Continuing Your Digital Assets Journey

A Tool for Audit Committees

May 2023

CAQ

About the Center for Audit Quality

The Center for Audit Quality (CAQ) is a nonpartisan public policy organization serving as the voice of U.S. public company auditors and matters related to the audits of public companies. The CAQ promotes high-quality performance by U.S. public company auditors; convenes capital market stakeholders to advance the discussion of critical issues affecting audit quality, U.S. public company reporting, and investor trust in the capital markets; and using independent research and analyses, champions policies and standards that bolster and support the effectiveness and responsiveness of U.S. public company auditors and audits to dynamic market conditions.

Contents

Executive summary

Looking to learn more about digital assets? This publication explores:

TOPIC	WHAT THIS MEANS FOR AUDIT COMMITTEES?
Legal and regulatory environment: The digital asset legal and regulatory environment is rapidly evolving with domestic and international regulators and legislators prioritizing this topic.	Involving individuals with appropriate knowledge and expertise to ensure compliance with existing laws and regulations is a critical risk management practice.
Risk assessment: Engaging with digital assets can introduce new or heightened risks for companies, including risks of fraud.	Audit committees have an important oversight role related to effective risk management around business strategies involving the use of digital assets.
Safeguarding digital assets: Custody practices are a key focus for companies holding and transacting with digital assets.	Understanding how management has selected an appropriate custody model, based on the company's specific facts and circumstances, is essential to effectively safeguarding digital assets.
Third-party service providers: For companies that rely on third-party service providers in the digital asset ecosystem it is important to perform due diligence on the third parties they plan to engage with.	If a company uses a third party to safeguard its digital assets, SOC 1 Type 2 reports are a key mechanism for management to understand the control environment at the service provider.
Accounting and auditing considerations: Engaging with digital assets introduces a number of new accounting and auditing considerations.	It is important to maintain focus on sound accounting and financial reporting practices while engaging with digital assets.

Introduction

Companies continue to engage with digital assets[1] and blockchain technology in a variety of ways, presenting new opportunities and risks for companies incorporating these assets into their business strategy. We also have seen increased calls for digital asset regulation amidst heightened concerns about fraud and misconduct related to digital assets. Despite uncertainty in the regulatory environment, it is clear that digital assets are here to stay. The audit committee[2] has an important responsibility on behalf of company shareholders to oversee the financial reporting process and external audit and therefore, is well positioned to provide oversight for companies engaging in digital asset transactions.

For those audit committee members with oversight of companies that hold or transact with digital assets, this publication examines key digital asset-related topics and provides questions for audit committees to consider when discussing these topics with management and the external auditor (see Appendix A for a list of questions for management and your auditor).[3,4]

1 A digital record made using cryptography for verification and security purposes on distributed ledger technology (referred to as a blockchain). A digital asset is characterized by its ability to be used for a variety of purposes, including as a means of exchange, as a representation to provide or access goods or services, or as a financing vehicle, such as a security, among other uses.

2 While this publication focuses specifically on audit committees, other committees of the Board may also have oversight responsibilities related to digital assets. In such cases, it is best practice for the committees to clarify and coordinate their oversight responsibilities.

3 This resource does not address more advanced topics relevant to crypto native companies, like digital asset exchanges, or miners, among others. Our initial publication on this topic for audit committees, Jumpstart Your Digital Assets Journey: A Tool for Audit Committees published in November 2022, covers foundational digital asset topics.

4 This resource focuses on digital asset-related considerations that the audit committee may address with management and the external auditor. Although this publication does not specifically address questions for internal auditors, the considerations may also be applicable for the audit committee's oversight of internal audit.

Regulatory, legal, and compliance with laws and regulation

The digital asset legal and regulatory environment is rapidly evolving and audit committees should expect continued developments. It is important for audit committees to exercise oversight and understand whether management involves the appropriate parties to monitor, evaluate, and comply with applicable laws and regulations. These may include compliance departments, internal or external legal counsel, and/or other external advisors. Compliance is important to monitor on an ongoing basis and is also a critical part of the due diligence process if a company is considering any potential business transactions.

Terms like digital asset and crypto asset are widely used, however, may have different meanings across regulators and others in the digital asset ecosystem. Throughout this publication, when we have used the term crypto asset, we use the term as it has been defined by the regulator or standard setting body that is being discussed.

COMPLIANCE AMIDST UNCERTAINTY

Some digital assets may not fit neatly within existing U.S. regulatory regimes (for example, those of the Securities and Exchange Commission (SEC) or Commodity Future Trading Commission (CFTC)). Some U.S. government agencies have used their enforcement authority to provide regulatory clarity in specific cases. Despite regulatory uncertainty with respect to digital assets, it is important that understanding and complying with the existing relevant legal and regulatory frameworks be a top priority for companies. It is important to understand the regulations impacting the digital assets the company uses – for example, whether the digital asset meets the definition of a security, which regulatory body is responsible for oversight of the digital asset, and any other legal or contractual requirements specific to the digital assets with which the company engages.

