PCAOB
PUBLIC COMPANY ACCOUNTING OVERSIGHT BOARD

SPOTLIGHT

Inspection Observations Related to Public Company Audits Involving Crypto Assets

June 2023

CONTENTS

OVERVIEW

This Spotlight highlights certain responsibilities under PCAOB standards for auditors of public companies and brokers and dealers[1] transacting in or holding crypto assets,[2] our inspection observations related to crypto assets, and important reminders for auditors when performing audits of public companies or broker-dealers, where activities associated with crypto assets are material to the financial statements. Specifically, these reminders include an emphasis on the importance of performing tests of controls and substantive procedures that are responsive to the assessed risks of material misstatement identified, consideration of the public company's or broker-dealer's relationships and transactions with its related parties, and application of professional skepticism when evaluating potential risk of material misstatement due to error or fraud.

One of the PCAOB's organizational priorities is to have our inspection program use a data-driven and risk-based approach that focuses on riskier engagements and audit areas.[3] The Division of Registration and Inspections ("we") recognizes that the use of crypto assets presents unique audit risks to public companies and broker-dealers and requires an appropriate risk assessment and audit response by audit firms. We have been monitoring developments in the crypto industry and the audit-related implications.

Activities associated with crypto assets may involve heightened risks to investors, public companies, and broker-dealers, including (but not limited to) high levels of volatility, lack of transparency of parties engaging in transactions and the purpose of such transactions, market manipulation, fraud, theft, scams, and significant legal uncertainties.

In this Spotlight, the term "crypto asset" refers to an asset secured through cryptography that resides on a distributed ledger based on blockchain technology. Crypto assets include but are not limited to "virtual currencies," "coins," or "tokens."[4]

A public company's (or broker-dealer's) involvement with crypto assets can be multifaceted. For example, activities associated with crypto assets that have been observed through our inspections included:

- Earning a fee, or "reward," for validating new blocks on a distributed ledger (which for some crypto assets, such as Bitcoin, is commonly known as "mining");
- Purchasing or selling goods or services in exchange for crypto assets;
- Exchanging one crypto asset for another;
- Purchasing or selling crypto assets in exchange for a fiat currency,[5] such as the U.S. dollar;
- Providing trading services to third parties, such as operating a platform that allows its users to transact in crypto assets;
- Acting as an intermediary, such as between a customer and a trading platform or mining operation;
- Investing in crypto assets; and/or
- Safeguarding crypto assets held for its users.

[1] This Spotlight does not highlight broker-dealer specific considerations for auditors of broker-dealers. However, many of the topics discussed in this Spotlight apply to audits of broker-dealers.

[2] This Spotlight does not address any other applications of distributed ledger technology.

[3] Please refer to PCAOB Strategic Plan 2022-2026 for more information on our strategic objectives.

[4] This Spotlight does not specifically address so-called "stablecoins," which, unlike other types of crypto assets, purport to use some means to stabilize their price relative to another asset (e.g., by reference to a fiat currency).

[5] In this Spotlight, the term "fiat currency" refers to a type of currency that is declared legal tender by a government.

In addition, transactions associated with crypto assets have certain unique technological risks – such as lack of governance mechanisms establishing oversight of crypto asset activities and markets – and vulnerabilities related to cyber-attacks, outages, lost assets, and illicit finance. Recent bankruptcies and financial distress among crypto asset market participants, including the collapse of crypto asset trading platform FTX, have caused significant disruptions in crypto markets and exposed the structural vulnerability of some business models involving crypto assets.

INSPECTION OBSERVATIONS

In fulfilling the PCAOB's mission to protect investors, since 2017 we have been reviewing audits of public companies where transactions or holdings involving crypto assets were material to the financial statements. During 2023, our target team will focus on emerging audit risks associated with crypto assets. In 2020, the PCAOB issued a Spotlight – "**Audits Involving Cryptoassets: Information for Auditors and Audit Committees**" – to highlight considerations for addressing responsibilities under PCAOB standards for auditors of public companies transacting in or holding crypto assets. This Spotlight is an update informed by our subsequent observations.

