate audit evidence, it is important for the user auditor to plan and perform procedures to obtain audit evidence about the operating effectiveness of relevant controls. Relevant controls may operate at both the user entity and service organization. The user auditor may obtain audit evidence about the operating effectiveness of the service organization's controls from a type 2 report.

[9] See paragraph .A10 of AU-C section 402.

[10] AU-C section 402 includes other requirements for consideration regarding tests of controls and using a type 2 report as audit evidence that controls at the service organization are operating effectively. AU-C section 402 also addresses required procedures to be performed if a type 2 report is not available.

- **Incremental planning and risk assessment considerations when a service organization provides services related to digital assets**

Challenges	Audit Considerations
Service organizations may not be subject to regulatory oversight.	A service organization that is operating or processing transactions related to digital assets for user entities may not be subject to regulatory oversight. Additionally, although regulations may exist, the service organization may not be registered with the appropriate regulator. **This may result in additional risks for the auditor to consider when identifying and assessing the risks of material misstatement for these digital asset transactions.**
Service organizations that provide custodian services may "commingle" or combine digital assets into a single public address.	The practice of commingling digital assets may make it difficult for the user auditor to trace the user entity's digital assets to the blockchain itself because the blockchain no longer represents either the user entity's holdings only or digital assets the user entity holds on behalf of others. **These scenarios may present risks of material misstatement related to the improper allocation of the digital assets to specific entities that would likely need to be addressed by effective controls at the service organization.** See "The SOC report may not include all the necessary reasonable control objectives" section of this chapter for considerations on how auditors may address these situations.
A SOC report may not be available from the service or subservice organization, or a SOC report exists but is not fit for purpose.	In these circumstances, additional procedures will likely be needed to understand, evaluate the design, determine the implementation, and, if applicable, test the operating effectiveness of controls at the service organization that are relevant to the audit (for example, contacting the service organization through the user entity and performing procedures that will provide the necessary audit evidence about the operation of the relevant controls).

The preceding table is not intended to be a complete list of challenges or audit considerations — other facts and circumstances may need to be considered. Ultimately, if substantive procedures alone are not sufficient and the user auditor is unable to obtain sufficient appropriate audit evidence regarding the services provided by the service organization relevant to the digital assets (including the operating effectiveness of controls relevant to the audit that operate at the service organization), **a limitation on the scope of the audit may exist.**

- **Using a SOC report to obtain an understanding of the service organization and evidence of the design and operating effectiveness of controls at a service organization**

  When a SOC report is available and the user auditor plans to use it as audit evidence to support the user auditor's understanding about the design and implementation of identified controls at the service organization, the user auditor should evaluate the sufficiency and appropriateness of the audit evidence provided by the SOC report for the understanding of the identified controls at the service organization.[11] The illustrative risks and considerations that follow may affect whether the SOC report provides sufficient appropriate audit evidence or whether a limitation on the scope of the audit may exist.

  1. *The service auditor who issued the SOC report may lack the experience and skills to properly assess the risks related to the digital asset transactions that the controls are intended to mitigate.*

     Because digital asset transactions can be highly complex, specialized knowledge may be needed to understand cryptographic methods, how such transactions are processed, the risks associated with the various technologies, and how digital assets are safeguarded as necessary. Thus, the user auditor should be satisfied with the service auditor's professional competence and independence from the service organization.[12] In this regard, the service auditor's experience and expertise in blockchain-inspired technologies is relevant. However, information about the service auditor's competency as it relates to digital assets may not be evident from the SOC report alone. For this reason, user auditors may perform (for instance) one or more of the following procedures to evaluate the service auditor's competency:

     - Make inquiries about the service auditor to the service auditor's professional organization or other practitioners and inquire whether the service auditor is subject to regulatory oversight.
     - Through contact facilitated by the user entity, make inquiries of the service auditor to obtain information about the service auditor's experience and qualifications relative to providing attestation services within the digital asset ecosystem.
     - Evaluate the sufficiency and appropriateness of the report, including whether
       - relevant risks related to digital assets were identified and addressed,
       - service organization system risks and controls related to digital assets are clearly described, and
       - tests of controls address the risks related to digital assets.

     If the user auditor determines that the service auditor lacks the appropriate skill sets and competency related to digital assets, the user auditor may conclude that the SOC report does not provide sufficient appropriate audit evidence and, therefore, that additional audit procedures are necessary. For example, if the user auditor expected to see within the report control objectives over cryptographic key management, custody, or record keeping of customer transactions and finds that the report either does not address or insufficiently addresses such risks, it may raise concerns about (*a*) the service auditor's competency, (*b*) the sufficiency and appropriateness of the SOC report, and (*c*) the reliability as audit evidence of the third-party confirmation.

[11] See paragraph .14b of AU-C section 402.

[12] See paragraph .13 of AU-C section 402.

2. *The SOC report may not provide sufficient appropriate audit evidence for the user auditor to understand the service organization's controls relevant to the audit.*

   When a user entity uses a service organization, it is typical for certain transactions to be initiated, recorded, or processed in a way that is physically and operationally separate from the user entity's system of internal control. After obtaining a SOC report and reading the description of the service organization's system, the user auditor should evaluate the sufficiency and appropriateness of the evidence provided by the report for the understanding of the identified controls at the service organization.[13] The system description generally discusses the features of the service organization's controls that would affect a user entity's ICFR. The user auditor also should obtain an understanding of the degree of interaction between the activities of the service organization and those of the user entity.[14]

   In certain instances, SOC reports may lack the transparency or detail necessary to enable the user auditor to sufficiently understand the nature of the services provided, including how the service organization processes digital asset transactions or how it safeguards digital assets. For example, due to the service organization's concerns over security or the disclosure of proprietary information, a SOC 1 report might not include detail sufficient for the user auditor to understand the processes and controls over certain complex digital asset transactions. SOC 2 reports are likely to include even less relevant information regarding the processing of transactions than would a SOC 1 report.

3. *The SOC report may not include all the necessary reasonable control objectives.*

   An important aspect of evaluating a SOC report is determining whether the control objectives included in the description are relevant in the circumstances (for example, controls that address the risks of material misstatement identified by the user auditor) and whether the effective design and implementation of CUECs are necessary to achieve certain control objectives. Examples follow:

   - A common concern of user auditors relates to the lack of proper controls over private key life-cycle management at the service organization, which could result in significant losses from misappropriation or inaccessibility of assets. Thus, given the importance of wallet architecture, key generation, backup, key-recovery seeds, and continued key security in addition to the typical reconciliation and reporting control objectives, a user auditor evaluating a SOC report may expect to see control objectives that cover wallet architecture and the full life cycle of cryptographic key generation (such as encryption, distribution, backups, and maintenance of privileged user access rights).
   - Because private keys may be stored offline (cold storage) or online (hot storage), it is important for user auditors to understand
     - the risks associated with the selected method of storage and
     - the controls designed to safeguard the private keys.

     For example, when a user entity uses the service organization's cold storage to maintain its private keys, the user auditor evaluates whether the SOC report addresses controls over the safeguarding of private keys.

[13] See paragraph .14b of AU-C section 402.

[14] See paragraph .09c of AU-C section 402.

- Permissionless blockchains may increase the potential for illegal activities (for example, money laundering) or for related party transactions due to the anonymity of parties to blockchain transactions. Although control objectives in the SOC report may not directly address these risks, user auditors may expect to see a combination of controls at both the service organization and the user entity, including the following:
  - The service organization's process for registering new customers, including identity verification upon opening an account
  - The user entity's processes and controls to
    - identify, authorize, and approve related parties and transactions with related parties,
    - onboard new customers (for example, know-your-customer (KYC) procedures and anti-money laundering procedures), and
    - review the record of account users and addresses for unauthorized activity. (See AU chapter 3, "Laws and regulations and related parties," of this practice aid.)
- Service organizations (for example, wallet providers, other custodians, or exchanges) may maintain key elements of the accounting records on behalf of the user entity. Controls over the completeness and accuracy of the user entity's financial statements may not be addressed in the SOC report or, if addressed, may not be sufficiently addressed, particularly when the service organization offers custody of digital assets as an ancillary service (for example, an exchange). In these instances, it may be important for the user auditor to understand and evaluate the design and operating effectiveness of the CUECs that address the completeness and accuracy of the user entity's financial statements. This includes evaluating whether the design of the relevant controls is responsive to the risks presented by the asset class. For example, performing a reconciliation of the information in the user entity's financial statements to the blockchain or to the user entity's subledger (or equivalent), or both, on a monthly basis only may not be responsive to the risks posed by the continuous updates to the blockchain.
- Service organizations (for example, a wallet provider or other custodian) may maintain custody of digital assets within commingled public addresses that include the digital assets of other depositors. This may hinder the user auditor's ability to inspect the user entity's specific assets held by the custodian to the blockchain itself because the commingled address does not represent only the user entity's holdings. In these circumstances, determining the sufficiency and appropriateness of the audit evidence provided by the SOC report includes understanding and evaluating evidence about the design and operating effectiveness of those controls that account for and reconcile segregated customer ledgers to the commingled public addresses.
- SOC reports may lack disclosure of the service organization's underlying IT architecture and the design of related IT controls. For example, the SOC report may not clarify whether the service organization leverages open-source software to support its operations.[15] In these circumstances, it is important for user auditors to understand whether the service organization uses open-source software and, if so, the design of relevant controls that address its reliability. User auditors may inquire of the service organization to understand how it monitors protocol updates and evaluates how those protocol updates on the blockchain affect open-source software.

[15] Open-source software is software with source code that anyone can inspect, modify, and enhance.

If the control objectives in the SOC report do not address the identified risks of (a) material misstatement or (b) material events (for example, creation of new wallets) because those events occur after the period covered by the SOC report, then the user auditor, through management of the service organization, may seek to determine if the service auditor can adjust the scope of the report or perform additional audit procedures at the service organization to obtain audit evidence and further support the user auditor's understanding of relevant controls. If the user auditor determines that substantive procedures alone are not sufficient, and the service auditor is unable to adjust the scope of the report or otherwise obtain sufficient appropriate audit evidence, a scope limitation may exist.

4. *Controls may have occurred prior to the period covered by the current SOC report.*

   When a user auditor plans to use a type 2 SOC report as audit evidence, the user auditor should consider whether the type 2 report is for a period appropriate for their purposes.[16] An often-critical control related to digital assets is the generation of the private key, which may have occurred in a prior period and may have been subject to controls in effect at that time. This is an important consideration when determining the extent of evidence provided by the SOC report. See Technical Questions and Answers 9560.01–.06, *Information About Controls Over Cryptographic Keys in a SOC 1® Report*.

5. *The description in the SOC report may indicate that certain CUECs are necessary to achieve certain control objectives.*

   It is important to identify which aspects of digital asset transactions are the responsibility of the user entity and which are the responsibility of the service organization. For example, in some situations, although a service organization that provides digital wallet services may control access to the digital assets under custody, the user entity may also need to have controls in place to restrict access to the service organization's digital wallet system.

Note: It is important for user auditors to understand and evaluate whether management has controls in place to review SOC reports and implement applicable CUECs.

6. *SOC reports may carve out the services of a subservice organization.*

   The scope of a SOC report may carve out relevant subservice organizations used to facilitate transaction processing, safeguard digital assets, or account for digital assets. In gaining an understanding of the services provided by the subservice organization and their effect on the user entity's ICFR, AU-C section 402 requirements apply when a SOC report's description of the system identifies services provided by a subservice organization that is carved out of the SOC report. (A SOC description includes the service organization's monitoring activities over the subservice organization.) This will likely involve obtaining a SOC report from the subservice organization or performing alternative procedures to obtain sufficient appropriate audit evidence in accordance with AU-C section 402.

[16] See paragraph .14a of AU-C section 402.

Part II: Overview

Part II of this practice aid addresses, in Q&A format, factors that may be relevant for the auditor to consider or potential procedures that the auditor may perform when designing and performing procedures in response to risks of material misstatement associated with digital assets.

If auditors encounter challenges related to obtaining sufficient appropriate audit evidence, auditors may need to revisit AU chapter 1, "Client acceptance and continuance," or AU chapter 2, "Risk assessment and processes and controls," of this practice aid and consider whether the challenges impose a scope limitation resulting in a disclaimer or qualification of opinion.

Part II includes the following chapters:

- AU chapter 5: Considerations for existence, rights, and obligations of digital assets
  - Q&A 1: Evaluating the reliability of information obtained from a public blockchain
  - Q&A 2: Accessing information recorded on a blockchain
  - Q&A 3: Audit procedures to address the existence and rights and obligations of digital assets held in self-custody
  - Q&A 4: Audit procedures to address the existence and rights and obligations of digital assets held by a third party
  - Q&A 5: Digital asset third-party confirmation considerations
- AU chapter 6: Considerations for valuation of digital assets
  - Q&A 1: Measuring digital assets using prices in active markets
  - Q&A 2: Measuring digital assets that are thinly traded
  - Q&A 3: Considerations for evaluating an entity's impairment analysis for indefinite-lived out-of-scope crypto intangible assets
  - Q&A 4: Considerations for an entity that recognizes realized gains and losses on sales of digital assets

Note:

Independence and ethics — The topics in this section of the practice aid focus on auditing applications and do not address ethics considerations, including those related to independence. It is important to note, however, that these considerations remain critical to an auditor's performance of the engagement in conformity with professional standards, and engagements in the digital asset ecosystem may introduce new or different compliance risks warranting additional consideration by the auditor.

For information regarding independence requirements and ethics responsibilities, see the AICPA Code of Professional Conduct at pub.aicpa.org/codeofconduct/Ethics.aspx.

In addition, see paragraph .07, "Operating Node Software on a Blockchain," in Q&A section 100, *Independence*, at the following link:

http://pub.aicpa.org/codeofconduct/resourceseamlesslogin.aspx?prod=ethics&tdoc=et-qa&tptr=et-qa100

Risk of material misstatement due to fraud — For entities in the digital asset ecosystem, the Q&As herein do not contemplate all potential risks of material misstatement, including all potential fraud risks. AU-C section 240, *Consideration of Fraud in a Financial Statement Audit,* includes further requirements regarding procedures to identify and respond to fraud risks.