MONITORING LEGISLATIVE AND REGULATORY ACTIONS AND RULEMAKING

We have observed that legislative action is a high priority at the state, federal and international levels. For example, developing a regulatory framework for digital assets is a priority of the Biden administration. In March 2022 the President signed an "Executive Order on Ensuring Responsible Development of Digital Assets" directing government agencies to form committees to research and form a regulatory framework for digital assets.[5] In September 2022, the White House released the "Comprehensive Framework for Responsible Development of Digital Assets."[6] The framework aims to protect those who invest in digital assets by encouraging regulators like the SEC and CFTC to pursue investigation and enforcement actions against unlawful practices related to digital assets. It also focuses on fostering financial stability,

5 FACT SHEET: President Biden to Sign Executive Order on Ensuring Responsible Development of Digital Assets
6 FACT SHEET: White House Releases First-Ever Comprehensive Framework for Responsible Development of Digital Assets

particularly by working with financial institutions to bolster their capacity to identify and mitigate cybersecurity vulnerabilities that can arise from holding and transacting with digital assets.

In the U.S., Congress is also focused on digital asset regulation. In January 2023, the U.S. House Committee on Financial Services created a subcommittee on Digital Assets, Financial Technology and Inclusion. This subcommittee is focused on "providing clear rules of the road among federal regulators for the digital asset ecosystem, developing policies that promote financial technology to reach underserved communities, [and] identifying best practices and policies that continue to strengthen diversity and inclusion in the digital asset ecosystem."[7]

Internationally, many countries are also focused on developing comprehensive digital asset regulation. For example, in the EU, the European Parliament approved the Markets in Crypto-Asset (MiCA) regulation in April 2023. MiCA regulates issuance and trading of certain crypto assets (as defined in the proposed regulation) as well as the management of the underlying assets, where applicable.[8]

LEGAL DEFINITION OF A SECURITY

A key topic in the digital asset regulatory environment is whether the characteristics of a digital asset meet the definition of a security under existing SEC rules. Currently the SEC and federal courts use the Howey Test to analyze whether a particular digital asset has the characteristics of an "investment contract" and would therefore be a security that is subject to the federal securities laws.[9] Some digital assets may not meet the definition of a security. For example, based on public comments made by the SEC, the common crypto asset, bitcoin, does not currently meet the definition of a security. However, in a September 2022 speech, SEC Chair Gary Gensler stated that he believes that "most crypto tokens are investment contracts under the Howey Test."[10]

Whether a digital asset is considered a security impacts the regulatory requirements to which the asset is subject.

Whether a digital asset is considered a security impacts the regulatory requirements to which the asset is subject. A digital asset that is a security is subject to SEC regulation (as are exchanges and other participants in the digital asset ecosystem when securities are involved). Other digital assets may be considered commodities for regulatory purposes. The CFTC regulates commodity derivatives, but it does not regulate commodity spot markets (although it does have enforcement authority for fraud and manipulation in commodity spot markets).[11]

This is an important area of focus for companies engaging with digital assets because the regulatory regime, if any, to which its digital assets are subject could give rise to disclosure, legal, or reputational risks for the company. For example, there could be risks that arise from transacting in digital asset securities that are not registered with the SEC or engaging in digital asset security transactions with a third party that is not registered with the appropriate regulatory authority. Digital asset

7 McHenry Announces Financial Services Subcommittee Chairs and Jurisdiction for 118th Congress
8 Markets in crypto-assets (MiCA)
9 Framework for "Investment Contract" Analysis of Digital Assets
10 Kennedy and Crypto Speech, Chair Gary Gensler
11 Refer to 10 Things Judges Should Know About Cryptocurrency by Lee Reiners for further discussion.

holders may also consider if any regulatory filing disclosures are required related to regulatory uncertainty.

Audit committees may find the following questions about compliance with laws and regulations useful to discuss with management and the auditor:

Questions for management:

- Has management involved appropriate internal resources or external advisors to understand the digital asset legal and regulatory environment?
- Does management, or external advisors engaged by management, have appropriate knowledge of and experience with the digital asset regulatory frameworks to which the company's digital assets are subject?
- Has management considered any new compliance or regulatory risks that are introduced by engaging with digital assets?
- How does management monitor changes in regulatory risks or emerging risks related to digital assets? How has management responded to any changes in the risk assessment related to digital assets?
- Does management have a process in place to analyze whether a specific digital asset is a security under SEC rules?
- Has management considered how the company's business strategy related to digital assets may be impacted by future regulation?

Questions for your auditor:

- What is the auditor's understanding of the legal and regulatory framework to which the company is subject?
- How does the auditor monitor emerging risks and developments in the digital asset regulatory environment?
- Does the auditor, including external specialists employed or engaged by the auditor, have appropriate knowledge of and experience with the digital asset regulatory frameworks to which the company's digital assets are subject?