Inspection Activity

We have reviewed audits of public companies with material or significant crypto asset activities. These public companies were mostly engaged in holding crypto assets or crypto asset mining activities. We have identified deficiencies where the auditor did not perform procedures to evaluate the sufficiency and appropriateness of audit evidence obtained over the existence, valuation, and the rights and obligations of crypto assets recorded at year end.

We have also identified deficiencies where the auditor did not perform sufficient procedures to test the occurrence and valuation of revenue related to crypto asset mining activities, and in some instances, assess the appropriateness of revenue recognition related to crypto assets. Observations from these inspections indicate the need for a greater focus by auditors on the identification and assessment of the risks of material misstatement to the financial statements associated with crypto assets and related activities, as well as designing and implementing an appropriate audit response. We issued comment forms to audit firms where we identified deficiencies from our inspections.

We will continue to focus on identifying public companies that have material crypto asset holdings and/or significant activity related to crypto assets, placing emphasis on relevant focus areas and assertions related to the existence, occurrence, valuation, rights and obligations, and presentation and disclosure of crypto assets.

Inspection Findings

We have identified the following common audit deficiencies related to crypto assets:

Fraud and Significant Unusual Transactions

We have identified deficiencies where the auditor may have identified activities associated with crypto assets but did not take into account whether such activities were significant transactions outside the normal course of business for the public company or otherwise unusual due to their timing, size, or nature ("significant unusual transactions").

Key Consideration

It is important for auditors to be aware that significant transactions associated with crypto assets may represent significant unusual transactions as described above. Significant unusual transactions

may be used to engage in fraudulent financial reporting or conceal misappropriation of assets.

Auditor's Responsibilities

AS 2401, *Consideration of Fraud in a Financial Statement Audit* ("AS 2401"), states that the auditor's identification of significant unusual transactions should take into account information obtained from: (a) the risk assessment procedures (e.g., inquiring of management and others, obtaining an understanding of the methods used to account for significant unusual transactions, and obtaining an understanding of internal control over financial reporting) and (b) other procedures performed during the audit (e.g., reading minutes of the board of directors meetings and performing journal entry testing).

In addition, auditors are required to design and perform procedures to obtain an understanding of the business purpose (or the lack thereof) of each significant unusual transaction that the auditor has identified.

Further, AS 2401 states that the auditor should evaluate whether the business purpose (or the lack thereof) for significant unusual transactions indicates that the transactions may have been entered into to engage in fraudulent financial reporting or conceal misappropriation of assets.

The auditor should also take into account information that indicates that related parties or relationships or transactions with related parties previously undisclosed to the auditor might exist when identifying significant unusual transactions.

Recommended Actions to Execute Responsibilities Under PCAOB Standards

It is important that the auditor consider whether a public company's activities associated with crypto assets represent significant transactions that are outside the normal course of business for the public company or that otherwise appear to be unusual due to their timing, size, or nature. When the auditor has identified a transaction associated with crypto assets as a significant unusual transaction, the auditor should also design and perform procedures to obtain an understanding of the business purpose of each significant unusual transaction the auditor has identified. Further, the auditor should evaluate whether the business purpose indicates that the significant unusual transaction may have been entered into to engage in fraudulent activities. For example, it is important that the auditor evaluates whether patterns relating to the timing, size, or nature of activities associated with crypto assets indicate that the transactions may have been entered to engage in fraud (e.g., existence of unusually high activity with public addresses[6] during the year, converting substantial amounts of fiat currencies into crypto assets without a reasonable business purpose, significant activities including transactions with related parties involving multiple crypto assets or multiple public addresses with no logical business explanation, or significant transactions on platforms that offer crypto asset mixing services to obfuscate crypto asset ownership).

Ownership of Crypto Assets

We have identified deficiencies where an auditor did not:

- Appropriately assess the risk of material misstatement related to the rights and obligations assertion of crypto assets because the auditor did not obtain a sufficient understanding of the related controls over crypto assets.
- Perform any procedures to establish that the public company has control over the crypto assets to support the rights and obligations assertion.