Risks of material misstatement due to fraud may be present, and the auditor should identify and assess such risks at the financial statement level and at the assertion level for classes of transactions, account balances, and disclosures.[1,2] See AU chapter 2 of this practice aid for factors to consider when identifying and assessing risks of material misstatement, including those that may be significant risks due to error or fraud.

Obtaining sufficient appropriate audit evidence — Planning further audit procedures that are responsive to risks of material misstatement requires the exercise of professional judgment. Further audit procedures may include both tests of controls and substantive procedures. Substantive procedures alone may not provide sufficient appropriate audit evidence (for example, ownership of digital assets). As stated in paragraph .08 of AU-C section 330, *Performing Audit Procedures in Response to Assessed Risks and Evaluating the Audit Evidence Obtained,* the auditor should design and perform tests of controls to obtain sufficient appropriate audit evidence about the operating effectiveness of relevant controls if (*a*) the auditor's assessment of risks of material misstatement at the relevant assertion level includes an expectation that the controls are operating effectively (that is, the auditor intends to rely on the operating effectiveness of controls in determining the nature, timing, and extent of substantive procedures) or (*b*) substantive procedures alone cannot provide sufficient appropriate audit evidence at the relevant assertion level.

The auditor may find it impossible to design effective substantive procedures that, by themselves, provide sufficient appropriate audit evidence at the relevant assertion level. This may occur when an entity conducts its business using IT and no documentation of transactions is produced or maintained, other than through the IT system. In such cases, paragraph .08b of AU-C section 330 requires the auditor to perform tests of relevant controls.[3]

The auditor may often conclude that a combination of tests of controls (for example, private key management controls) and substantive procedures is needed to obtain sufficient appropriate audit evidence to address the risks of material misstatement associated with digital assets. Due to these considerations and challenges associated with digital assets, it will be important for auditors to carefully evaluate, exercising professional judgment, whether sufficient appropriate audit evidence has been obtained to address the risks of material misstatement.

[1] Paragraph .26 of AU-C section 315, *Understanding the Entity and Its Environment and Assessing the Risks of Material Misstatement.*

[2] Paragraph .25 of AU-C section 240, *Consideration of Fraud in a Financial Statement Audit.*

[3] Paragraph .A25 of AU-C section 330, *Performing Audit Procedures in Response to Assessed Risks and Evaluating the Audit Evidence Obtained.*

AU Chapter 5: Considerations for existence, rights, and obligations of digital assets

Note: Auditing Q&As 1–5 of this chapter do not contemplate digital assets held on behalf of others that give rise to a safeguarding liability and corresponding safeguarding asset in accordance with SEC's Staff Accounting Bulletin (SAB) No. 121.[1] Different considerations and procedures may apply for entities that safeguard digital assets held on behalf of others subject to SAB No. 121. (See appendix B, "SEC Staff Accounting Bulletin (SAB) No. 121 Questions and Answers," of this practice aid for more information about SAB No. 121.)

Evaluating the reliability of information obtained from a public blockchain

Question 1:

When evaluating the reliability of information obtained from a public blockchain to be used as audit evidence, what factors may be relevant for an auditor to consider?

Response 1:

AU-C section 500, *Audit Evidence,* requires auditors to evaluate information to be used as audit evidence by taking into account the relevance and reliability of the information, including its source.[2] Paragraphs 5–8 of appendix A, "Considerations Regarding the Use of External Information Sources," of AU-C section 500 provides guidance regarding the relevance and reliability of information obtained from external information sources, including its accuracy and completeness. Specific to the evaluation of the reliability of information obtained from a public blockchain, important factors may include, but are not limited to

- the nature and authority of the external information source;
- the competence and reputation of the external information source with respect to the information, including whether, in the auditor's professional judgment, the information is routinely provided by an external information source with a track record of providing reliable information;
- past experience of the auditor with the reliability of the information provided by the external information source;
- evidence of general market acceptance by users of the relevance or reliability of information from an external information source for a similar purpose to that for which the information has been used by management or the auditor; and
- whether the reporting entity has in place controls to address the relevance and reliability of the information obtained and used.

[1] On January 30, 2025, SEC Staff Accounting Bulletin (SAB) No. 122 was published in the Federal Register and became effective. SAB No. 122 rescinds SAB No. 121, *Accounting for Obligations to Safeguard Crypto-Assets an Entity Holds for its Platform Users.* For more information on SAB No. 122, see note at top of Appendix B, "SEC Staff Accounting Bulletin No. 121 Questions and Answers".

[2] Paragraph .07a of AU-C section 500, *Audit Evidence.*

Given the decentralized governance mechanisms employed by multiple blockchains, an auditor’s evaluation of the reliability of the information obtained from a blockchain may also involve considering the methods used by the technology in producing the information. The following considerations may assist auditors in obtaining an understanding of the technology and its impact on the reliability of information to be used as audit evidence that is obtained from a blockchain.

The degree of applicability of such considerations will vary depending on specific facts and circumstances, including the nature of the blockchain (for example, the type of consensus mechanism used).

In addition, the nature, timing, and extent of audit procedures performed to evaluate the reliability of the information used in the audit may vary depending on, among other factors,

- the assessed risks of material misstatement,
- the degree of reliance placed on the information obtained from the blockchain as audit evidence,
- whether the entity has in place controls to address the relevance and reliability of the information obtained and used, and
- the evaluation of other evidence obtained throughout the audit.

Depending on the degree of expertise of the auditor and the assessed risks of material misstatement, auditors may conclude an auditor's specialist (for example, cryptography and cybersecurity specialists) is necessary to assist them in evaluating the reliability of information obtained from a blockchain used as audit evidence.

Reliability of the information obtained from a public blockchain

Consensus mechanism

The consensus mechanism enables a network of participants to agree that only transactions that follow pre-established rules are deemed valid and added to the blockchain. Correspondingly, the validity of transactions recorded on the blockchain is directly affected by the consensus mechanism and risks associated with the consensus mechanism. The reliability of blockchain records may be diminished when a blockchain’s code contains design vulnerabilities, which, if exploited, could trigger unintended consequences. Therefore, it may be important for auditors to understand the consensus mechanism as part of their procedures to determine where a blockchain falls on the spectrum of producing reliable information (for example, producing more or less reliable information). In considering the consensus mechanism, auditors obtain an understanding of the type and nature of the consensus mechanism used by the blockchain and may consider, among other factors, the following:

- The method for handling unconfirmed transactions and validating and recording confirmed transactions
- The process for resolving issues associated with forks (for example, multiple blocks may be accepted and built on top of each other, forking the chain and allowing for the double-spending of transactions)
- The unique risks associated with the type of consensus mechanism (for example, weaknesses in a proof-of-work or proof-of-stake consensus mechanism could lead to issues such as double-spending or a 51% attack)[3]
- Whether the same information is disseminated to all nodes on the blockchain, thereby ensuring the nodes are operating based on the same information
- If the blockchain has a history of accepting invalid transactions as valid, resulting in inaccurate or invalid transaction details and balances

[3] A 51% attack is the threat that the network’s consensus mechanism used to regulate network activity may be compromised by controlling a majority of the validators needed for adding a subsequent block. For example, where a proof-of-work consensus mechanism is used, a 51% attack refers to an attack on a blockchain by a group of miners of that blockchain controlling more than 50% of the network’s mining hash rate, or computing power. The theory is that attackers would be able to prevent new transactions from gaining confirmations, allowing them to halt new transactions being added to the ledger. Similarly, in a proof-of-stake consensus mechanism, a group of validators holding more than 50% of staked assets may perform a similar attack.

Auditors may consider involving specialists as part of these procedures. The nature and complexity of consensus mechanisms vary across different blockchains (for example, proof of work or proof-of-stake) and identifying changes to or risks associated with consensus mechanisms may be beyond the traditional auditor's skill set.

Network validators

Network validators perform the essential tasks of validating and confirming new blocks that are added to the blockchain and may be rewarded for completing those tasks depending on the consensus mechanism's incentive model. Depending on how the consensus mechanism is designed, a blockchain may be vulnerable to attacks that may result in transactions being removed, reorganized, and replaced. A key design feature of a more reliable blockchain is an incentive model that promotes good behaviors and discourages bad behaviors. Therefore, auditors may need to understand how validators are rewarded under the consensus mechanism as part of the auditor's procedures to determine where a blockchain falls on the spectrum of producing reliable information. In addition, the reliability of a blockchain's records may decrease when the participation of the validators becomes centralized within the network. When the network is dominated by an individual or small group of validators, their influence may disrupt the proper distribution of validation rewards and may allow inappropriate actions on the networks, such as reversals of transactions and payments being rearranged by the attackers (that is, by nodes/validators that are bad actors). Auditors may obtain an understanding of the consensus mechanism's incentive models and whether network validators have significant influence to identify whether any risks are present. In obtaining this understanding, the auditor may consider engaging specialists, as the pseudo-anonymous nature of most blockchains often leads to challenges in determining the identity of network validators and whether they have significant influence.

Occasionally, transactions are not accepted by the network validators and, therefore, such transactions are not confirmed on the blockchain network. Unconfirmed transactions may be caused by a variety of reasons, including but not limited to insufficient fees paid to blockchain miners or transactions that violate the blockchain protocols (for example, double-spending attempts). Inclusion of such transactions within the information pulled from the blockchain without proper methods of identifying confirmed or unconfirmed transactions could render information obtained from the blockchain to be less reliable. Therefore, obtaining an understanding of policies and procedures implemented by management of the reporting entity for validating that only confirmed transactions are obtained from the blockchain (for example, management policies surrounding the number of confirmations needed to record blockchain transactions in their internal books and records) may assist auditors in evaluating the reliability of information.

Blockchain governance — Community of developers

A community of developers is needed to perform ongoing maintenance, development, and enhancement of the consensus mechanism, and code changes. An effective community promotes blockchain adoption, responds to feedback from users and validators, provides learning material, performs research and development for the source code, organizes version updates, and performs source code testing and monitoring, among other functions. In the absence of an effective community, risks associated with the reliability of the network may arise, such as a fork in the network or unstable processing on the blockchain due to the lack of governance or coordination over changes to the blockchain's consensus mechanism. In understanding the community, auditors may work with specialists to obtain an understanding of processes, including governance or coordination related to ongoing maintenance, development and enhancement of the consensus mechanism, and changes in the blockchain code. Although changes to the blockchain code may be public, a lack of proper governance surrounding changes to the consensus mechanism across the community of developers could lead to unreliable information being processed and maintained on the blockchain and result in an auditor assessing the information obtained from the blockchain as less reliable.

Other considerations

Auditors may also need to consider other decentralized applications built on top of the blockchain that may be used by management when executing digital asset transactions. Examples of decentralized applications include smart contracts and second-layer payment channels (for example, bitcoin lightning network). In addition, certain digital assets may provide specific features unique to the specific assets. For example, a digital asset may have privacy mechanisms that shield or obfuscate transaction detail recorded on a blockchain, which can make it difficult to obtain audit evidence related to a given transaction. If such applications or features are being used, auditors may need to consider additional factors when evaluating the reliability of information recorded on a blockchain. For example, in addition to understanding the underlying blockchain, auditors may obtain an understanding of how the applications interface with the blockchain, methods used by the application, the extent to which the reporting entity relies on the system to process data, and controls the entity has in place to consider the reliability of the information.

Accessing information recorded on a blockchain

Question 2:

How may an auditor access information recorded on a public blockchain and what factors may an auditor consider when selecting an appropriate approach?

Response 2:

There are multiple approaches that an auditor might take to access information recorded on a public blockchain. Although this Q&A focuses on the auditor's use of these approaches, similar considerations apply when entity management uses these approaches. In addition to the following methods, entity management may have developed their own ability to query the blockchain, and the auditor may obtain an understanding of and perform substantive procedures or assess the effectiveness of the controls over such methods and related tools to evaluate whether they provide reliable information to be used as audit evidence.

- **Operate own node[4]** – The auditor maintains its own node software that extracts the underlying blockchain data and obtains information recorded on the blockchain in a format useful for audit purposes.
- **Engage a third party** – An auditor may engage a third party who maintains a copy of the underlying blockchain data (for example, by operating their own node). That third party may provide access to software that may be used by the auditor to query and process information recorded on the blockchain in a format useful for audit purposes.
- **Use free public blockchain explorer websites** – There are many free blockchain explorers for various public blockchains that can be accessed online, whereby an auditor may enter search parameters (for example, a public address) and receive information that purports to reflect the information recorded on the blockchain. Note, evaluating the reliability of information obtained from these websites requires the application of professional judgment as the auditor may face challenges in understanding the processes and controls used by free public blockchain explorers to obtain and process information recorded on a blockchain.

Each method previously described has its own considerations, which are discussed in the following section. Given the unique challenges and complexities associated with accessing information recorded on a blockchain, it is important that the auditor has the suitable skills, knowledge, and experience in this area.