Risk assessment and consideration of fraud

Generally, transacting with digital assets can give rise to new or heightened risks, including fraud risks. The audit committee can utilize its oversight role to understand management's and the external auditor's risk assessment, including consideration of fraud risks arising from the company's digital asset activities.

RISK ASSESSMENT

Throughout this publication, we discuss various risks that may arise related to the digital asset regulatory environment, nature of the blockchain,[12] custody practices, and use of service providers and other engagement with third parties. It is important that companies that are transacting with digital assets perform robust risk assessments to understand how digital asset transactions introduce new or additional risks. It is also important to develop appropriate processes and controls to address such risks. This may require additional skillsets given the technology-dependent nature of digital assets and therefore, an important part of the risk management process is ensuring that the company has the appropriate resources internally or engages external service providers with appropriate expertise.

It is important that companies that are transacting with digital assets perform robust risk assessments to understand how digital asset transactions introduce new or additional risks.

FRAUD

Blockchain and digital asset transactions can introduce increased risks of fraud for companies, including risks of fraud perpetrated by management and risks that the company is a victim of fraud perpetrated by external parties.

Fraud Perpetrated by Management

Transacting with digital assets can provide additional opportunities or pressures for management to engage in fraudulent financial reporting or misappropriation of assets schemes. According to the Association of Certified Fraud Examiners *Occupational Fraud 2022: A Report to The Nations*, 8% of the occupational frauds that were reported involved the use of cryptocurrency. Most schemes involved bribery or kickback payments, conversion of misappropriated assets, money-laundering, and manipulation of assets on financial statements.[13] The underlying principles and concepts of these fraud schemes are similar to fraud schemes that may be perpetrated with physical assets, but the nature of digital assets may make it easier to perpetrate these schemes.

For example, the pseudo-anonymous nature of blockchain transactions may present increased opportunities for related party fraud schemes,

12 Refer to the Anti-Fraud Collaboration's Fraud and Emerging Tech: Blockchain publication for further discussion on risks arising from blockchain design and protocols.
13 Refer to ACFE's Occupational Fraud 2022: A Report to the Nations, 2022 for further discussion.

such as multiple related parties fraudulently claiming ownership of the same digital assets through the sharing of private keys allowing them to demonstrate access to those digital assets. Additionally, insufficient safeguarding practices over private keys may also give rise to an opportunity for an individual within the company to misappropriate digital assets (see discussion on safeguarding below).

Frauds Perpetrated by External Parties

Transacting and holding digital assets can also create a risk that a company (or third-party service providers the company engages with) may be the target or victim of a fraud perpetrated by external parties. For example, the company could be defrauded by a third-party service provider that misuses customer assets for personal gain or the company could be the victim of a breach and have its digital assets stolen by a third party. Due to the nature of these assets, they may be more difficult to recover in the event of theft.

Throughout this publication, we will present fraud examples that connect to some of the key considerations for audit committees.

Audit committees may find the following questions related to risk assessment and fraud useful to discuss with management and the auditor:

Questions for management:

- What is management's process for evaluating risks related to digital asset transactions?
- Does management, or external advisors engaged by management, have appropriate knowledge of and experience with digital asset and blockchain technology to understand the risks arising from the company's digital asset transactions and to design and implement corresponding controls to address such risks?
- What fraud risks associated with digital assets has management identified and how have they been addressed?
- Has management evaluated how relationships with service providers or other external parties may give rise to risks that the company may be a victim of fraud perpetrated by an external party?
- What policies and controls has management implemented to address the fraud risks related to digital assets?

Questions for your auditor:

- What risks impacting the financial statements has the auditor identified based on how the company has structured their digital asset holdings and transactions?
- Has the auditor identified any deficiencies or lack of internal controls to mitigate against risks?
- Has the auditor identified any fraud risks related to the company's digital assets? How has the auditor addressed such risks in the audit?

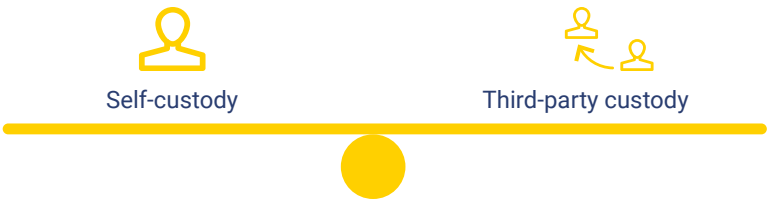
Transacting and holding digital assets can also create a risk that a company (or third-party service providers the company engages with) may be the target or victim of a fraud perpetrated by external parties.

Safeguarding digital assets

Most digital assets are akin to bearer assets – meaning whoever has access to the private key for a digital asset has the ability to control the digital asset. Therefore, private key custody and private key management are essential aspects of safeguarding digital assets.