[6] In this Spotlight, the term "public address" refers to a unique identifier which is used to record receipts of crypto assets on a public distributed ledger. Distributed ledger addresses are derived from hashing (that is, a cryptographic process used to convert data into a string of numbers and letters) of the public key and can be shared with anyone to receive messages.

Key Considerations

- **Ownership** – Addressing a risk of material misstatement to the rights and obligations assertion relating to crypto assets may involve performing procedures that are different from procedures that are performed for other types of assets because of the pseudo-anonymity (i.e., concealing an account holder's real identity behind an alphanumeric code) of the transacting parties on public distributed ledgers.
- **Third-party confirmations** – Certain applications of distributed ledger technology can eliminate the need for a central third party (e.g., a bank) for the completion of transactions. Correspondingly, audit evidence traditionally obtained from these central third parties surrounding the rights and obligations of assets (e.g., third-party confirmations) may not be available.
- **Fraud** – The potential for material misstatement due to fraud may include, for example:
  - The risk of fraud due to the risk that multiple parties can access the same crypto assets. In addition, other entities or individuals including related parties may maintain a private key[7] associated with the public address that contains a public company's crypto assets. For example, a third-party crypto asset custodian may inappropriately record customer-owned crypto asset balances as its own.
  - The risk of management override of controls over private keys, which may result in misuse or misappropriation of crypto assets by those who control the private keys.

Auditor's Responsibilities

AS 2110, *Identifying and Assessing Risks of Material Misstatement* ("AS 2110"), states that the auditor should perform risk assessment procedures that are sufficient to provide a reasonable basis for identifying and assessing the risks of material misstatement, whether due to error or fraud, and designing further audit procedures. In performing the risk assessment procedures, the auditor should obtain a sufficient understanding of each component of internal control over financial reporting to (a) identify the types of potential misstatements, (b) assess the factors that affect the risks of material misstatement, and (c) design further audit procedures.

AS 2301, *The Auditor's Responses to the Risks of Material Misstatement* ("AS 2301"), states that when a significant amount of information supporting one or more relevant assertions is electronically initiated, recorded, processed, or reported, it might be impossible to design effective substantive tests that, by themselves, would provide sufficient appropriate evidence regarding the assertions. For such assertions, significant audit evidence may be available only in electronic form. In such cases, the sufficiency and appropriateness of the audit evidence usually depends on the effectiveness of controls over its accuracy and completeness. Also, tests of controls must be performed in the audit of financial statements for each relevant assertion for which substantive procedures alone cannot provide sufficient appropriate audit evidence and when necessary to support the auditor's reliance on the accuracy and completeness of financial information used in performing other audit procedures.

AS 2310, *The Confirmation Process*, states that the auditor should assess whether the evidence provided by confirmations reduces audit risk for the related assertions to an acceptably low level. In making that assessment, the auditor should consider the materiality of the account balance and his or her inherent and control risk assessments. When the auditor concludes that evidence provided by confirmations alone is not sufficient, additional procedures should be performed.

If information about the respondent's competence, knowledge, motivation, ability, or willingness to

[7] In this Spotlight, the term "private key" refers to the cryptographic key that is privately held and is required to be used in conjunction with a public key to decipher encrypted messages.

respond, or about the respondent's objectivity and freedom from bias with respect to the audited entity comes to the auditor's attention, the auditor should consider the effects of such information on designing the confirmation request and evaluating the results, including determining whether other procedures are necessary. In addition, there may be circumstances (such as for significant unusual year-end transactions that have a material effect on the financial statements or where the respondent is the custodian of a material amount of the audited entity's assets) in which the auditor should exercise a heightened degree of professional skepticism relative to these factors about the respondent. In these circumstances, the auditor should consider whether there is sufficient basis for concluding that the confirmation request is being sent to a respondent from whom the auditor can expect the response will provide meaningful and appropriate evidence.

AS 2410, *Related Parties*, states that the auditor should perform procedures to obtain an understanding of the company's relationships and transactions with its related parties that might reasonably be expected to affect the risks of material misstatement of the financial statements in conjunction with performing risk assessment procedures in accordance with AS 2110.