[4] It is important for auditors to consider the impact on independence and ethics when operating their own node. In addition, see paragraph .07, "Operating Node Software on a Blockchain," in Q&A section 100, *Independence*, at the following link: http://pub.aicpa.org/codeofconduct/resourceseamlesslogin.aspx?prod=ethics&tdoc=et-qa&tptr=et-qa100

Operate own node

When the auditor operates its own node software to extract information directly from a public blockchain, considerations include the following, which are not intended to be all-inclusive:

- Additional software (or other tools) needed to transform the underlying blockchain data into a format that is easily queried to obtain relevant information (for example, transaction history for a particular public address)
- Additional technical expertise necessary to develop and maintain the associated infrastructure with respect to the underlying blockchain's protocols and related software
- Whether a node and the associated infrastructure are operating as intended, including whether
  - data inputs are complete and accurate;
  - the intended uses of the node and associated infrastructure are consistent with the purpose for which they were designed;
  - the outputs of the IT application achieve the purpose for which they will be used;
  - appropriate general IT controls surrounding the node and associated infrastructure, such as security, change management, and other general IT controls, have been designed, implemented, and tested for operating effectiveness on an ongoing basis; and
  - protocols and resources have been established to evaluate the appropriate operation of the node and appropriate investigation and resolution of issues, if identified.
- How to document the auditor's understanding of the technology used to obtain information (for example, the node and associated infrastructure) and the associated processes and controls used to evaluate whether the resulting information is relevant and reliable
- The different types of nodes available, as well as the functionality that each node provides on the blockchain

Engage a third party

An auditor may engage a third party that maintains a copy of the underlying blockchain data and provides access to software through which blockchain data can be obtained. Such software may be used by the auditor to query and process the data to obtain information recorded on the blockchain in a format useful for audit purposes. In such circumstances, the auditor may follow established firm protocols in assessing and reviewing vendors (for example, obtain approval through the audit firm's vendor management process) and evaluate the reliability of the information received from the vendor. If third-party software is used, the auditor may follow established firm protocols in assessing software used in the audit.

As part of evaluating the reliability of information provided by a third party,[5] the auditor may consider factors as mentioned previously (see "Operate own node" in this section) in considering whether the software, or node and associated infrastructure, performed as intended. To assess such factors, an auditor may consider obtaining and reading any available SOC reports and consider the type of SOC report and its relevance to the audit (for example, whether the SOC report addresses controls over the reliability of data such as control objectives related to the timeliness, accuracy, and completeness of the data sets obtained from the blockchain). See AU chapter 4, "Consideration of an entity's use of a service organization," of this practice aid. The auditor may also seek to understand whether the third party is in fact operating its own node or utilizing a subservice provider. If a SOC report is not available or if a SOC report exists but is not fit for purpose, the auditor should determine whether sufficient appropriate evidence is available from records held at the user entity. If sufficient appropriate evidence is not available from entity records, the auditor should perform further procedures to obtain sufficient appropriate audit evidence or use another auditor to perform those procedures at the service organization on the user auditor's behalf.[6]

[5] AU-C section 500, appendix A, "Considerations Regarding the Use of External Information Sources."

[6] Paragraph .15 of AU-C section 402, *Audit Considerations Relating to an Entity Using a Service Organization.*

In addition to reviewing available SOC reports, an auditor may also perform certain procedures over the information received from the third party (such as comparing the data provided from the third party to other sources of information available to the auditor) to evaluate its reliability.

Use free public blockchain explorer websites

There are several websites that allow public users to access information for certain blockchains free of cost. Although auditors may access information recorded on a blockchain from these websites, it may be difficult to evaluate the reliability of the information because, among other factors, the auditor typically does not have a commercial vendor relationship with the provider, and the websites typically do not obtain a SOC report. Because of this, the auditor is generally unable to obtain a sufficient understanding of how such websites obtain information from the blockchain and the processes and controls surrounding such information. As a result, information from free public blockchain explorer websites is generally less reliable than blockchain information accessed through the aforementioned methods.

Further, free public blockchain explorer websites may have other limitations that auditors may need to consider, such as the following:

- Inability to access historical data (for example, address balance), as some of these explorers typically provide historical data only for a limited period of time — In these instances, auditors may consider the impact on the timing of and ability to complete their audit procedures (for example, accessing information at the period-end date or multiple times throughout the period under audit).
- The transitory nature of the explorers, which may result in the need to consider what happens if the auditor uses an explorer that ceases to exist before the completion of the audit.
- Inability of free explorers to keep pace with changes to blockchain technology (for example, changes to a blockchain's code), resulting in observed instances of inaccuracy.
- Inability of free explorers to provide the level of detailed information needed to effectively perform audit procedures.
- Disclaimer provided by free explorers indicating the site takes no responsibility for the accuracy and completeness of the data. In these instances, auditors would consider the impact of the disclaimer on the auditor's ability to evaluate the reliability of the data obtained from the free explorer.

In some circumstances, an auditor may be able to evaluate the reliability of information obtained from blockchain explorer websites by obtaining an understanding of how certain free public blockchain explorer websites work (for example, reading available information on the blockchain explorer's websites and terms of service); understanding and evaluating whether information obtained from blockchain explorer websites is obtained from different nodes; comparing various data across multiple free blockchain explorer websites, considering whether they are consistent, complete and accurate (for example, comparing the transaction listing at a specific block height); and reconciling the activity in a given address across multiple blockchain explorer websites. In the event an auditor uses a free blockchain explorer, professional judgment is exercised to evaluate the reliability of the information obtained.

Audit procedures to address the existence and rights and obligations of digital assets held in self-custody

Question 3:

If an entity's digital assets are held in "self-custody," what procedures may be performed in response to risks of material misstatement identified in association with the existence of the digital assets and the entity's rights to the digital assets?

Response 3:

In some instances, an entity may have legal or contractual rights to digital assets and elect to hold and safeguard the private key(s) associated with its digital assets itself (that is, self-custody).

AU-C section 330, *Performing Audit Procedures in Response to Assessed Risks and Evaluating the Audit Evidence Obtained*, explains that the auditor is required to design and perform audit procedures whose nature, timing, and extent are based on, and responsive to, the assessed risks of material misstatement at the assertion level.[7]

The nature, timing, and extent of the procedures to be performed is a matter of professional judgment and depends on the specific facts and circumstances of the entity, including the auditor's understanding of the design, implementation, and, if necessary, operating effectiveness of the controls at the entity. (See AU chapter 2, "Risk assessment and processes and controls," of this practice aid, for further discussion and examples of controls over safeguarding and transacting digital assets and identification of risks of material misstatement.)

The auditor should design and perform tests of controls to obtain sufficient appropriate audit evidence about the operating effectiveness of controls if substantive procedures alone cannot provide sufficient appropriate audit evidence at the relevant assertion level.[8] The auditor may find it impossible to design effective substantive procedures that, by themselves, provide sufficient appropriate audit evidence at the relevant assertion level.[9] In such cases, in addition to substantive procedures, in accordance with paragraph .08*b* of AU-C section 330, the auditor should design and perform tests of controls (for example, testing private key management controls over digital asset safeguarding and access to private keys) to obtain sufficient appropriate audit evidence about the operating effectiveness of controls associated with digital assets. This may particularly be the case when the digital assets are commingled or when there is an assessed risk of material misstatement related to circumstances in which multiple parties have access to private keys and could potentially demonstrate "control" of the digital asset.

In addition, as discussed in AU-C section 315, *Understanding the Entity and Its Environment and Assessing the Risks of Material Misstatement,* if the auditor has determined that a significant risk exists, the auditor should identify controls that address such significant risk[10] and for each identified control, evaluate whether the control is designed effectively to address the risk of material misstatement at the assertion level or effectively designed to support the operation of other controls and determine whether the control has been implemented by performing procedures in addition to inquiry of the entity's personnel.[11]

[7] Paragraph .06 of AU-C section 330, *Performing Audit Procedures in Response to Assessed Risks and Evaluating the Audit Evidence Obtained.*

[8] Paragraph .08*b* of AU-C section 330.

[9] Paragraph .A25 of AU-C section 330.

[10] Paragraph .27 of AU-C section 315.

[11] Paragraph .30 of AU-C section 315.

Tests of controls

When planning audit procedures to obtain sufficient appropriate audit evidence regarding the existence of and rights to the digital assets, the auditor may consider testing the design and operating effectiveness of controls at the entity, including controls related to

- hardware and software procurement and deployment,
- initial generation of the private key,
- ongoing safeguarding of the private key,
- relevant service organizations, and
- general IT controls, including
  - controls over backups or other recovery mechanisms,
  - logical and/or physical access control around digital assets,
  - segregation of duties,
  - general IT controls with respect to the digital wallet software, and
  - cybersecurity.

This list of factors is not intended to be all-inclusive. If the auditor determines that sufficient appropriate audit evidence cannot be obtained, the auditor is required to consider the effect on the auditor's report (such as a scope limitation) in accordance with AU-C section 705, *Modifications to the Opinion in the Independent Auditor's Report.*

Substantive procedures

The following section includes substantive procedures that may be performed in some combination to address the risks related to the existence and rights and obligations assertions. It is important for the auditor to consider the timing of these procedures to obtain sufficient appropriate audit evidence as of the balance sheet date. For example, auditors may need to coordinate with management to perform digital asset transaction testing or message signing on the balance sheet date. The procedures described are not intended to be all-inclusive. Additional or different procedures may be more appropriate depending on the specific facts and circumstances, and often a combination of procedures is necessary to obtain sufficient appropriate audit evidence. Selecting the appropriate combination of procedures, which often includes tests of controls, is a matter of professional judgment.

Agreeing digital asset balances recorded by the entity to the blockchain

Substantive procedures may include agreeing the digital asset balances recorded by the entity to the blockchain. To support this procedure, it is important to evaluate the reliability of the information to be used as audit evidence that is obtained from the blockchain as discussed in Q&A 1, "Evaluating the reliability of information obtained from a blockchain," and Q&A 2, "Accessing information recorded on a blockchain," of this chapter.

Inspecting external information

Substantive procedures may include inspecting external information, such as cash movements or agreements with counterparties, to determine whether the transactions relate to the entity and provide evidence of the entity's rights to the digital assets. For example, the auditor may evaluate whether the cash movement indicates that the price paid for the digital assets is consistent with the market price at the time of the transaction (for example, within the day's high- and low-price range).

Digital asset transactions testing

An auditor may request and observe the entity initiate a digital asset transaction by sending a specified amount of digital assets between public addresses, as dictated by the auditor. This process requires the entity to initiate and digitally sign each transaction with the private key. Each transaction recorded on a blockchain is included within a block that contains details such as a cryptographic hash of the previous block, a timestamp, and transaction data. Once the transaction is completed and recorded on the blockchain, the auditor may inspect the blockchain for relevant details of the selected amount and date of the transfer using relevant tools.[12] This provides evidence of the entity's ability to initiate transactions from a specific public address at a point in time and, hence, the entity's access to the private key. However, this procedure does not address the risk of exclusive ownership (that is, the risk that multiple parties have access to the private keys, and that each party could claim to "control" the digital assets), which, if identified as a risk of material misstatement, would likely need to be addressed by the auditor by obtaining evidence about the effective design and operating effectiveness of the entity's private key management controls.

Signed messages

An auditor may request that the entity cryptographically sign a message to demonstrate access to the private key. This procedure involves the auditor providing a unique message to management (for example, Message20X1) or leveraging other messages (for example, messages signed using the private key as a part of the key-generation process). The entity then uses its private key to digitally sign the message. The signed message uses the same functionality that the entity would use to process on-chain transactions but does not need to be broadcast to the blockchain to be verified. The signed message is a unique string of letters and numbers (also known as a message digest or hash). The auditor may then independently obtain audit evidence as to the integrity of the signed message by determining the association between the signed message, the public address, and the original message (for example, Message20X1) using automated tools. This procedure provides audit evidence that the message was signed using the private key that is associated with a specific public address for a digital asset and, hence, management has access to the private key. However, this procedure does not address the risk of exclusive ownership (that is, the risk that multiple parties have access to the private keys, and that each party could claim to "control" the digital assets), which, if identified as a risk of material misstatement, would likely need to be addressed by the auditor by obtaining evidence about the effective design and operating effectiveness of the entity's private key management controls.

In obtaining audit evidence through the execution of digital asset transaction testing or signing messages, the auditor may observe entity personnel initiating the digital asset transaction on the blockchain or signing the message and providing the resulting details. Observation of management signing the message or initiating a transaction can provide additional audit evidence about the entity's process, also corroborating the auditor's understanding of certain private key management controls.

[12] When using tools to obtain information whether internally or externally sourced, it will be important for the auditor to document how they have evaluated that the tools have performed as intended. See Q&A 1, "Evaluating the reliability of information obtained from a blockchain," and Q&A 2, "Accessing information recorded on a blockchain," of this chapter.

Audit procedures to address the existence and rights and obligations of digital assets held by a third party

Question 4:

If an entity uses a third party (for example, a custodian or an exchange) to hold its digital assets, what procedures may be performed in response to risks of material misstatement identified in association with the existence of the digital assets and the entity's rights to the digital assets?

Response 4:

AU-C section 330, *Performing Audit Procedures in Response to Assessed Risks and Evaluating the Audit Evidence Obtained,* explains that the auditor is required to design and perform audit procedures whose nature, timing, and extent are based on, and responsive to, the assessed risks of material misstatement at the assertion level.[13]

The nature, timing, and extent of the procedures to be performed is a matter of professional judgment. In exercising professional judgment, auditors may, among other factors, consider the following:

- Whether a significant risk of material misstatement has been identified in association with the existence and/or the reporting entity's rights to digital assets
- Whether the digital assets are held in a segregated public address or a commingled public address
- The auditor's understanding of the design, implementation, and, if necessary, operating effectiveness of the controls at the third party and the entity in relation to digital assets (See AU chapter 4 and AU chapter 2 of this practice aid for further discussion and examples of controls over safeguarding and transacting digital assets and identification of risks of material misstatement.)

The auditor should design and perform tests of controls to obtain sufficient appropriate audit evidence about the operating effectiveness of controls if substantive procedures alone cannot provide sufficient appropriate audit evidence at the relevant assertion level.[14] The auditor may find it impossible to design effective substantive procedures that, by themselves, provide sufficient appropriate audit evidence at the relevant assertion level.[15] In such cases, in addition to substantive procedures, in accordance with paragraph .08*b* of AU-C section 330, the auditor should design and perform tests of controls (for example, testing private key management controls over digital asset safeguarding and access to private keys) to obtain sufficient appropriate audit evidence about the operating effectiveness of controls associated with digital assets. This may particularly be the case when the digital assets are commingled or when there is an assessed risk of material misstatement related to circumstances in which multiple parties have access to private keys and could potentially demonstrate "control" of the digital asset.