PRIVATE KEY CUSTODY METHODS

Depending on their specific facts, circumstances, and risk profile, digital asset holders may elect to self-custody their digital assets, where they are responsible for the safeguarding of their private keys in a non-custodial wallet, or they may choose to use a third-party custodian to safeguard digital assets on their behalf.[14] There are different risk considerations associated with each custody model.



Self-Custody

Companies may elect to use a self-custody model based on the nature and extent of their engagement with digital assets and when they have the appropriate expertise and technological resources in-house to effectively manage their own digital asset wallets and other aspects of private key management. Self-custody provides a company with full control over and visibility into private key lifecycle management practices and access to its digital assets. However, it also means the company has sole responsibility for key management and key security. It often necessitates new skillsets and requires management oversight and involvement in the processes and controls to safeguard digital assets.

In order to effectively self-custody its digital assets, a company needs to have appropriate hardware or software solutions. The company may purchase an off-the-shelf software solution or may use an internally developed solution. If management purchases an off-the-shelf software solution, it is important for the company to perform due diligence on the software to understand how the solution meets the company's needs and identify any risks that may arise from using the software that can be addressed with necessary internal controls. Similarly, if the company develops the solution in-house, it is important that the solution has gone through robust testing and is fit for purpose.

FRAUD CONSIDERATION: SELF-CUSTODY

Company A was the victim of a phishing scheme that targeted individuals in the company with access to the company's digital asset wallet. One individual fell for the scheme and the attackers were able to gain access to the individual's credentials. The attackers used the credentials to access the company's wallet and transfer the digital assets to a blockchain address controlled by the attackers.

14 See detailed discussions regarding self-custody and third-party custody, including questions to ask management, in the *Jumpstart Your Digital Assets Journey: A Tool for Audit Committees* publication.

In considering the risks associated with a self-custody solution, it may be helpful to first think about these risks similar to risks associated with any other in-house IT system, including, but not limited to, access management and segregation of duties. However, there are also unique risks related to digital assets to be considered. For example, consider the risks related to the loss of private keys, including the need for backups that are accessible yet appropriately secured, and risks related to physical security and the misappropriation of private keys.

Third-Party Custody

Companies may elect to use a third-party custody solution if they do not have the capabilities in-house to implement a self-custody solution or prefer to utilize the expertise and experience of a third-party custodian. However, using a third-party custody solution does not relieve management of oversight responsibilities.

Specifically, it is important to understand and evaluate the third-party custodian's ability to effectively safeguard the company's digital assets. This would include assessing risks related to safeguarding practices throughout the private key management lifecycle (including key generation, access management, segregation of duties, key backups, and other practices to prevent misappropriation of assets), and other risks around the custodian inappropriately using or lending customer's digital assets or otherwise mismanaging digital assets in their custody.

The risk considerations related to using a third-party custodian may vary depending on the mix of services offered by the custodian, the specific terms of the custodial agreement, and the related procedures and controls of the custodian. For example, third-party custodians may offer a combination of services (that are typically required to be separated in a regulated environment) that could lead to conflicts of interest in a less regulated environment. Recordkeeping practices at the custodian can also give rise to risks. If the custodian has poor recordkeeping practices, there is a risk that there could be a mismatch between management's records and the custodian's records, which could lead to financial reporting issues (if data from the third party is not reliable). Additionally, it is important to understand if the customer bears the risk of loss if a digital asset is not retrievable by the custodian (due to security breach, theft, or fraud)[15] and if there are any restrictions on customer withdrawals.

Third-party custodians have different models for holding digital assets on behalf of customers. Some custodians may maintain segregated addresses on the blockchain for each customer's digital assets. Other custodians may commingle the digital assets of all customers in an address on the blockchain (often referred to as an omnibus custody model), which is similar to the approach commonly used to custody traditional asset classes such as securities. These models have different risk considerations. The omnibus model places additional reliance on the custodian and the company to maintain appropriate records off the blockchain because it is difficult for the company to independently validate the existence of its specific digital assets on the blockchain in a commingled address. Both custody models are generally acceptable, provided that the custodian and the company have implemented

FRAUD CONSIDERATION: THIRD-PARTY CUSTODY

Company A uses third-party Custodian X to custody their digital assets. Custodian X commingles Company A's digital assets and those of other customers with Custodian X's own assets. Custodian X then uses those commingled assets for trading activity and other uses to benefit Custodian X. Custodian X experienced significant losses from trading activities and was not able to fulfill its obligation to return the digital assets to Company A.

15 See also AICPA's Accounting for and Auditing of Digital Assets Practice Aid Question 10.

appropriate processes and controls to address the risks inherent in the custody model. SOC 1 Type 2 reports (discussed in the *Due diligence and third party monitoring section* on page 16) can be used to understand the controls at a third-party custodian and any complementary user entity controls (CUECs) that the company should implement.

PRIVATE KEY MANAGEMENT PRACTICES

Regardless of the custody method selected by management, it is important to understand the private key lifecycle, either because the company is directly responsible for each step of the private key lifecycle (if using self-custody method) or the company is responsible for verifying that the third-party custodian has appropriate practices, controls, and procedures around each part of the private key lifecycle (see further discussion of third-party monitoring and due diligence below).