Recommended Actions to Execute Responsibilities Under PCAOB Standards

It is important that the auditor tailor its audit response to specific facts and circumstances (including those identified during risk assessment) related to the public company's involvement with crypto assets, which would include considering whether confirmations obtained from third parties provide sufficient and appropriate evidence in addressing the assessed risk of material misstatement.

As described above, tests of controls must be performed for each relevant assertion for which substantive procedures alone cannot provide sufficient and appropriate audit evidence. For example, performing substantive procedures to verify that a public company has access to the private keys associated with the public addresses that contain a public company's crypto assets may not provide sufficient evidence that the public company has sole ownership rights over the crypto assets, as access does not necessarily imply ownership. In this instance, testing the design and operating effectiveness of the public company's internal controls over the generation and maintenance of the keys, including segregation of duties related to the key management process may be necessary to obtain sufficient appropriate audit evidence of the public company's ownership of crypto assets.

If the public company is using a third-party[8] custodian to hold the crypto assets, it is important for the auditor to assess the terms and conditions of the custodial arrangement (including any side arrangements and whether the custodian commingles the public company's crypto assets in a public address that includes crypto assets of other depositors) to determine how the terms and conditions affect the rights and obligations of the depositor.

[8] If the third party is a service organization that is part of the public company or broker-dealer's information system over financial reporting, AS 2601, *Consideration of an Entity's Use of a Service Organization*, describes the auditor's responsibilities for obtaining an understanding of controls at the service organization.

Relevance and Reliability of Information Used as Audit Evidence

We have identified deficiencies where an auditor did not evaluate the relevance and/or reliability of:

- Information obtained from the download of self-custodied crypto asset digital wallets[9] and external providers' data used as audit evidence to support the existence, occurrence, valuation, and completeness of crypto asset balances and/or revenue transactions;
- Information obtained from the public company to test occurrence and completeness of crypto asset mining revenue; and/or
- Pricing information from third parties used as audit evidence to support the valuation of crypto assets and mining revenue.

Key Considerations

Auditors may use information from the applicable distributed ledger as audit evidence to evaluate amounts of crypto assets and related activities recorded in a public company's books and records. In performing these procedures, the auditors may use tools called block explorers or other applications ("blockchain explorer tools") that provide information that is recorded in distributed ledgers.

It is important that the auditor determines whether and how information from a distributed ledger can be used as audit evidence. Based on that assessment, the auditor considers the relevance and reliability of distributed ledger records to establish a basis for using information from a distributed ledger as audit evidence. For example, tracing the rewards earned by the public company as a result of crypto asset mining activities to the distributed ledger records may not provide reliable evidence if the auditor did not assess the reliability of data obtained from the distributed ledger that is relevant to the audit. The auditor may also need to engage professionals with specialized skills or knowledge (e.g., cryptography, distributed ledger technology) to assist them in designing and executing an appropriate audit approach.

In addition, the public company may have omitted crypto assets at certain distributed ledger addresses, including in accounts with intermediaries such as exchanges and/or custodians. Organizations that provide crypto asset custodial services may combine customers' crypto assets in commingled digital wallets, and therefore a lack of clear segregation may present risks of material misstatement related to the improper allocation of the crypto assets to specific entities.

Further, when crypto assets are measured at or based on fair value, the auditor should evaluate whether the fair value is determined in accordance with the applicable financial reporting framework. When third-party[10] pricing information used by the public company is significant to the valuation of crypto assets, the auditor should evaluate whether the public company has used that information appropriately and whether it provides sufficient appropriate evidence.[11]

[9] In this Spotlight, the term "digital wallet" refers to a software application, piece of hardware, or other device or service that stores a user's public and private cryptographic keys, which allow users to interact with one or more distributed ledgers and, inter alia, to send and receive crypto assets. With self-custodied digital wallets, users are responsible for safeguarding their own public and private cryptographic keys.

[10] See supra note 8.

[11] For additional guidance please refer to *Staff Guidance – Insights for Auditors Evaluating Relevance and Reliability of Audit Evidence Obtained From External Sources*.