In addition, as discussed in AU-C section 315, if the auditor has determined that a significant risk exists, the auditor should identify controls that address such significant risk[16] and for each identified control, evaluate whether the control is designed effectively to address the risk of material misstatement at the assertion level or effectively designed to support the operation of other controls and determine whether the control has been implemented by performing procedures in addition to inquiry of the entity's personnel.[17]

[13] Paragraph .06 of AU-C section 330.

[14] Paragraph .08*b* of AU-C section 330.

[15] Paragraph .A25 of AU-C section 330.

[16] Paragraph .27 of AU-C section 315.

[17] Paragraph .30 of AU-C section 315.

Tests of controls

When planning audit procedures to obtain sufficient appropriate audit evidence regarding the existence of and rights to the digital assets, the auditor may consider the following:

- The design and operating effectiveness of controls at the third party, including controls related to private key management and transferring digital assets, segregation of assets, tracking the reporting entity's digital assets when such are held in commingled addresses, private key life cycle, and reconciliation of digital assets recorded on the blockchain to internal books and records (See AU chapter 4 of this practice aid.)
- The sufficiency of the SOC report (if available) for the user auditor's purposes
- The design and operating effectiveness of controls implemented by the entity to evaluate the reliability of the information obtained from the third party, including the reconciliation of the entity's independent digital asset transaction records and the third-party information
- The reliability and nature of audit evidence obtained from responses to confirmation requests received from the third party (See Q&A 5, "Digital asset third-party confirmation considerations," of this chapter.)
- Whether the third party is subject to external oversight or regulation (for example, as a qualified custodian under relevant jurisdictional regulations) or has certain fiduciary responsibilities[18]

This list of factors is not intended to be all-inclusive. If the auditor determines that sufficient appropriate audit evidence cannot be obtained, the auditor is required to consider the effect on the auditor's report (such as a scope limitation) in accordance with AU-C section 705. For example, this may be the case when the auditor determines it is necessary to test controls to obtain sufficient appropriate audit evidence and such controls are not appropriately designed and implemented or operating effectively.

Substantive procedures

The following table includes substantive procedures that may be performed in some combination to address the risks related to the existence and rights and obligations assertions.

Note: Due to the nature of digital assets held in a commingled public address (for example, the entity's digital assets are held in public addresses that also include the digital assets not owned by the reporting entity), an entity may see its individual account balances for each digital asset through the third party's interface, but it may not be transparent to the entity whether those digital assets exist on the blockchain. Therefore, the practice of commingling digital assets affects the auditor's ability to trace the entity's digital assets to the blockchain itself, as the blockchain no longer represents the entity's holdings alone. These scenarios may present risks of material misstatement related to the proper allocation of the digital assets that would likely need to be addressed by effective controls at the service organization. (See AU chapter 4 of this practice aid.) Procedures that may not be feasible when commingled public addresses are used are indicated as "N/A" in the following table.

[18] While external oversight or regulation over a third party may be considered to support the auditor's professional judgment and determination of planned procedures to obtain sufficient appropriate audit evidence, it is one factor among many. Therefore, the auditor may gather the same amount of evidence from a third party that is subject to external oversight or regulation or given certain fiduciary responsibilities as from a third party that is not subject to such oversight or regulations.

Substantive procedure	Segregated public address	Commingled public address
Obtaining and inspecting the custodial (or similar) agreement and obtaining an understanding of both the nature of the agreement and the types of digital assets held in custody. (See Q&A 10, "Recognition of digital assets when an entity uses a third-party hosted wallet service," in AC chapter 1, "Classification, measurement, and recognition," of this practice aid for factors to consider.)	X	X
Confirming with an appropriate third party regarding the existence of and rights to the digital assets and evaluating the reliability of the response. (See Q&A 5, "Digital asset third-party confirmation considerations," of this chapter for further details around information to confirm.)	X	X
Tracing and agreeing digital asset balances recorded by the entity directly to the blockchain.	X	N/A
Inspect the external blockchain for relevant details of the selected digital asset transaction, including the amount and date of the transfer using relevant tools.[19] The auditor may perform these procedures for transactions initiated upon request from the auditor (sending a specified amount of digital assets between public addresses) or for transactions initiated independently by the entity in the normal course of business.[20] This provides evidence of the entity's ability to direct the third party to initiate transactions from a specific address at a point in time and, hence, the entity's access to the private key via use of a third party. **Note:** This procedure does not address the risk of exclusive ownership (that is, the risk that multiple parties have access to the private keys, and that each party could claim to "control" the digital assets), which, if identified as a risk of material misstatement, would likely need to be addressed by the auditor by obtaining evidence about the effective design and operation of the private key management controls.	X	X (See AU chapter 4, "Consideration of an entity's use of a service organization," of this practice aid for additional considerations)

[19] When using tools to obtain information, whether internally or externally sourced, it will be important for the auditor to document how they have evaluated that the tools have performed as intended. See Q&A 1, "Evaluating the reliability of information obtained from a blockchain," and Q&A 2, "Accessing information recorded on a blockchain," of this chapter.

[20] For transactions initiated independently by the entity in the normal course of business, the auditor will need to obtain evidence of the entity directing the third party to initiate the transaction for the specified amount and on the specified date.

Substantive procedure	Segregated public address	Commingled public address
Requesting that the entity cryptographically sign a message to demonstrate access to the private key. The auditor may provide a unique message to management, and the entity then uses its private key to digitally sign the message. The signed message is a unique string of letters and numbers, and the auditor may independently confirm the integrity of the signed message by validating the association between the signed message, the public address, and the original message by using automated tools. **Note:** This procedure does not address the risk of exclusive ownership (that is, the risk that multiple parties have access to the private keys, and that each party could claim to "control" the digital assets), which, if identified as a risk of material misstatement, would likely need to be addressed by the auditor by obtaining evidence about the effective design and operation of private key management controls. Additionally, in certain instances, if the entity uses a third party who custodies the private key, operational limitations may prohibit the third party from signing messages using the private keys, and hence may reduce available substantive evidence to support the rights and obligations assertion.	X	N/A
Inspecting third-party custodian or exchange statements, bank statements, or other relevant documentation, tracing related transactions to the entity's internal books and records and evaluating the reliability of information obtained.	X	X

This list of procedures is not intended to be all-inclusive. Additional or different procedures may be appropriate depending on the specific facts and circumstances and, often, a combination of procedures is necessary to obtain sufficient appropriate audit evidence. Selecting the appropriate combination of procedures, which often includes testing third-party and complementary user entity controls, is a matter of professional judgment.

Digital asset third-party confirmation considerations

Question 5:

What are the considerations for sending digital asset confirmations to third parties that hold an entity's digital assets and evaluating the reliability of the responses?

Response 5:

When digital assets are held by a third party (for example, a custodian or an exchange), external confirmation procedures may be among the substantive procedures an auditor performs to obtain audit evidence over the existence of, and rights to, digital assets. However, confirmations alone likely do not provide sufficient appropriate audit evidence, and there are many considerations when evaluating the reliability of the confirmation responses.

Considerations related to the appropriateness and reliability of confirmations

Professional judgment is exercised by the auditor to determine if the use of external confirmation procedures is appropriate and if the response to a confirmation request is reliable.

Before deciding to send external confirmations, it is important for the auditor to identify the appropriate confirming party who the auditor believes is knowledgeable about the information to be confirmed. The auditor may read the relevant agreements (for example, custody agreements) to determine the appropriate party to confirm the type of digital asset (for example, BTC or ETH) and the reporting entity's rights to the digital assets and to understand the relationship and services being offered by the third party to the reporting entity (for example, the third party provides custody services to the entity and, therefore, is able to confirm existence of the digital assets).

In addition, paragraphs .A12–.A22 of AU-C section 505, *External Confirmations,* provide guidance on evaluating the reliability of responses to confirmation requests. The auditor may consider the following factors as a part of this evaluation:

- Whether the third party has a SOC report, the type of SOC report (for example, SOC 1 or SOC 2; type 1 or 2)
- How the content of the SOC report affects the auditor's evaluation of the reliability of the response
- The design and operating effectiveness of controls implemented by the entity to evaluate the reliability of the information obtained from the third party, including the reconciliation of the entity's independent digital asset transaction records and the third-party information
- Whether and how the third party is subject to external oversight or regulation (for example, as a qualified custodian under relevant jurisdictional regulations) or has certain fiduciary responsibilities
- Whether the third party's financial statements have been audited by a reputable audit firm that has demonstrated professional competence and independence
- The reputation and history of the third party (for example, the entity's history of cyberattacks or negative press that may lead the auditor to question the integrity of the respondent)

If the auditor identifies factors that give rise to doubts about the reliability of the response to a confirmation request, the auditor should obtain further audit evidence to resolve those doubts.[21] If the auditor determines that a response to a confirmation request is not reliable, the auditor should evaluate the implications on the assessment of the relevant risks of material misstatement, including risks of fraud, and on the related nature, timing, and extent of other audit procedures.[22]

[21] See paragraph .10 of AU-C section 505, *External Confirmations.*

[22] See paragraph .11 of AU-C section 505.

Information to confirm

Confirmation requests are tailored to the specific audit objective, and the auditor exercises professional judgment when considering information to confirm. In addition to confirming the balances of digital assets held by the third party on behalf of the entity, the auditor may also consider confirming the following:

- Whether any oral modifications or side arrangements exist other than agreements known to the auditor
- Whether the reporting entity's digital assets have been staked, assigned as collateral for borrowing or similar arrangements, or otherwise encumbered
- Whether the reporting entity's digital assets are held in commingled or segregated addresses
- Whether the third party carries insurance and, if so, the level and nature of the insurance
- Whether the third party has sole custody of the private key or whether the key is shared and only portions are kept with the entity or another third party
- Whether there have been any cybersecurity or other risk events that may have compromised the security of the private key(s) through the date of the confirmation
- The list of authorized individuals that have logical and/or physical access to digital assets at the reporting entity
- Digital asset balances in any accounts that may not be listed on the confirmation but pertain to the reporting entity
- The population of public addresses wherein the reporting entity's digital assets are stored (applicable to segregated addresses only)
- The number of wallets managed on behalf of the reporting entity by the third party across the third-party platform (for example, exchange wallets and custodian wallets) and the number of assets in each wallet
- Selected transaction details for all or a sample of transactions

This list of information to confirm is not intended to be all-inclusive. Additional or different types of information may be more appropriate depending on the specific facts and circumstances of the digital asset balances and transactions and the nature of the entity under audit.

Confirmation nonresponses or unreliable confirmation responses

If a response to a confirmation is not received[23] or if the response is incomplete or underlying details are not provided, the auditor should perform alternative audit procedures, which may include the procedures described in Q&A 4, "Audit procedures to address existence and rights and obligations of digital assets held by a third party," of this chapter, to obtain sufficient appropriate audit evidence over the existence of and rights to digital assets held by third parties. If the auditor determines that a response to a confirmation request is not reliable, the auditor should evaluate the implications on the assessment of relevant risks of material misstatement, including risks of fraud, and on the related nature, timing and extent of other audit procedures.[24] Although alternative procedures may be performed, alternative procedures may not provide sufficient appropriate audit evidence to respond to the risk(s) of material misstatement; in such circumstances, the auditor is required to determine the implications on the audit and the auditor's report.

[23] See paragraph .12 of AU-C section 505.

[24] See paragraph .11 of AU-C section 505.

AU Chapter 6: Considerations for valuation of digital assets

Note: When the auditor's assessment of risks of material misstatement at the relevant assertion level includes an expectation that the controls are operating effectively (that is, the auditor intends to rely on the operating effectiveness of controls in determining the nature, timing, and extent of substantive procedures), paragraph .08 of AU-C section 330, *Performing Audit Procedures in Response to Assessed Risks and Evaluating the Audit Evidence Obtained,* requires the auditor to design and perform tests of those controls to obtain sufficient appropriate audit evidence about the operating effectiveness of those controls.

In such circumstances, relevant controls to test may include (but are not limited to) the following:

- Controls around valuation, including how the entity determines the entity's principal market for each digital asset, which could include a periodic reassessment of its principal market — It is important for the auditor to evaluate the relevance and reliability of the data used in the analysis. For instance, this could include evaluating whether the pricing information is about the specific digital asset being measured[1] and whether the principal market has sufficient depth and liquidity.
- Controls over the entity's valuation methodology, including the valuation model, significant assumptions, underlying data used by management, and determining the level of digital assets' fair values for disclosure purposes.
- Controls over measuring and recognizing realized/unrealized gains and losses, including how the entity
  - tracks the individual carrying values of digital assets sold (for example, FIFO)
  - determines digital asset fair value for purposes of measuring gain and loss activity on exchanges for other digital assets (for example, the exchange of bitcoin for ether).
- Controls over timing of impairment of indefinite-lived out-of-scope crypto intangible assets (for example, controls over use of appropriate price when preparing impairment analyses).
- General IT controls associated to any relevant systems and technology-based tools (for example, blockchain explorer tools).

See AC chapter 4, "Fair value measurement," of this practice aid for accounting considerations for digital assets that require fair value measurement. In addition, see section D, "Digital asset valuation," in AU chapter 2 of this practice aid for an overview of unique attributes of digital assets, which often make valuation more complex.

[1] For instance, a token developed by the same group of developers may be deployed on multiple blockchains. In other cases, two tokens may share the same "ticker" abbreviation; this circumstance could be purely coincidental, but it might also arise when bad actors attempt to "spoof" a legitimate token.

Measuring digital assets using prices in active markets

Question 1:

What procedures might an auditor consider if an entity measures its digital asset[2] using prices in active markets that it determines to be the principal market?