Key Generation

Cryptographic key pairs are the public and private keys needed to encode and decode encrypted messages on a blockchain network. The public key or address is analogous to a bank account number and is the address used to send or receive digital assets on the blockchain. A private key is needed to authorize transactions, like the transfer of digital assets from a public address. The development of a secure and robust private key is important to protect the company's digital assets. Private keys are developed using cryptography and are long strings of numbers and text. The underlying cryptographic technology makes it virtually impossible to determine a private key using the public key or address.

The development of a secure and robust private key is important to protect the company's digital assets.

It is important for a company to understand the risks around the generation of private keys. Such considerations may include, but are not limited to, the technology or software used to generate the private key, who attends the key generation ceremony, and the individuals within the company that have authority and access to generate private keys.

Key Storage

As we discuss in our initial publication, private keys and the associated public key or blockchain address are generally stored in a cryptographic wallet. There are several different types of wallets that can be used depending on the specific needs and risk profile of the digital asset holder. These include cold storage wallets, hardware wallets, hot storage wallets, mobile wallets, multi-signature wallets, physical wallets, and software wallets.[16] These wallets have varying degrees of risks and benefits for users based on the facts and circumstances of the company and their digital assets portfolio.

Key Security and Use

Given the importance of private keys, it is essential that there are appropriate processes and controls around logical and physical security to safeguard private keys. Access management controls, including which individuals have authority to access private keys and periodic access reviews, and controls around segregation of duties and levels of authority

16 Refer to detailed discussion of each wallet type in the *Jumpstart Your Digital Assets Journey: A Tool for Audit Committees* publication.

in the private key lifecycle, including responsibilities for key generation, custody/safeguarding, and transaction authorization, are key safeguarding practices. Techniques such as using multi-signature addresses and "sharding" also add additional security around private keys.

Multi-signature addresses require consensus or approval of multiple parties to complete a transaction. For example, three out of five different private keys would be required to sign a transaction. The additional step of requiring multiple private keys adds an additional level of security to initiate a transaction. The distinct private keys can be maintained in separate locations and under the control of different individuals.

"Sharding"[17] is the process of splitting private keys into multiple components using cryptographic techniques. This process adds additional security to the storage of private keys because the private key needs to first be reassembled from its different pieces before it can be used to initiate a transaction. The shards may be maintained in separate locations and under the control of different individuals.

Audit committees may find the following questions around digital assets safeguarding and custody useful to discuss with management and the auditor:

Questions for Management:

- What are some of the key risks and responses that management has considered related to the company's safeguarding and custody practices?
- How has management evaluated the sufficiency of existing policies and procedures related to the safeguarding of digital assets?
- What custody model has management selected to safeguard the company's digital assets and why?
- If the company self-custodies their digital assets, has management evaluated the sufficiency of technological resources and skills of those responsible for custody?
- How has management assigned roles and authorities around private key generation and private key safeguarding and custody practices?
- When a third party is used to assist with safeguarding assets, does management have a comprehensive due diligence and monitoring framework in place which considers the custody model used and the unique risks associated with safeguarding the assets? Is a SOC 1 Type 2 report available?

Questions for your Auditor:

- What risks has the auditor identified related to the custody model selected by management?

17 See additional discussion in AICPA's Accounting for and Auditing of Digital Assets Practice Aid AU Chapter 2 Section IV A.

- If the company self-custodies their digital assets, has the auditor identified any risks related to management's skills and technological resources?
- If the company self-custodies their digital assets, does the auditor believe that management has implemented the appropriate processes and controls to address the risks?
- If a third-party custodian is used, does the auditor have any concerns about management's due diligence or oversight of the third-party custodian?
- If a third-party custodian is used, does the auditor believe the SOC 1 Type 2 report covers the necessary processes and controls to address the relevant risks?

Due diligence and third party monitoring

BLOCKCHAIN DUE DILIGENCE

It should be a priority for companies transacting with digital assets to understand the digital assets and underlying blockchain that the company is engaging with. As part of the risk assessment process and prior to engaging in digital asset transactions, companies should perform due diligence on the digital assets and underlying blockchain with which they intend to transact. Currently, there are many different active blockchains with varying levels of maturity. Some blockchains are well-known and have been operating for many years without significant issues, while others are newer or have had vulnerabilities in the past.

Key considerations about the blockchain include understanding the purpose of the blockchain, the company's reason for engaging with the blockchain, and understanding the blockchain's reliability and key features. Understanding these topics, among others, can help management assess the risks that may arise from transacting with digital assets.

Procedures to understand the blockchain and digital assets the company engages with should be performed by individuals with appropriate skills and experience to review this information. This may involve the Chief Information Security Officer (CISO), IT team, or external advisors with specific expertise. It is also important to keep in mind that some blockchains are periodically updated and therefore, it may be necessary to monitor the blockchain to identify any new risks.