Auditor's Responsibilities

AS 1105, *Audit Evidence* ("AS 1105"), states the auditors must plan and perform audit procedures to obtain sufficient appropriate audit evidence to provide a reasonable basis for their opinion. Sufficiency is the measure of the quantity of audit evidence. The quantity of audit evidence needed is affected by the following:

- **Risk of material misstatement (in the audit of financial statements) or the risk associated with the control (in the audit of internal control over financial reporting)** – As the risk increases, the amount of evidence that the auditor should obtain also increases.
- **Quality of the audit evidence obtained** – As the quality of the evidence increases, the need for additional corroborating evidence decreases. Obtaining more of the same type of audit evidence, however, cannot compensate for the poor quality of that evidence.

To be appropriate, audit evidence must be both relevant and reliable in providing support for the auditor's conclusions. The relevance of audit evidence depends on the design and timing of the audit procedure used to test the assertion or control. The reliability of audit evidence depends on the nature and source of the evidence and the circumstances under which it is obtained, such as whether the information is provided to the auditor by the company being audited and whether the company's controls over that information are effective. For example, the evaluation of the reliability of information may differ depending on whether the information is coming from a public distributed ledger or a private distributed ledger.

AS 2501, *Auditing Accounting Estimates, Including Fair Value Measurements*, states that when the auditor uses pricing information from a third party to develop an independent expectation or evaluates pricing information provided by a third party used by the company, the auditor should perform procedures to determine whether the pricing information provides sufficient appropriate evidence to respond to the risks of material misstatement. For example, the auditor should determine the reliability of the pricing information from the public company, or third parties used to support the valuation of crypto assets.

Recommended Actions to Execute Responsibilities Under PCAOB Standards

As noted above, the auditor may use information from a distributed ledger as audit evidence to corroborate amounts related to crypto assets and related activities recorded in a public company's books and records. In performing these procedures, the auditor may use technology-based tools (e.g., blockchain explorer tool) that provide information recorded in distributed ledgers. When using such technology-based tools in the audit, it is important for the auditor to evaluate whether the tools used, including controls around the tools, are properly designed and operating effectively to accurately and completely extract and display distributed ledger data used as audit evidence that is relevant for the audit.

It is important that the auditor determine whether a risk of material misstatement exists that crypto assets and related activities are not completely captured and disclosed in the public company's books and records. If so, the auditor needs to assess the risk and design and implement audit responses that address it. For example, in identifying and assessing risks of material misstatement, the auditor may consider whether there is a risk that financial statements and disclosures are materially misstated because a public company (inadvertently or intentionally) did not record a complete population of crypto assets.

Revenue Recognition in Crypto Asset Transfer

We have identified deficiencies where an auditor did not perform procedures to assess the appropriateness of revenue recognition related to the transfer of crypto assets.

Key Considerations

It is important that the auditor assesses whether a transfer of crypto assets (including a transfer to a related party) qualifies as a contract with a customer pursuant to ASC 606, *Revenue from Contracts with Customers* ("ASC 606"),[12] and if so, whether the revenue recognition criteria set out in ASC 606 have been met.

Auditor's Responsibilities

AS 2301 states that the auditor should evaluate whether the company's selection and application of significant accounting principles, particularly those related to subjective measurements and complex transactions, are indicative of bias that could lead to material misstatement of the financial statements.

AS 2810, *Evaluating Audit Results* ("AS 2810"), states that the auditor must evaluate whether the financial statements are presented fairly, in all material respects, in conformity with the applicable financial reporting framework.

Recommended Actions to Execute Responsibilities Under PCAOB Standards

As a reminder, when performing procedures over revenue, including revenue related to the transfer of crypto assets, it is important that the auditor obtains an understanding of a public company's significant activities related to crypto assets, including the business purpose for engaging in such activities. Additionally, the auditor must understand and evaluate the public company's selection and application of its accounting policies regarding crypto assets and related activities, including the related disclosures, and evaluate whether they are consistent with the applicable financial reporting framework.

Arrangements With Mining Pool Operators

We have identified deficiencies where an auditor did not:

- Obtain an understanding of the terms and conditions of the public company's arrangements with mining pool operators where related mining revenue was material to the public company's financial statements.
- Evaluate the public company's conclusion that there were no indicators of potential impairment for property and equipment used in crypto asset mining operations, even though certain indicators of potential impairment existed.