Response 1:

When an entity measures its digital assets using prices in active markets, the auditor may consider the following procedures:

- Evaluating the entity's policy for determining the fair value of digital assets, including whether the policy is in accordance with FASB ASC 820, *Fair Value Measurement*
- Understanding the market(s) in which the entity normally transacts (for example, whether the digital asset has an active market and whether the market prices, volume, and other data are reliable)
- Independently obtaining prices directly from the entity's principal market or testing management's process for obtaining such prices. If such prices are obtained indirectly (that is, through a third-party intermediary data source), procedures to evaluate such prices would be focused on the relevance and reliability of the information, including its source — For instance, the auditor may consider whether these sources provide reliable information about market activity, including both prices and trade volumes. In addition, it is important for the auditor to consider whether the data source provides the correct time in accordance with management's accounting policy and whether the data source provides historical information at sufficient granularity.[3] (For additional information related to continuously operating markets, see Q&A 20 in AC chapter 4, "Fair value measurement," of this practice aid.)
- Evaluating the entity's policy to monitor transactions that take place after the cut-off time but before the end of the reporting period. (For additional information related to cut-off time for determine fair value of digital assets, see Q&A 20 in AC chapter 4 of this practice aid.)
- If fair value measurement, including the analysis of principal market, is facilitated by the entity's use of a service organization, understanding the services provided, including the third-party price provider's methodology, processes, and controls. This might include an evaluation of any SOC or similar control reports provided by the third party. For additional information, see AU chapter 4, "Consideration of an entity's use of a service organization," of this practice aid.

[2] Refer to the definition of *digital asset* in the Blockchain Universal Glossary.

[3] Some data sources sunset certain data after a period of time. If a data source does not maintain historical data at sufficient granularity, an auditor may need to perform testing closer to the reporting period.

Measuring digital assets that are thinly traded

Question 2:

What procedures might an auditor consider when an entity measures the fair value of digital assets that are thinly traded (for example, in nonactive markets)?

Response 2:

When an entity measures its digital assets that are thinly traded, the auditor may consider the following:

- Evaluating the entity's policy for determining the fair value of digital assets, assessing whether it is in accordance with FASB ASC 820, *Fair Value Measurement*, and understanding the market(s) in which the entity normally transacts
- Obtaining and evaluating the entity's analysis of its principal (**or most advantageous**) market
- Understanding, evaluating, and testing the entity's valuation methodology, including the valuation model, significant assumptions, and underlying data used by management
- Obtaining and evaluating the entity's assessment of whether the market for identical or comparable digital assets is active or not, including market depth and liquidity

Note: Auditors may face challenges in performing this procedure given the nature of most digital assets. It may be difficult to conclude that two digital assets are sufficiently comparable in the context of applying FASB ASC 820.

- Evaluating whether reported trades are orderly and whether or not they involve related parties
- Evaluating the reasonableness of assumptions, which may include adjustments made to transaction prices
- Independently obtaining prices for identical or comparable digital assets if any (see previous Note) — If such prices are obtained indirectly (for example, through a third-party intermediary data source), it is important for the auditor to establish a basis for reliance on that source.
- Developing its own fair value estimate or reviewing subsequent events or transactions occurring prior to the date of the auditor's report.
- If fair value measurement, including the analysis of principal market, is facilitated by a third party, obtain an understanding of the third party's methodology, processes, and controls. This might include an evaluation of any SOC or similar control reports provided by the third party.

The auditor should consider whether specialized skills are needed in performing the audit.[4] If expertise in a field other than accounting or auditing is necessary to obtain sufficient appropriate audit evidence, the auditor should determine whether to use the work of an auditor's specialist[5] such as a valuation specialist. For example, specialists may be involved when relevant observable market data (that is, benchmark assets, information related to relevant underlying operations or collateral if any) is not available and fair value is estimated using another valuation technique based on the assumptions that market participant would make.

[4] Paragraph .12 of AU-C section 300, *Planning an Audit.*

[5] Paragraph .07 of AU-C section 620, *Using the Work of an Auditor's Specialist.*

Considerations for evaluating an entity's impairment analysis for indefinite-lived out-of-scope crypto intangible assets

Question 3:

What are some key audit considerations for evaluating an entity's impairment analysis for indefinite-lived out-of-scope crypto intangible assets?[6]

Response 3:

In accordance with FASB ASC 350-30-35-15, intangible assets with an indefinite useful life are not subject to amortization. Rather, FASB ASC 350-30-35-18 provides they should be tested for impairment annually, and more frequently if events or changes in circumstances indicate that it is more likely than not that the asset is impaired. Consistent with FASB ASC 350-30-35-19, if the carrying amount of an indefinite-lived intangible asset exceeds its fair value, an entity should recognize an impairment loss in an amount equal to that excess. (See Q&A 4 in AC chapter 1, "Classification, measurement, and recognition," of this practice aid.) Unlike other intangible assets, indefinite-lived out-of-scope crypto intangible assets may trade in active, liquid markets that are almost always open. Therefore, the impairment analysis for indefinite-lived out-of-scope crypto intangible assets poses challenges, related to both the frequency and timing of the impairment analysis, as well as the determination of the unit of account for impairment testing. The following are audit considerations for evaluating the entity's impairment analysis for indefinite-lived out-of-scope crypto intangible assets:

Frequency and timing of impairment analysis:

- Entities are responsible for establishing, implementing, and maintaining processes and controls to monitor triggering events (for example, fair value being lower than cost) that may be a result of micro- or macro-economic factors such as market conditions that can cause a drop in value of the indefinite-lived out-of-scope crypto intangible asset, liquidity restrictions with limited options to liquidate the asset, absence of active markets, and so on. To identify and assess risks of material misstatement, auditors typically obtain an understanding of the entity's policies and procedures to monitor triggering events for reasonableness and consistency in application across other similar indefinite-lived intangible assets.
- Such understanding typically takes into account whether the entity has a policy for assessing triggering events throughout the reporting period as opposed to only performing an analysis based on the asset's fair value on the reporting date, such that the entity identifies the lowest value of the indefinite-lived out-of-scope crypto intangible asset throughout the holding period, and not just the value as of the period-end.
- Because many indefinite-lived out-of-scope crypto intangible assets trade in markets that are almost always open, the impairment analysis may need to consider trading information throughout the day, every day (including weekends and holidays).

[6] Refer to the definition of *crypto intangible asset* in Q&A 1 of AC chapter 1 of this practice aid.

Determination of unit of account for impairment testing:

- The cost basis of batches of an indefinite-lived out-of-scope crypto intangible asset purchased on different dates and times and at different prices cannot be combined for impairment analysis.[7] Audit procedures to evaluate the reporting entity's policies for determining the unit of account may include understanding and testing the entity's approach to tracking the carrying value and acquisition date and time of the indefinite-lived out-of-scope crypto intangible assets acquired in various separate or individual transactions, including how this is factored into the impairment analysis.
- Additionally, audit procedures typically include testing the accuracy of the cost basis and evaluating the reliability of the source of the fair value information.

[7] Each fractional tranche of the indefinite-lived out-of-scope crypto intangible asset acquired is treated as a unit of account for impairment testing. See Q&A 7 of AC chapter 1 for guidance on how an entity should determine the unit of account when assessing impairment of indefinite-lived out-of-scope crypto intangible asset holdings.

Considerations for an entity that recognizes realized gains and losses on sales of digital assets

Question 4:

What audit considerations might be relevant for an entity that recognizes realized gains or losses on sales (or exchanges) of digital assets?

Response 4:

Entities that sell or exchange digital assets recognize realized gains or losses equal to the difference between each asset's carrying value and the respective proceeds from sale. Measuring realized gains or losses at the unit of account level may involve tracking and analyzing multiple digital assets acquired on different dates and at different prices.[8] When an entity sells or exchanges its digital assets, an auditor may consider performing the following:

- Understanding the characteristics of the population to determine the nature and extent of audit procedures necessary to obtain sufficient appropriate audit evidence. For example, auditors may consider:
  - Whether variability in the size and type of transactions that give rise to realized gains or losses may require that the auditor disaggregate the transactions into separate populations (for example, sales for fiat currency versus crypto-for-crypto exchanges) for purposes of risk assessment or designing further audit procedures
  - The volume of transactions to determine the method of selecting items for substantive procedures (that is, statistical/nonstatistical sampling, selecting key items, or 100% examination). — For example, when an entity routinely trades digital assets (with a high volume of sales activities), the auditor may determine that designing and performing tests of details via audit sampling would provide sufficient appropriate audit evidence.
- For each transaction selected for tests of details, an auditor may perform the following:
  - Trace and agree the digital asset transaction recorded by the entity directly to the blockchain or to relevant and reliable source evidence[9] if the transactions are not recorded directly to the blockchain[10] (for example, if the transaction is off-chain and, thus, does not result in a transfer of digital assets between two blockchain addresses)
  - Inspect the delivery or receipt of fiat currency, digital assets, other assets, or services received in the exchange to source documentation
  - Confirm the transaction with the counterparty

[8] Consistent with FASB ASC 350-30-35-24, because entities can usually sell or otherwise dispose of each unit or a divisible fraction of a unit of a digital asset separately from any other units (for example, bitcoin [BTC] or fractional units of BTC purchased in different periods at different prices), the individual unit (or a divisible fraction of a unit) typically represents the unit of account for purposes of measuring realized gains or losses. See Q&A 7 of AC chapter 1 of this practice aid for guidance on how an entity should determine the unit of account for digital asset holdings accounted for as an indefinite-lived intangible asset.

[9] See AU chapter 5, "Considerations for existence, rights, and obligations of digital assets," of this practice aid.

[10] See Q&A 2, "Accessing information recorded on a blockchain," in AU chapter 5 of this practice aid.

- In addition, auditors may consider the following procedures for gains or losses recognized on the exchange of digital assets for fiat currency, other digital assets, or other assets or services:
  - Fiat currency — Tracing cash receipt(s) into a roll-forward of the respective account and confirming the year-end cash balance
  - Other digital assets — Obtaining fair value information directly from the entity's principal (or most advantageous) market or indirectly through a reliable third-party intermediary data source
  - Other assets or services — Obtaining evidence to support the existence of and rights to assets or services received in exchange for digital assets — For instance, if an entity purchases mining hardware from a third party and pays for the purchase with digital assets, the auditor could obtain evidence that the mining hardware was received by the entity and that the entity has title to the hardware. An auditor might also consider testing the fair value of the assets or services received if such values are more readily available and, therefore, more appropriate in measuring the transaction.

AU Chapter 7: Considerations for crypto intangible asset lending and borrowing

Note: When the auditor's assessment of risks of material misstatement at the relevant assertion level includes an expectation that the controls are operating effectively (that is, the auditor plans to test the operating effectiveness of controls in determining the nature, timing, and extent of substantive procedures), paragraph .08 of AU-C section 330, *Performing Audit Procedures in Response to Assessed Risks and Evaluating the Audit Evidence Obtained,* requires the auditor to design and perform tests of those controls to obtain sufficient appropriate audit evidence about the operating effectiveness of those controls.

In such circumstances, relevant controls to test may include (but are not limited to) the following:

- Controls with respect to contract reviews in accordance with the entity's established accounting policy
- Controls regarding crypto intangible asset payments and receipts
- Controls over the determination of the allowance for credit losses
- Controls over the entity's valuation methodology for crypto intangible asset loan receivables and any embedded derivatives, including the valuation model, significant assumptions, underlying data used by management, and determining the level in the fair value hierarchy for disclosure purposes
- General IT controls associated with any relevant systems and technology-based tools (for example, blockchain explorer or other analytical tools)

The tables in this chapter provide examples of substantive procedures that could address risks of material misstatement associated with crypto intangible asset lending and borrowing transactions, some of which are similar to substantive procedures that address similar risks associated with fiat lending and borrowing transactions. These procedures are not intended to be all-inclusive. Additional or different procedures may be appropriate depending on the specific facts and circumstances; often, a combination of procedures is necessary to obtain sufficient appropriate audit evidence. In all cases, the auditor is required to evaluate the relevance and reliability of information to be used as audit evidence in accordance with AU-C section 500, *Audit Evidence,* and other relevant AU-C sections, including information such as statements and confirmations obtained from third parties.

The auditor may find it impossible to design effective substantive procedures that, by themselves, provide sufficient appropriate audit evidence at the relevant assertion level.[1] In such cases, in addition to substantive procedures, in accordance with paragraph .08*b* of AU-C section 330, the auditor should design and perform tests of controls to obtain sufficient appropriate audit evidence about the operating effectiveness of certain controls over crypto intangible asset lending and borrowing.

In addition, in forming a conclusion on whether sufficient appropriate audit evidence has been obtained, the auditor should consider all relevant audit evidence, regardless of whether it appears to corroborate or contradict the assertions in the financial statements. If the auditor has not obtained sufficient appropriate audit evidence about a relevant assertion, the auditor should attempt to obtain further audit evidence in accordance with paragraph .29 of AU-C section 330. If the auditor determines that sufficient appropriate audit evidence cannot be obtained, the auditor is required to consider the effect on the auditor's report (such as a scope limitation) in accordance with AU-C section 705, *Modifications to the Opinion in the Independent Auditor's Report.*[2]

[1] Paragraph .A25 of AU-C section 330, *Performing Audit Procedures in Response to Assessed Risks and Evaluating the Audit Evidence Obtained.*

[2] Paragraphs .28–29 of AU-C section 330.

Crypto intangible asset lending and borrowing with no collateral

Question 1:

Assume a lender lends 100 units of a crypto intangible asset (Crypto Intangible Asset ABC) for a term of one (1) year to a borrower. The borrower will pay a fee in total of 12 units of Crypto Intangible Asset ABC for borrowing Crypto Intangible Asset ABC during the 12-month loan period, paying one unit of Crypto Intangible Asset ABC each month in arrears during the term (typically referred to as "interest payment" in the agreement). At the end of 12 months, the borrower is required to deliver 100 units of Crypto Intangible Asset ABC back to the lender. For purposes of the Q&A, assume the following:

- Crypto Intangible Asset ABC is an intangible asset under FASB ASC 350, *Intangibles — Goodwill and Other.*
- Upon transfer of the loaned Crypto Intangible Asset ABC to the borrower, the borrower has the right to transfer, encumber, or pledge the crypto intangible asset in any way it chooses.
- The borrower is not required to post collateral to the lender in the arrangement.
- The borrower has identified its functional currency as the U.S. dollar under FASB ASC 830, *Foreign Currency Matters*.
- The lender originates and manages a portfolio of such loans as part of its business activities.