Audit committees may find the following questions related to blockchain due diligence useful to discuss with management and the auditor:

Questions for management:

+ What blockchain(s) is the company interacting with?
+ What due diligence procedures has management performed to assess the reliability of the blockchain(s) the company uses?
+ What is management's process for monitoring the reliability of the blockchain(s) the company uses?
+ Has management identified any issues with the blockchain(s) it interacts with? How is management mitigating those risks?

FRAUD CONSIDERATION: BLOCKCHAIN DUE DILIGENCE

An update to Blockchain A led to a major vulnerability in its protocol. The update caused the validation of certain transactions to always be true or valid (even if they were not). Blockchain participants exploited this vulnerability to process transactions to withdraw funds from the platform through transactions that should not have been valid but because of the vulnerability were still processed.

Questions for your auditor:

- What is the auditor's understanding of the blockchain technology underlying the company's digital asset-related activities?
- Does the auditor have experience and expertise dealing with the digital assets and blockchain(s) management engages with?
- How does the auditor evaluate reliability of information obtained from blockchain that is used as audit evidence?

THIRD PARTY DUE DILIGENCE

In addition to understanding the blockchain itself, it is important to understand the risks that arise from engaging with third parties in the digital asset ecosystem. The risks may vary based on the nature of the relationship between the company and the third party. Practicing careful due diligence and monitoring for changes with third parties is important to safeguarding a company's digital assets. It is also important to keep in mind that the pseudo-anonymity provided by the blockchain can sometimes make it hard to identify counterparties to transactions.[18]

There are many different types of third parties that a company may have relationships with depending on the nature and complexity of the transactions it enters into. The most common are the counterparty (buyer or seller on the other side of the transaction) or service providers such as an exchange[19] or clearing firm that acts as an intermediary between the company and the counterparty and third-party custodians (discussed above). Understanding these relationships, including any rights or obligations of the company or third party, is critical to evaluating the risks to which such relationships may give rise. It also may be important to understand any key relationships between relevant third parties. In the current environment, many participants engaging in digital asset activities are highly interconnected and therefore, issues at one third party could ultimately have broad implications for other entities in the digital asset ecosystem.[20]

In the current environment, many participants engaging in digital asset activities are highly interconnected and therefore, issues at one third party could ultimately have broad implications for other entities in the digital asset ecosystem.

UNDERSTANDING RISKS BASED ON THE THIRD PARTY'S FUNCTION AND THE NATURE OF THE AGREEMENT

Counterparty to a Transaction

When the company is entering into a transaction to buy or sell digital assets the identity of the counterparty may not be known because of the pseudo-anonymity provided by the blockchain. Companies should be mindful of compliance with laws and regulations, including Office of Foreign Assets Control (OFAC) sanctions, Know Your Customer (KYC) measures, and Anti-Money Laundering (AML) to mitigate the risk of engaging with bad actors or sanctioned groups. Many digital asset exchanges or platforms have policies and procedures in place to address compliance, but it is the responsibility of the company to evaluate how

18 As discussed above, in a blockchain environment, digital assets are exchanged between public addresses and therefore, the identity of the counterparty in a transaction may not be apparent.
19 In some instances, exchanges may also act as custodians.
20 Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, and Office of the Comptroller of the Currency Joint Statement on Crypto-Asset Risks to Banking Organizations

the exchanges they transact on verify compliance and if any additional processes are needed at the company-level to ensure compliance.

Further, companies need to consider the identities of their counterparties in order to completely identify all related party transactions for financial reporting purposes (see further discussion below). It is important that the company develops appropriate policies and procedures around identification of related party transactions.

Digital Asset Exchange or Platform

Companies may enter into digital asset transactions through an exchange or platform. As discussed above, it is important to consider compliance with KYC and AML regulations. Additionally, it is important to understand where the platform is registered and how it is regulated (for example, consider if the platform is, or should be, registered with regulators like the SEC).[21] Regulation, or lack thereof, impacts investor protections, including recourse, in the event that there is an issue with the third party.

Audit committees may find the following questions related to third parties useful to discuss with management and the auditor (see also questions related to the use of third-party custodians above):

Questions for management:

- What third parties has management identified related to its digital asset transactions?
- How does management perform due diligence on third parties? Based on due diligence procedures, what risks or concerns were identified?

Questions for your auditor:

- Has the auditor identified any financial reporting risks related to the company's interactions with third parties related to its digital asset transactions?

SOC 1 TYPE 2 REPORTS

There is a wide range of maturity of third-party service providers (exchanges, trading platforms, custodians, etc.) and the sophistication of internal controls over the service provider's activities and reliability of data may vary. Management should evaluate service providers upon initial selection and periodically assess risks and understand the processes and controls in place to address those risks.

In most circumstances companies should obtain a SOC 1 Type 2 report[22] from a service provider, if available, to understand and evaluate the control environment at the service provider. This is particularly important

It is important that the company develops appropriate policies and procedures around identification of related party transactions.