Key Considerations

Entities may combine their computing power in mining pools with other participants to increase their chances of being the first to add a new block to the blockchain. When the mining pool is successful, a participant's share of the reward is determined and distributed based on an allocation method under the terms and conditions of the mining pool. The allocation approach is usually based on the number of computational resources that each participant contributed to the pool over some period of time.

[12] See FASB Accounting Standards Update ("ASU") No. 2014-09, *Revenue from Contracts with Customers* (Topic 606) (May 2014) ("FASB ASU 2014-09"), as codified in FASB Accounting Standards Codification ("ASC") Topic 606, *Revenue from Contracts with Customers*, and additional ASUs that link to the transition guidance in FASB ASC paragraph 606-10-65-1 (the "new revenue standard").

Auditor's Responsibilities

AS 2301 states that auditors should design and perform audit procedures to address the assessed risks of material misstatement for each relevant assertion of each significant account and disclosure. For example, the auditor should design and perform procedures to evaluate whether the public company's crypto asset mining revenue was recognized in accordance with ASC 606.

AS 1105 states that the auditor must plan and perform audit procedures to obtain sufficient appropriate audit evidence to provide a reasonable basis for his or her opinion. To be appropriate, audit evidence must be both relevant and reliable in providing support for the conclusions on which the auditor's opinion is based. For example, determining whether information provided by the mining pool operator which was used by the public company to recognize its revenue is relevant and reliable and can be used as audit evidence involves examining the terms of the mining pool arrangement.

AS 2810 states that in forming an opinion on whether the financial statements are presented fairly, in all material respects, in conformity with the applicable financial reporting framework, the auditor should take into account all relevant audit evidence, regardless of whether it appears to corroborate or to contradict the assertions in the financial statements. For example, in evaluating management's conclusion that there were no indicators of potential impairment for property and equipment used in crypto asset mining operations, it is important that the auditor consider whether declines in crypto asset prices during the fiscal year indicate that potential impairment may exist.

Recommended Actions to Execute Responsibilities Under PCAOB Standards

If mining revenue is material to the public company's financial statements, it is important for the auditors to understand the terms and conditions of the mining pool arrangement, including how the mining pool operator calculates and distributes the allocated rewards to the pool's participants. The auditors will need to understand how revenue is earned, evaluate whether the public company's arrangement with the mining pool operator represents a contract with an identifiable customer in accordance with ASC 606, and design and implement the audit response based on the risks identified. In addition, it is important that the auditors test the relevance and reliability of information obtained from the mining pool that is used as audit evidence.

It is also important that the auditor evaluate whether the public company appropriately identified impairment indicators with respect to the property and equipment used in crypto asset mining operations.

GOOD PRACTICES

Through our inspections, we observed the following good practices we believe may enhance audit quality:

1. **Consultations** – Engagement teams at some audit firms are encouraged to consult with members of their firm's professional practice group and/or subject matter specialists related to crypto assets. The consultations included considerations of the planned audit approach regarding crypto assets and, in some instances, an assessment of whether the public company's accounting policy regarding crypto assets is consistent with the applicable financial reporting framework.

2. **Subject matter specialists** – Certain audit firms have established centralized groups related to distributed ledger technology (e.g., cryptography, blockchain technology). These auditor-employed specialists assist audit teams with conducting audit procedures related to crypto assets, as needed.

3. **Technology-based tools** – To support public company audits involving crypto assets, some audit firms have developed proprietary technology-based tools. Each such tool has,

to some degree, similar functionalities, such as retrieving certain public companies' crypto asset transaction data from distributed ledgers and analyzing the data using sophisticated algorithms. The tools are generally compatible with multiple distributed ledgers and related crypto assets. The engagement teams used the tools in conducting audit procedures to obtain and corroborate data included in the relevant records that was used as audit evidence, including observing how transactions are initiated, processed, recorded, and reported on the distributed ledger.

REMINDERS FOR AUDITORS

Auditors should design and perform their audit procedures as required by PCAOB auditing standards. Below, we share reminders for auditors about certain key areas of responsibility under PCAOB standards at the firm level and at the audit engagement level.