What substantive procedures may address risks of material misstatement associated with these crypto intangible asset lending and borrowing transactions?

Note: For accounting considerations on the previous scenario, see Q&A 25 in AC chapter 7, "Crypto intangible asset lending and borrowing," of this practice aid.

Response 1:

To determine appropriate substantive procedures, it is helpful to understand how the loan is funded, as that may impact the nature and source of the evidence available.

Two scenarios for how the loan is funded are considered as follows:

- Scenario 1: On-chain borrowing transaction — Crypto Intangible Asset ABC is transferred from the lender's crypto intangible asset public address to the borrower's crypto intangible asset public address.
- Scenario 2: Off-chain borrowing transaction — Crypto Intangible Asset ABC is transferred between the lender's account and the borrower's account on the same crypto intangible asset exchange with no corresponding on-chain transfer.

The following are potential audit procedures that may be performed when auditing crypto intangible asset loans receivable and the associated income of a lender based on the auditor's identification and assessment of risks of material misstatement.

Lender	
Substantive audit procedure	**Assertions addressed**
Procedures applicable to both scenarios 1 and 2	
Obtain a roll-forward schedule of crypto intangible asset loans receivable and perform the following procedures: • Recalculate the mathematical accuracy of the roll-forward schedule. • Agree the opening balances[3] to the prior period audited roll-forward schedule and the crypto intangible assets loan receivable subledger. • Agree the ending balances to the crypto intangible asset loans receivable subledger. • Reconcile each roll-forward component included in the roll-forward schedule (for example, loan repayments, loan drawdown, fee accruals, and changes in the fair value of the lent crypto intangible assets) to underlying substantive testing procedure results, such as loan confirmations, vouching loan disbursements and repayments, fee calculations, fair value testing, etc. **Note:** See the following for examples of substantive procedures testing for each component.	Completeness Accuracy Existence
Obtain a reconciliation of the crypto intangible asset loans receivable subledger to the general ledger for related balances as of period-end. Evaluate whether reconciling items have been subsequently resolved in an appropriate and timely manner.	Accuracy Completeness
Make inquiries of management regarding crypto intangible asset lending, inspect minutes of board of directors and other relevant committee meetings, and inspect other relevant documentation to determine whether crypto intangible asset lending included in the roll-forward schedule is complete.	Completeness
Agree the units borrowed by each counterparty selected as part of lending fee detail testing to the lending activity roll-forward to verify that the assets loaned are properly included in the lending roll-forward.	Completeness

[3] The auditor should consider guidance in AU-C section 510, *Opening Balances – Initial Audit Engagements, Including Reaudit Engagements,* if the auditor has not audited the entity in the prior year.

Obtain and inspect the executed agreements (including subsequent modifications to the agreements, if any) between the borrower and the lender (the lending agreement), and trace activity details per the roll-forward (where applicable) to the lending agreements.	Existence Rights and obligations Completeness Presentation
Obtain and inspect the entity's lending agreements (including subsequent modifications to the agreements, if any) to evaluate whether the entity's documented accounting conclusions are appropriate.	Presentation
Send a loan confirmation request directly to the borrower to confirm information such as balances, key terms based on the loan agreements and statements (for example, crypto intangible asset type, loan fee percent, loan fee payments, frequency of loan fee settlement, loan date, maturity date), and the existence of any other agreements between the borrower and the entity that are not included in the confirmation request. Perform alternative procedures for confirmations with no written responses. Alternative procedures may include examination of subsequent activities.	Existence Accuracy Completeness Rights and obligations
Recalculate the fee income and vouch the data used in the calculation to relevant and reliable evidence, such as the corresponding lending agreement and/or confirmation.	Accuracy Occurrence
Perform procedures over the valuation of lent crypto intangible assets. (See AU chapter 6, "Considerations for valuation of digital assets," of this practice aid.)	Valuation
Obtain and assess the lender's evaluation of allowance for credit losses that incorporates forecasts reflecting the lender's expectation of credit losses related to the crypto intangible asset loan receivable, utilizing the principles in FASB ASC 326, *Financial Instruments — Credit Losses.*	Valuation
Evaluate the completeness and accuracy of the financial statement presentation (including current or noncurrent presentation) and disclosures (including, for example, loan disclosures, credit loss disclosures, related party disclosures, risks and uncertainties disclosures, fair value disclosures, and commitment disclosures, if applicable).	Presentation
Evaluate the cash flow statement for proper disclosure in noncash activities; for example, income earned.	Presentation

Procedures applicable to scenario 1 only	
Vouch the loan disbursement(s) from the lender to the borrower to Crypto Intangible Asset ABC blockchain; use an appropriate reciprocal population (for example, transactions with a receiving address used solely for lending activity), if available, for testing the loan activity per the roll-forward; and reconcile the loan disbursement amount to the loan confirmation received from the borrower or applicable agreement(s).	Existence Accuracy Rights and obligations Completeness
Vouch the borrower's payments of Crypto Intangible Assets ABC borrowed and fees to Crypto Intangible Asset ABC blockchain and reconcile the payment amount to the loan confirmation received from the borrower and applicable agreement(s).	Existence Accuracy
Procedures applicable to scenario 2 only	
Vouch the loan disbursement(s) amount from the lender to the borrower to exchange transaction statements; use an appropriate reciprocal population (for example, transactions with a receiving address used solely for lending activity), if available, for testing the loan activity per the roll-forward; and reconcile the loan disbursement amount to the loan confirmation received from the borrower and applicable agreement(s).	Existence Accuracy Rights and obligations Completeness
Vouch the borrower's payments of Crypto Intangible Assets ABC borrowed and fees to exchange transaction statements and reconcile the payment amount to the loan confirmation received from the borrower and applicable agreement(s).	Existence Accuracy

The following are potential audit procedures that may be performed when auditing the liability recognized by the borrower.

Borrower	
Substantive audit procedure	**Assertions addressed**
Procedures applicable to both scenarios 1 and 2	
Obtain a roll-forward schedule of the obligation to return Crypto Intangible Asset ABC and perform the following procedures: • Recalculate the mathematical accuracy of the roll-forward schedule. • Agree the opening balances[4] to the prior period audited roll-forward schedule and the crypto intangible asset borrowing payable subledger. • Agree the ending balances to the crypto intangible asset borrowing payable subledger. • Reconcile each component of activity in the roll-forward schedule (for example, Crypto Intangible Asset ABC returned, additional borrowing of Crypto Intangible Asset ABC) to underlying substantive testing procedure results, such as vouching loan disbursement from the lender to the borrower, the borrower's return of crypto intangible assets borrowed, fee calculations, etc. **Note:** See the following for examples of substantive procedures testing for each component.	Completeness Accuracy Existence
Obtain a reconciliation of the crypto intangible asset borrowings payable subledger to the general ledger for related balances as of period-end. Evaluate whether reconciling items have been subsequently resolved in an appropriate and timely manner.	Accuracy Completeness
Make inquiries of management regarding crypto intangible asset borrowing, inspect minutes of board of directors and other relevant committee meetings, and inspect other relevant documentation to determine whether crypto intangible asset borrowing included in the roll-forward schedule is complete.	Completeness
Obtain and inspect the executed agreement(s) (including subsequent modifications to the agreement, if any) between the borrower and the lender (the borrower agreement), and trace activity details per the roll-forward (where applicable) to the borrower agreement.	Rights and obligations Completeness Presentation

[4] The auditor should consider guidance in AU-C section 510 if the auditor has not audited the entity in the prior year.

Obtain and inspect the entity's borrowing agreements (including subsequent modifications to the agreement, if any) to evaluate whether the entity's accounting conclusions are appropriate.	Presentation
Send a confirmation directly to the lender, which confirms information such as balances, key terms based on the loan agreements and statements (for example, crypto intangible asset type, loan fee percent, loan fee payments, frequency of loan fee settlement, loan date, maturity date), and the existence of any other agreements between the lender and the entity that are not included in the confirmation request. Perform alternative procedures for confirmations with no written responses. Alternative procedures may include examination of subsequent activities.	Existence Accuracy Completeness Rights and obligations
Recalculate the fee and vouch the data used in the calculation to relevant and reliable evidence, such as the corresponding agreement(s).	Accuracy Occurrence
Perform audit procedures over valuation of embedded derivative. (See AU chapter 6 of this practice aid.)	Valuation
Inspect management's documentation detailing compliance with terms and covenants (if any) in the agreement. If applicable, obtain specific written management representation related to debt agreement compliance. Perform procedures over covenants to determine whether any have been violated.	Presentation
Evaluate the completeness and accuracy of financial statement presentation (including current or noncurrent presentation) and disclosure of the obligation to return Crypto Intangible Asset ABC.	Presentation
Determine completeness and accuracy of disclosures, including, for example, disclosure on the obligation to return Crypto Intangible Asset ABC, related party disclosure, or derivative disclosures.	Presentation
Evaluate the cash flow statement for proper disclosure in noncash financing activities, including fees associated with the borrowing.	Presentation

Procedures applicable to scenario 1 only	
Vouch the loan disbursement(s) from the lender to the borrower to Crypto Intangible Asset ABC blockchain; use an appropriate reciprocal population (for example, transactions with a receiving address used solely for lending activity), if available, for testing the borrowing activity per the roll-forward, and reconcile the loan disbursement amount to the confirmation received from the lender or applicable agreement(s).	Existence Accuracy Completeness
Vouch the borrower's return of Crypto Intangible Assets ABC borrowed and fees to Crypto Intangible Asset ABC blockchain and reconcile loan payment amount to the confirmation received from the lender and applicable agreement(s).	Existence Accuracy
Procedures applicable to scenario 2 only	
Vouch the loan disbursement(s) from the lender to the borrower to crypto intangible asset exchange transaction statements; use an appropriate reciprocal population (for example, transactions with a receiving address used solely for lending activity), if available, for testing the borrowing activity per the roll-forward; and reconcile the loan disbursement amount to the confirmation received from the lender and applicable agreement(s).	Existence Accuracy Completeness
Vouch the borrower's return of crypto intangible assets borrowed and fees to crypto intangible asset exchange transaction statements and reconcile loan payment amount to the confirmation received from the lender and applicable agreement(s).	Existence Accuracy

Crypto intangible asset lending and borrowing with collateral

Question 2:

Assume the same facts as Q&A 1, with the addition that the borrower was required to post collateral for Crypto Intangible Asset ABC. For purposes of this Q&A, we also assume the following:

- The borrower is required to post initial collateral in the form of Crypto Intangible Asset XYZ with a value of at least 115% of the value of borrowed Crypto Intangible Asset ABC.
- The borrower is required to post additional collateral to meet the minimum 115% collateral value requirement if the fair value of the posted collateral falls below 110% of the value of borrowed Crypto Intangible Asset ABC.
- Both Crypto Intangible Asset ABC and XYZ are accounted for as intangible assets under FASB ASC 350.
- For some loans, the lender recognizes collateral on its balance sheet; and for other loans, the borrower continues to recognize the collateral on its balance sheet.

What substantive procedures may address risks of material misstatement associated with these crypto intangible asset lending and borrowing transactions?

Response 2:

To determine appropriate substantive procedures, it is helpful to understand how the collateral is posted. Two scenarios for how the collateral is posted are considered as follows:

- Scenario 1: On-chain collateral transaction — Crypto Intangible Asset XYZ is transferred from the borrower's crypto intangible asset public address to the lender's crypto intangible asset public address.
- Scenario 2: Off-chain collateral transaction — Crypto Intangible Asset XYZ is transferred from the borrower's account to the lender's account on the same crypto intangible asset exchange with no corresponding on-chain transfer.

The following are potential audit procedures that may be performed related to the posted collateral based on the auditor's identification and assessment of risks of material misstatement.