21 Statement on Potentially Unlawful Online Platforms for Trading Digital Assets

22 A SOC 1 Type 2 report is a report on the fairness of the presentation of management's description of the service organization's system and the suitability of the design and operating effectiveness of the controls to achieve the related control objectives included in the description throughout a specified period. The reports are prepared by a CPA in accordance with AICPA attestation standards. See additional information from the AICPA regarding SOC 1 Type 2 reports.

when the company is using a third party to custody its digital assets so that management can evaluate the service provider's ability to effectively safeguard those digital assets. If a SOC 1 Type 2 report is not available, additional procedures are often necessary to understand and evaluate the controls and the reliability of data obtained from the service provider. Audit committees should be aware that the lack of SOC 1 Type 2 reports for custodians may not only add challenges related to identifying financial reporting risks and evaluating controls for management, but also for the external auditor.

When evaluating a SOC 1 Type 2 report, it is important to consider the scope of the report, risks addressed, and level of precision. For example, when evaluating a SOC 1 Type 2 report for a service provider who is safeguarding the entity's digital assets, it is important to consider whether there are control objectives related to wallet architecture, key generation, backup, recovery, and continued key security, in addition to the typical reconciliation and reporting control objectives. It is also important to evaluate if there are any risks that have not been sufficiently mitigated, and what CUECs need to be in place at the company to complement the controls at the service provider.

Audit committees may find the following questions about SOC 1 Type 2 reports useful to discuss with management and the auditor:

Questions for management:

- Is management able to obtain a SOC 1 Type 2 report for service providers, including custodians? If not, what alternative procedures will management perform?
- If available, has management reviewed the SOC 1 Type 2 report(s) and established any necessary CUECs? Is the scope of the SOC 1 Type 2 report sufficient for management's needs?
- Does management have any concerns about custodians or other service providers based on the SOC 1 Type 2 report or any alternative procedures performed?
- Is management relying on a proof of reserve report? If so, how has management considered the inherent limitations of such reports?

Questions for the auditor:

- Is the auditor able to obtain sufficient appropriate audit evidence (through SOC 1 Type 2 report or alternative procedures) about the company's digital asset transactions with, or digital assets held at third parties?
- Has the auditor evaluated the company's CUECs?

PROOF OF RESERVE REPORTS

Recently, certain services, commonly referred to as "proof of reserve" reports for digital asset exchanges have gained considerable attention. These reports are the result of an engagement comprised of specified procedures performed at a point in time for specific users and provide no assurance. These engagements are limited to a specific subject matter (such as, demonstrating that assets cover outstanding liabilities at a point in time) and are therefore significantly different than an audit of financial statements and do not show the full picture of the financial health of the entity subject to the engagement. Further, these engagements enable management of the entity, not the service provider, to determine the procedures to be performed by the third party when conducting the engagement. The PCAOB recently issued an Investor Advisory alerting investors that "proof of reserve reports are inherently limited, and customers should exercise extreme caution when relying on them to conclude that there are sufficient assets to meet customer liabilities."[23] The SEC also recently issued an Investor Alert which, among other reminders to investors regarding the risks of investing in crypto assets, included the same recommendation that investors exercise extreme caution when relying on proof of reserve reports.[24]

23 PCAOB Investor Advisory - Exercise Caution With Third-Party Verification/Proof of Reserve Reports
24 SEC Exercise Caution with Crypto Asset Securities: Investor Alert

Accounting and auditing

Throughout digital asset transactions, it is important to maintain focus on sound accounting and financial reporting practices. This means that it is important for management to design and operate internal controls around digital asset processes, maintain sufficient and appropriate documentation for transactions, and maintain independent books and records. The fact that certain digital asset transactions are recorded on the blockchain, or are documented in custodial statements, does not change management's responsibility with respect to maintaining the company's documents and records for all digital asset transactions.

Companies engaging with digital assets should be careful not to lose sight of the importance of governance, oversight, and internal control over financial reporting matters. Maintaining strong internal controls and corporate governance are essential for high-quality financial reporting around digital assets. These topics also remain a key focus of external auditors.

Maintaining strong internal controls and corporate governance are essential for high-quality financial reporting around digital assets.

MAINTAINING INDEPENDENT BOOKS AND RECORDS

Management may obtain information from the exchange where they trade digital assets or where digital assets are custodied. However, when obtaining information from third parties, it is important to consider the reliability of that data. This may involve reviewing the SOC 1 Type 2 report (as discussed above) and implementing controls to reconcile management's records to the custodian's statement and the blockchain.

Additionally, it is important to validate that the company has the appropriate infrastructure to support the financial reporting process as it relates to digital asset transactions. There can be several challenges when accounting for digital asset transactions with traditional accounting software. Software capabilities to consider include, but are not limited to, detailed transaction records, automatic mark-to-market capabilities, tracking cost basis, and calculating capital gains and other tax implications. Infrastructure needs may vary depending on the nature and volume of the company's digital asset transactions.