Client Acceptance and Retention Evaluation

The audit firm should undertake only those engagements that it can reasonably expect to be completed with professional competence, as the performance of audits involving crypto assets will likely require specialized skill and knowledge. In addition, both the engagement partner and the engagement quality reviewer will require an appropriate level of knowledge and competence relating to accounting, auditing, and financial reporting involving crypto assets. It is important that the audit firm obtain an understanding of how and why the public company or broker-dealer uses crypto assets, the public company or broker-dealer's underlying information technology (IT) infrastructure, the public company or broker-dealer's personnel and expertise to deal with and appropriately account for crypto asset activities, and the public company or broker-dealer's governance necessary to engage in crypto asset activities. The audit firm may also conclude that consultation with others, including specialists, is warranted in conducting the client acceptance and retention evaluation.

IT Infrastructure

A public company or broker-dealer's existing IT infrastructure may not be appropriately configured to capture, process, record, and report crypto asset activities accurately and completely. The auditor should obtain an understanding of how the public company or broker-dealer uses IT to support transactions and how IT affects the financial statements in accordance with AS 2110. The auditor should also obtain an understanding of manual and automated controls used by the public company or broker-dealer, including the IT general controls that are important to the effective operation of the manual and automated controls.

Consideration of Fraud

PCAOB standards require that the auditor plan and perform the audit to obtain reasonable assurance about whether the financial statements are free of material misstatement due to error or fraud. Fraud risks may arise from a variety of sources. Financial statements may be susceptible to material misstatement through transactions with related parties, as identities of related parties may be difficult to ascertain because of the pseudonymous nature of transactions associated with crypto assets. In addition, certain crypto assets may have privacy features that shield or obfuscate the transaction history on the blockchain. Further, the pseudo-anonymity of blockchain records may provide management with the opportunity to engage in fraudulent financial reporting, including executing fictitious transactions that have no economic substance.

The auditor should perform risk assessment procedures and evaluate whether the information gathered from those procedures indicates that one or more fraud risk factors are present, and it is important the auditor takes the information into account when identifying and assessing fraud risks related to crypto assets. The auditor's responses

to the identified and assessed fraud risks should include responses that have an overall effect on the nature, timing, and extent of audit procedures with respect to crypto assets.

Related Parties

The auditor should obtain sufficient appropriate audit evidence to determine whether related parties and relationships and transactions with related parties have been properly identified, accounted for, and disclosed in the financial statements. The pseudonymous nature of activities involving crypto assets may obscure the true identity of the public company's or broker-dealer's counterparties, creating the risk of not identifying involvement of related parties.

Evaluating whether a public company or broker-dealer has properly identified its related parties and relationships and transactions with related parties involves more than assessing the process used by the public company or broker-dealer. This evaluation requires the auditor to perform procedures to test the accuracy and completeness of the related parties and relationships and transactions with related parties identified by the public company or broker-dealer, taking into account information gathered during other audit procedures.

Evaluating the Presentation of the Financial Statements, Including Disclosures

The auditor must evaluate whether the financial statements are presented fairly, in all material respects, in conformity with the applicable financial reporting framework. The auditor will need to understand the public company or broker-dealer's accounting policies regarding crypto assets and related activities, including the related disclosures, and evaluate whether they are consistent with the applicable financial reporting framework. Each crypto asset may have different characteristics that would need to be considered by the auditor in their evaluation of the public company or broker-dealer's accounting policies.

We Want to Hear From You

The PCAOB strives to improve our external communications and provide information that is timely, relevant, and accessible. We invite you to share your views on this document by filling out **our survey**, which should take no more than two minutes to complete.

Critical Audit Matters

An auditor's communication of critical audit matters (CAMs) in the auditor's report is intended to inform investors and other financial statement users about certain matters that required especially challenging, subjective, or complex auditor judgment, and the auditor's response to those matters. The engagement team must determine whether certain matters related to accounts or disclosures that were material to the financial statements (e.g., the valuation, existence and/or ownership of crypto assets held by the public company or broker-dealer), which were communicated or required to be communicated to the audit committee, were CAMs.