Lender (that is, the recipient of the posted collateral)	
Substantive audit procedure	**Assertions addressed**
Obtain the entity's accounting analysis and evaluate for consistency and compliance with GAAP regarding whether to recognize the collateral on the lender's balance sheet. Inspect evidence relating to the contractual or other legal rights of the lender related to the collateral and evaluate whether this is consistent with the entity's accounting analysis.	Accuracy Rights and obligations Presentation
Compare the collateral posted to collateral requirements per loan agreement(s) (including subsequent modifications to the agreement, if any) as of period-end to determine if sufficient collateral was posted.	Accuracy
Perform audit procedures over valuation of collateral assets and embedded derivative related to the obligation to return the collateral. (See AU chapter 6 of this practice aid.)	Valuation
Perform audit procedures over the existence, rights, and obligation of the crypto intangible assets received as collateral. (See AU chapter 5 of this practice aid.)	Existence Rights and obligations
Send a confirmation request directly to the borrower to confirm collateral information (for example, collateral requirements, collateral type, number of units). Perform alternative procedures for confirmations with no written responses. Alternative procedures may include examination of subsequent activities.	Existence Completeness Accuracy Rights and obligations
Evaluate the completeness and accuracy of disclosures related to collateral.	Presentation

Procedures applicable to scenario 1 only	
Vouch the collateral disbursement from the borrower to the lender to Crypto Intangible Asset XYZ blockchain and reconcile the collateral disbursement amount to the loan confirmation received from the borrower and applicable agreement(s).	Existence Accuracy
Vouch the return of collateral from the lender to the borrower to Crypto Intangible Asset XYZ blockchain and reconcile the return of collateral amount to the loan confirmation received from the borrower and applicable agreement(s) (including subsequent modifications to the agreement, if any).	Existence Accuracy
Procedures applicable to scenario 2 only	
Vouch the collateral disbursement from the borrower to the lender to exchange transaction statements and reconcile the collateral disbursement amount to the loan confirmation received from the borrower and applicable agreement(s).	Existence Accuracy
Vouch the return of collateral from the lender to the borrower to exchange transaction statements and reconcile the return of collateral amount to the loan confirmation received from the borrower and applicable agreement(s) (including subsequent modifications to the agreement, if any).	Existence Accuracy
Procedures applicable when the lender uses a third party-hosted wallet service (that is, custodian) and applicable to both scenarios 1 and 2	
Obtain and evaluate the entity's accounting analysis regarding whether the collateral should be recognized on the financial statements of the lender or the custodian. (See Q&A 10 in AC chapter 1, "Classification, measurement, and recognition," of this practice aid.)	Accuracy Presentation

Borrower (that is, the collateral poster)	
Substantive audit procedure	**Assertions addressed**
Obtain the entity's accounting analysis and evaluate for consistency and compliance with GAAP, including whether to derecognize the collateral on the borrower's balance sheet. Inspect evidence relating to the contractual or other legal rights of the borrower related to the collateral and assess whether this is consistent with the entity's accounting analysis.	Accuracy Rights and Obligations Presentation
Compare the collateral posted to the collateral requirements per the loan agreement(s) (including subsequent modifications to the agreement, if any) as of period-end to determine if sufficient collateral was posted.	Accuracy
Perform audit procedures over valuation of collateral posted related to the obligation to return the collateral. (See AU chapter 6 of this practice aid.)	Valuation
Send a confirmation request directly to the lender to confirm collateral information (for example, collateral requirements, collateral type, number of units). Perform alternative procedures for confirmations with no written responses. Alternative procedures may include examination of subsequent activities.	Existence Completeness Accuracy Rights and obligations
Evaluate the completeness and accuracy of disclosures related to collateral.	Presentation

Procedures applicable to scenario 1 only	
Vouch the collateral disbursement from the borrower to the lender to Crypto Intangible Asset XYZ blockchain and reconcile the collateral disbursement amount to the loan confirmation received from the lender and applicable agreement(s) (including subsequent modifications to the agreement, if any).	Existence Accuracy
Vouch the return of collateral from the lender to the borrower to Crypto Intangible Asset XYZ blockchain and reconcile the returned collateral amount to the confirmation received from the lender and applicable agreement(s).	Existence Accuracy
Procedures applicable to scenario 2 only	
Vouch the collateral disbursement from the borrower to the lender to the exchange transaction statements and reconcile the collateral disbursement amount to the confirmation received from the lender and applicable agreement(s) (including subsequent modifications to the agreement, if any).	Existence Accuracy
Vouch the return of collateral from the lender to the borrower to the exchange transaction statements and reconcile the returned collateral amount to the confirmation received from the lender and applicable agreement(s).	Existence Accuracy
Procedures applicable when the borrower uses a third-party hosted wallet service (that is, custodian) and applicable to both scenarios 1 and 2	
Obtain and evaluate the entity's accounting analysis and evaluate for consistency and compliance with GAAP, including whether the collateral should be recognized on the financial statements of the borrower or the custodian. (See Q&A 10 in AC chapter 1 of this practice aid.)	Accuracy Presentation

Appendix A

Blockchain Universal Glossary

Appendix B

SEC Staff Accounting Bulletin No. 121 Questions and Answers

NOTE: On January 30, 2025, SEC Staff Accounting Bulletin (SAB) No. 122 was published in the Federal Register and became effective. SAB No. 122 rescinds SAB No. 121, *Accounting for Obligations to Safeguard Crypto-Assets an Entity Holds for its Platform Users* (that is, Topic 5.FF).

As stated in SAB No. 122, upon application of the rescission of Topic 5.FF, an entity that has an obligation to safeguard crypto-assets for others should determine whether to recognize a liability related to the risk of loss under such an obligation, and if so, the measurement of such a liability, by applying the recognition and measurement requirements for liabilities arising from contingencies in Financial Accounting Standards Board Accounting Standards Codification ("FASB ASC") Subtopic 450-20, *Loss Contingencies,* or International Accounting Standard ("IAS") 37, *Provisions, Contingent Liabilities and Contingent Assets* under U.S. generally accepted accounting principles and IFRS Accounting Standards, respectively. Entities should effect the rescission of Topic 5.FF on a fully retrospective basis in annual periods beginning after December 15, 2024. Entities may elect to effect the rescission in any earlier interim or annual financial statement period included in filings with the Commission after the effective date of this SAB. Entities should include clear disclosure of the effects of a change in accounting principle upon initial application of this rescission.

Entities should refer to FASB ASC 250, *Accounting Changes and Error Corrections* for guidance and disclosure requirements for changes in accounting principle.

Introduction and background:

On March 31, 2022, the SEC staff released Staff Accounting Bulletin No. 121 (SAB No. 121), which expresses the staff's views on how an entity that has an obligation to safeguard "crypto-assets"[1] for another party should account for that obligation. The SEC staff believes these safeguarding arrangements "involve unique risks and uncertainties not present in arrangements to safeguard assets that are not crypto-assets, including technological, legal, and regulatory risks and uncertainties." The SEC staff further believes the guidance in SAB No. 121 "will enhance the information received by investors and other users of financial statements about these risks, thereby assisting them in making investment and other capital allocation decisions."

Under SAB No. 121, an entity with a safeguarding obligation recognizes a safeguarding liability with an accompanying safeguarding asset, both initially measured at the fair value[2] of the safeguarded "crypto-assets." SAB No. 121 also discusses certain quantitative and qualitative information the staff would expect to see disclosed, both inside and outside the financial statements, about the safeguarding obligation.

[1] The use of the term *crypto-assets* in this appendix is based on the definition used in SEC Staff Accounting Bulletin No. 121 (SAB No. 121).

[2] See Q&As 16–21 in AC chapter 4, "Fair value measurement," of this practice aid for more detailed discussion of the fair value accounting considerations related to digital assets.

Accounting Questions and Answers

The following questions and answers (Q&As) focus on interpretive matters arising from SAB No. 121 based on recent discussions with the SEC staff:

Question 1:

SAB No. 121 discusses the accounting for entities that have obligations to safeguard “crypto-assets.” What does the SAB No. 121 definition of a “crypto-asset” include?

Response 1:

Footnote 3 of SAB No. 121 explains that “[f]or purposes of this SAB, the term ‘crypto-asset’ refers to a digital asset that is issued and/or transferred using distributed ledger or blockchain technology using cryptographic techniques.” As used in SAB No. 121, the term “crypto-asset” includes, but is not limited to, crypto intangible assets (as defined in Q&A 1 in AC chapter 1, “Classification, measurement, and recognition,” of this practice aid), stablecoins (see Q&As 22 and 23 in AC chapter 5, "Stablecoins," of this practice aid), nonfungible tokens (NFTs), and other tokens (collectively similar to “digital assets” as used in the practice aid.)

Some “crypto-assets” can have differences that may warrant further analysis to determine if they are in scope of SAB No. 121. For example, “crypto-assets” on a public permissionless blockchain likely present many of the risks outlined in SAB No. 121. However, “crypto-assets” on a private permissioned blockchain may not contain those same risks and may be out of the scope of SAB No. 121 if, for example, the ability to amend, correct, or cancel transactions exists. Consultation with your professional adviser or the SEC is recommended for such fact patterns.

Question 2:

Must all the risks identified in SAB No. 121 be present for an entity to have an obligation to safeguard “crypto-assets”?

Response 2:

No. Although SAB No. 121 references various risks — technological, legal, and regulatory — that can arise from an entity’s arrangement to safeguard “crypto-assets,” there is no requirement for all the risks to be present for an entity to have an obligation to safeguard the “crypto-assets.” In addition, the risks referenced in SAB No. 121 are not all-inclusive; therefore, entities should also consider whether their “crypto-asset” safeguarding activities give rise to other types of risks or uncertainties that indicate a safeguarding obligation exists under SAB No. 121.

Question 3:

Must an entity operate a platform to be subject to the potential recognition of a safeguarding liability?

Response 3:

No. Although SAB No. 121 uses the example of an entity that “safeguard[s] crypto-assets held for [its] platform users,” an entity need not operate a platform to be subject to recognition of a safeguarding liability.

Question 4:

If an entity determines that it controls "crypto-assets," and therefore recognizes them on its balance sheet, must the entity also recognize a safeguarding liability under SAB No. 121?

Response 4:

No. When an entity concludes that it controls "crypto-assets" (see Q&A 10 in AC chapter 1 of this practice aid), SAB No. 121 does not apply because the "crypto-assets" are recognized on the entity's balance sheet and treated as its own assets. Consequently, the entity would not record a liability to safeguard its own assets under SAB No. 121.

Question 5:

If an entity only provides wallet software tools to a customer whereby the customer generates and controls the private key information, would the entity's transaction with the customer give rise to a safeguarding obligation within the scope of SAB No. 121?

Response 5:

No. If the entity only provides software tools to the customer, who then generates and controls the private key information, the transaction does not give rise to a safeguarding obligation.

Question 6:

Could two entities recognize a safeguarding liability and safeguarding asset for the same "crypto-asset" being safeguarded?

Response 6:

Yes. All entities that conclude they have an obligation to safeguard the "crypto-assets" of a third party must recognize a safeguarding liability and a safeguarding asset in accordance with SAB No. 121. For example, a custodian of a third party's "crypto-assets" may, as part of its custodial relationship, engage a sub-custodian. In such cases, both the custodian and the sub-custodian might conclude they have a safeguarding obligation and therefore need to recognize a safeguarding asset and safeguarding liability for the safeguarding of the same population of "crypto-assets" regardless of which entity holds the private key information.

Question 7:

How does an entity determine if it has a safeguarding obligation to a third party, either directly or through an agent and, therefore, must recognize a safeguarding liability and a safeguarding asset under SAB No. 121? (See Q&A 10 of this appendix for information specific to broker dealers and Q&A 11 in this appendix for information specific to regulated banks and savings institution.)

Response 7:

The determination of whether an entity is responsible for safeguarding "crypto-assets" will depend on the totality of the facts and circumstances, including consideration of the involvement of the entity's agents and other third parties. The following should all be considered and, depending on the facts and circumstances, may *individually or in combination* suggest a safeguarding obligation exists (this list is not intended to be exhaustive):

- The nature of the entity's involvement (including that of its agents) with the safeguarded assets.
- The entity's level of involvement (including that of its agents) with the safeguarded assets.
- The contractual terms of the arrangement with the third party whose assets are being safeguarded.
- The contractual terms of any arrangement between the entity and other parties involved in the safeguarding of the assets.
- The perception of the third parties whose "crypto-assets" are being safeguarded. For example, would the third party believe the entity is responsible for safeguarding the "crypto-assets"?
- The degree to which the entity can transact in the "crypto-assets" without the involvement of other parties (for example, move them between wallets).
- The level of involvement the entity has in handling complaints and resolving disputes.
- The entity's involvement with recordkeeping, including whether the entity knows the public key information or balances, or both of "crypto-assets" safeguarded for third parties.
- The degree of the entity's involvement with transactions involving the safeguarded "crypto-assets," including who controls the flow of transactions.

Question 8:

How are changes in the fair value measurement[3] of the safeguarding liability and safeguarding asset recognized under SAB No. 121 presented in an entity's statement of operations?

Response 8:

SAB No. 121 explains that the safeguarding liability is measured "at each reporting date at the fair value of the crypto-asset that [the entity] is responsible for." The safeguarding asset is measured at "each reporting date at the fair value of the crypto-assets held…." The changes in the fair value of the safeguarding liability and the safeguarding asset can be presented in the same line item in the statement of operations. When the changes in the fair value of the safeguarding liability and safeguarding asset are the same in a reporting period, there would be no net effect in the statement of operations. If, however, an entity incurs a loss on the safeguarding asset (for example, "crypto-assets" held for third parties are lost), then any difference between the change in the fair value of the safeguarding liability and safeguarding asset would be reflected in the entity's statement of operations, and accordingly, would not net to zero.

[3] See Q&As 16–21 in AC chapter 4 of this practice aid for more detailed discussion of the fair value accounting considerations related to digital assets.

Question 9:

When an entity's financial statements are filed with the SEC in accordance with Rule 3-09 and Rule 3-05 of Regulation S-X, are those financial statements subject to SAB No. 121?

Response 9:

Yes. Although SAB No. 121 does not specifically reference these entities, the financial statements thereof are subject to SAB No. 121.

Question 10:

Are broker-dealers subject to SAB No. 121 and, if so, are there any special considerations for such entities when determining if they have a safeguarding obligation?

Response 10:

Yes. Although SAB No. 121 does not specifically reference these entities, the financial statements thereof are subject to SAB No. 121. Like all other entities, the facts and circumstances of the entity's digital assets activities will determine if it is required to record a safeguarding liability (and related asset) under SAB No. 121 (see Q&A 7 of this appendix for considerations).

At the February 2024 AICPA Stockbrokerage and Investment Banking Expert Panel meeting and September 2024 AICPA & CIMA Conference on Banks & Savings Institutions, members of the SEC staff from the Office of the Chief Accountant shared facts about certain SAB No. 121 broker-dealer consultations, in which the SEC staff did not object to the broker-dealer not recording a safeguarding liability. When evaluating whether arrangements that involve digital assets give rise to a safeguarding obligation, broker-dealers may find it useful to consider highlights from the February 2024 meeting and the remarks of SEC Chief Accountant Paul Munter at the Banks & Savings Institutions conference.

Question 11:

Are there any special considerations for regulated banks and savings institutions related to SAB No. 121 when determining if they have a safeguarding obligation?

Response 11:

Yes. When evaluating whether arrangements that involve digital assets give rise to a safeguarding obligation, regulated banks and savings institutions may find it useful to consider the remarks of SEC Chief Accountant Paul Munter at the September 2024 AICPA & CIMA Conference on Banks & Savings Institutions.

Auditing Question and Answer

The following Q&A provides potential procedures that the auditor may perform when designing and performing procedures in response to risks of material misstatement associated with SAB No. 121.

NOTE:

Independence and Ethics — The topic in this section of the practice aid focus on auditing applications and do not address ethics considerations, including those related to independence. It is important to note, however, that these considerations remain critical to an auditor's performance of the engagement in conformity with professional standards, and engagements in the digital asset ecosystem may introduce new or different compliance risks warranting additional consideration by the auditor.

For information regarding independence requirements and ethics responsibilities, see the AICPA Code of Professional Conduct at pub.aicpa.org/codeofconduct/Ethics.aspx.

In addition, see paragraph .07, "Operating Node Software on a Blockchain," in Q&A section 100, *Independence,* at the following link:

http://pub.aicpa.org/codeofconduct/resourceseamlesslogin.aspx?prod=ethics&tdoc=et-qa&tptr=et-qa100

Risk of Material Misstatement Due to Fraud — For entities in the digital asset ecosystem, the Q&As herein do not contemplate all potential risks of material misstatement, including all potential fraud risks. AU-C section 240, *Consideration of Fraud in a Financial Statement Audit,* includes further requirements regarding procedures to identify and respond to fraud risks.

Risks of material misstatement due to fraud may be present, and the auditor should identify and assess such risks at the financial statement level and at the assertion level for classes of transactions, account balances, and disclosures.[4,5] See AU chapter 2 of this practice aid for factors to consider when identifying and assessing risks of material misstatement, including those that may be significant risks due to error or fraud.

Obtaining Sufficient Appropriate Audit Evidence — Planning further audit procedures that are responsive to risks of material misstatement requires the exercise of professional judgment. Further audit procedures may include both tests of controls and substantive procedures. Substantive procedures alone may not provide sufficient appropriate audit evidence (for example, ownership of digital assets). As stated in paragraph .08 of AU-C section 330, *Performing Audit Procedures in Response to Assessed Risks and Evaluating the Audit Evidence Obtained,* the auditor should design and perform tests of controls to obtain sufficient appropriate audit evidence about the operating effectiveness of relevant controls if (*a*) the auditor's assessment of risks of material misstatement at the relevant assertion level includes an expectation that the controls are operating effectively (that is, the auditor intends to rely on the operating effectiveness of controls in determining the nature, timing, and extent of substantive procedures) or (*b*) substantive procedures alone cannot provide sufficient appropriate audit evidence at the relevant assertion level.

[4] Paragraph .26 of AU-C section 315, *Understanding the Entity and Its Environment and Assessing the Risks of Material Misstatement.*

[5] Paragraph .25 of AU-C section 240, *Consideration of Fraud in a Financial Statement Audit.*

The auditor may find it impossible to design effective substantive procedures that, by themselves, provide sufficient appropriate audit evidence at the relevant assertion level. This may occur when an entity conducts its business using IT and no documentation of transactions is produced or maintained, other than through the IT system. In such cases, paragraph .08*b* of AU-C section 330 requires the auditor to perform tests of relevant controls.[6]

The auditor may often conclude that a combination of tests of controls (for example, private key management controls) and substantive procedures is needed to obtain sufficient appropriate audit evidence to address the risks of material misstatement associated with digital assets. Due to these considerations and challenges associated with digital assets, it will be important for auditors to carefully evaluate, exercising professional judgment, whether sufficient appropriate audit evidence has been obtained to address the risks of material misstatement.

SEC Staff Accounting Bulletin No. 122 — On January 30, 2025, SEC Staff Accounting Bulletin (SAB) No. 122 was published in the Federal Register. SAB No. 122 rescinds SAB No. 121, *Accounting for Obligations to Safeguard Crypto-Assets an Entity Holds for its Platform Users* (that is, Topic 5.FF). As stated in SAB No. 122:

> Upon application of the rescission of Topic 5.FF, an entity that has an obligation to safeguard crypto-assets for others should determine whether to recognize a liability related to the risk of loss under such an obligation, and if so, the measurement of such a liability, by applying the recognition and measurement requirements for liabilities arising from contingencies in Financial Accounting Standards Board Accounting Standards Codification ("FASB ASC") Subtopic 450-20, *Loss Contingencies*, or International Accounting Standard ("IAS") 37, *Provisions, Contingent Liabilities and Contingent Assets* under U.S. generally accepted accounting principles and IFRS Accounting Standards, respectively. Entities should effect the rescission of Topic 5.FF on a fully retrospective basis in annual periods beginning after December 15, 2024. Entities may elect to effect the rescission in any earlier interim or annual financial statement period included in filings with the Commission after the effective date of this SAB. Entities should include clear disclosure of the effects of a change in accounting principle upon initial application of this rescission.

It is important for auditors to obtain an understanding of the effects of the recission of SAB No. 121 on an entity's financial statements and assess related risks that need to be addressed. Depending on specific facts and circumstances, considerations may include, but are not limited to, risks related to:

- Management's evaluation of the risk of loss related to the obligation to safeguard digital assets for others in accordance with FASB ASC 450, *Contingencies*
- Disclosure requirements for a change in accounting principle (FASB ASC 250, *Accounting Changes and Error Corrections*)
- Any other required additional disclosures

[6] Paragraph .A25 of AU-C section 330, *Performing Audit Procedures in Response to Assessed Risks and Evaluating the Audit Evidence Obtained.*

Question 1:

What procedures may be performed in response to identified risks of material misstatement associated with safeguarding liabilities and safeguarding assets recorded in accordance with SAB No. 121?

Response 1:

AU-C section 330, *Performing Audit Procedures in Response to Assessed Risks and Evaluating the Audit Evidence Obtained,* explains that the auditor is required to design and perform audit procedures whose nature, timing, and extent are based on, and responsive to, the assessed risks of material misstatement at the assertion level.[7]

The nature, timing, and extent of the procedures to be performed is a matter of professional judgment. In exercising professional judgment, auditors may consider, among other factors, the design, implementation and, if planned or otherwise required, the operating effectiveness of controls, including controls associated with service organizations (for example, sub-custodians or other third parties).

The auditor should design and perform tests of controls to obtain sufficient appropriate audit evidence about the operating effectiveness of controls if substantive procedures alone cannot provide sufficient appropriate audit evidence at the relevant assertion level.[8] The auditor may find it impossible to design effective substantive procedures that, by themselves, provide sufficient appropriate audit evidence at the relevant assertion level.[9] In such cases, in addition to substantive procedures, in accordance with paragraph .08b of AU-C section 330, the auditor should design and perform tests of controls to obtain sufficient appropriate audit evidence about the operating effectiveness of controls associated with safeguarding liabilities and safeguarding assets.

In addition, as discussed in AU-C section 315, *Understanding the Entity and Its Environment and Assessing the Risks of Material Misstatement,* if the auditor determined that a significant risk exists, the auditor should identify controls that address such significant risk[10] and for each identified control, evaluate whether the control is designed effectively to address the risk of material misstatement at the assertion level or effectively designed to support the operation of other controls and determine whether the control has been implemented by performing procedures in addition to inquiry of the entity's personnel.[11]

Note: Designing procedures that are responsive to risks of material misstatement associated with the fair value of safeguarding assets and safeguarding liabilities are outside the scope of this Q&A.

[7] Paragraph .06 of AU-C section 330

[8] Paragraph .08*b* of AU-C section 330.

[9] Paragraph .A25 of AU-C section 330.

[10] Paragraph .27 of AU-C section 315.

[11] Paragraph .30 of AU-C section 315.

Tests of controls

When planning audit procedures to obtain sufficient appropriate audit evidence regarding safeguarding liabilities and safeguarding assets, the auditor may consider the design and operating effectiveness of controls at the entity, including the following:

- Reconciliation of digital assets held on behalf of others that give rise to a safeguarding liability between the blockchain and internal books and records
- Controls over customer digital asset deposits and withdrawals (for example, transaction authorization controls, controls to validate those transactions executed in relation to digital assets held on behalf of others have been appropriately authorized)
- Controls over cash received and disbursed associated with customer purchases and sales
- Private key management controls
- If digital assets within the scope of SAB No. 121 are maintained in commingled addresses with other digital assets, controls over tracking and determining the amount of digital assets that are subject to SAB No. 121 and those that are not, in order to determine appropriate financial statement classification (for example, auditors may test controls over the entity's internal systems used to record customer account balances)
- If the entity engages a service organization (for example, a sub-custodian), controls implemented by such service organizations and relevant complementary user entity controls
- Controls over management's identification and evaluation of potential loss events (for example, transaction-monitoring controls implemented to identify unusual activity associated with digital assets held on behalf of others)
- Controls that allow the entity to fulfill commitments/obligations made to customers in accordance with the terms of the contract

Refer to the section "Understanding the entity's processes and controls" in AU chapter 2, "Risk assessment and processes and controls," and AU chapter 4, "Considerations of an entity's use of a service organization," of this practice aid for additional considerations surrounding relevant controls.

This list of factors is not intended to be all-inclusive. If the auditor determines that sufficient appropriate audit evidence cannot be obtained, the auditor is required to consider the effect on the auditor's report (such as a scope limitation) in accordance with AU-C section 705, *Modifications to the Opinion in the Independent Auditor's Report.* For example, this may be the case when the auditor determines it is necessary to test controls to obtain sufficient appropriate audit evidence and such controls are not appropriately designed and implemented or operating effectively.

In accordance with SAB No. 121, the safeguarding asset and safeguarding liability should be measured at the fair value of the underlying digital asset held on behalf of others. The measurement of the safeguarding asset would also factor in any potential loss events.

Substantive procedures

The following substantive procedures may be performed, in some combination, to address identified risks of material misstatement associated with safeguarding liabilities and safeguarding assets. The practice of commingling digital assets affects the auditor's ability to directly trace the digital assets to the blockchain because the blockchain address no longer includes the balance of digital assets held on behalf of others alone. These scenarios may present risks of material misstatement related to the proper allocation of the digital assets that would likely need to be addressed by effective controls. As such, obtaining an understanding of whether the entity or, if applicable, the service organization engaged by the entity holds digital assets in commingled wallets or addresses is relevant to identifying and assessing the risks of material misstatements.

The following audit procedures are not intended to be all-inclusive. Additional or different procedures may be appropriate depending on the specific facts and circumstances and, often, a combination of procedures is necessary to obtain sufficient appropriate audit evidence. Auditors may also consider involving specialists (for example, engaging cryptography and cybersecurity specialists) to respond to risks of material misstatement associated with safeguarding liabilities and safeguarding assets.

- Obtaining and evaluating management's accounting analysis and reviewing relevant contracts to determine if the entity has appropriately identified safeguarding obligations to a third party, either directly or through an agent. In evaluating management's analysis, auditors may consider the factors in Accounting Q&A 7 of this appendix.
- Inquiring of those charged with governance, management, or others (for example, regulatory, compliance, IT, and legal departments) regarding their knowledge of arrangements whereby the entity has an obligation to safeguard digital assets on behalf of others.[12]
- Inspecting relevant evidence (for example, board of director and audit committee meetings minutes, custodial agreements, marketing materials, or websites) for indications of assets held on behalf of others that may not be included in management's analysis.
- Tracing and agreeing the balance of digital assets subject to SAB No. 121 as recorded by the entity directly to the blockchain — In circumstances where digital assets that are subject to SAB No. 121 are held in commingled addresses with digital assets outside the scope of SAB No. 121, the auditor may agree the total balance of digital assets held in commingled addresses to the blockchain; however, additional procedures would need to be performed to test the tracking of digital assets subject to SAB No. 121 as described in the procedure following.
- Testing management's records used to track and determine the amount of digital assets held on behalf of others that give rise to a safeguarding liability and the amount of digital assets outside the scope of SAB No. 121[13] — For example, the auditor may test the entity's internal record of customer digital asset balances (in units) and entity digital asset balances, which has been agreed, in total, to the blockchain. In completing this procedure, auditors may also evaluate proper presentation of assets in the financial statements.
- If the auditor has used information from a blockchain as audit evidence, evaluate the reliability of such information. (See Q&A 1, "Evaluating the reliability of information obtained from a blockchain," in AU chapter 5, "Considerations for existence, rights, and obligations of digital assets," of this practice aid)
- Confirming digital asset balances with the appropriate party for whom the entity holds or has held digital assets. In addition to confirming the balance of digital assets held by the entity on behalf of the counterparty, the auditor may also confirm the terms and conditions of existing agreements with the counterparty, including the existence of any side agreements.[14]
- Inspecting documents supporting the subsequent movement of digital assets held on behalf of others that may indicate authorization by the appropriate counterparty, such as cash, contracts or agreements, and invoices.
- Inspecting counterparty onboarding documentation associated with safeguarding liabilities, such as documentation collected as a part of the entity's KYC and other due diligence procedures to validate existence of safeguarding liabilities.
- Tracing and agreeing selections made from a reciprocal population (for example, population of customers to which asset safeguarding services are provided, or population of revenue transactions recorded in association with providing custodial services) into the underlying details of safeguarding liability and asset balance to validate proper inclusion or exclusion thereof.

[12] In accordance with paragraph .A63 of AU-C section 500, *Audit Evidence,* responses to inquiries may provide a basis for the auditor to modify or perform additional audit procedures.

[13] This procedure is relevant only in circumstances when digital assets are commingled.

[14] In some circumstances, such as confirmations with retail customers, the auditor may have previously experienced low response rates to confirmation requests. In such circumstances, to obtain relevant and reliable audit evidence, the auditor may decide not to perform confirmation procedures and instead perform a combination of other substantive procedures. The nature of the alternative procedures which may be performed is dependent upon the facts and circumstances of the engagement.

AICPA®

The American Institute of CPAs, powering leaders in accounting and finance around the globe