Audit committees may find the following questions useful to discuss with management and the auditor:

Questions for management:

+ How does management obtain and record digital asset transaction information in the general ledger? Does the company have appropriate systems and technology to support recording digital asset transactions?

+ Does management rely on third-party or other external data to record digital asset transactions? How does management evaluate

the reliability of external data?

+ Does management have processes to reconcile its books and records to third-party data and the blockchain?

Questions for your auditor:

+ Has the auditor identified any risks related to the systems and controls that support recording digital asset transactions?

+ Has the auditor identified any risks related to the reliability of internal or external data used to record digital asset transactions?

RELATED PARTIES

As discussed above, the pseudo-anonymous nature of blockchain transactions may give rise to risk of unidentified related party transactions or may be used to obfuscate certain related party transactions. It may be challenging for management and the external auditor to identify related party transactions, particularly if management or service providers (such as exchanges) do not perform KYC or other procedures that assist with determining the identity of counterparties. From a financial reporting perspective, it is important for management to develop appropriate processes and controls to determine the identity of counterparties in transactions. This is essential to validate the completeness of related party transactions for disclosure in the financial statements. External auditors may also be focused on related party digital asset transactions that are not conducted at arms-length as such transactions could fraudulently inflate the price of a digital asset, particularly if the asset is thinly traded.

Audit committees may find the following questions about related parties useful to discuss with management and the auditor:

Questions for management:

+ Has management identified risks around related party transactions? What procedures and controls has management implemented to identify related party transactions?

+ What additional transparency-related risks (e.g., risks related to the identification of related parties and illegal acts) has management considered? How does management plan to address these risks?

Questions for your auditor:

+ Has the auditor identified any risks to the financial statements related to related party transactions?

+ Is the auditor able to obtain sufficient evidence about any related party transactions?

FRAUD CONSIDERATION: RELATED PARTIES

Company A holds several digital art non-fungible tokens (NFTs). In order to make it appear that the values of the NFTs have been steadily increasing, Company A engages in transactions with related parties, Company B and Company C, to "sell" some of the NFTs at inflated prices, artificially increasing the value of the digital asset. Due to the pseudo-anonymous nature of blockchain transactions, it is not obvious that the transactions occurred between related parties and were not at an arms-length.

CRITICAL AUDIT MATTERS

Audit committees should also be aware that depending on the nature, complexity, magnitude, and materiality of digital asset transactions

and account balances, the audit procedures over such accounts may involve especially challenging, subjective, or complex auditor judgement and may be determined to be a critical audit matter (CAM). The specific account and disclosure determined to be a CAM may vary depending on the nature of the business or transaction. It is good practice for audit committees to engage with the auditor to understand the existence of any CAM and how the matter was handled during the audit. We often see CAMs related to existence (including ownership of private keys) of digital assets and matters related to rights and obligations.

In fiscal year 2022 Form 10-K and 20-F filings, we observed 20 CAMs related to digital assets across 18 distinct companies. The majority of the CAMs related to revenue from contracts with customers (typically for crypto native companies) (8 CAMs) and existence, valuations, and/or control of digital assets (10 CAMs).[25]

In fiscal year 2022 Form 10-K and 20-F filings, we observed 20 CAMs related to digital assets across 18 distinct companies.

Audit committees may consider discussing the following about CAMs with the auditor:

- Has the auditor identified any CAMs related to digital assets? How did the auditor reach their conclusion?
- If the auditor identified any CAMs related to digital assets, how has the auditor addressed the CAM(s)?

RECENT ACCOUNTING UPDATES

As the digital asset space continues to evolve, additional accounting guidance is being developed and released. It is important for management and external advisors to monitor these updates as they may impact the accounting for digital assets at their company.

Staff Accounting Bulletin (SAB) No. 121 (SAB 121)

SAB 121 was released by the SEC staff in March 2022.[26] SAB 121 provides guidance for entities that have an obligation to safeguard their customers' crypto assets. This results in entities, or agents working on their behalf, who have an obligation to safeguard crypto assets recording a safeguarding liability for those assets they safeguard for others (even though the entity does not control the assets), a difference from how entities reflect safeguarding arrangements for other types of assets. SAB 121 highlights unique risks and uncertainties arising from crypto asset custody arrangements, including technological, legal, and regulatory risks, that are not present in arrangements to safeguard assets that are not crypto assets.

Financial Accounting Standards Board (FASB) Project on Crypto Assets

The FASB has an active project to improve the accounting for and disclosure of certain crypto assets. In August 2022, the FASB narrowed the scope of the project to focus on fungible tokens that meet specified criteria.[27] In October 2022, the FASB tentatively decided that crypto

25 Based on data from Audit Analytics as of April 14, 2023.
26 SEC Staff Accounting Bulletin No. 121
27 In the Proposed ASU (Intangibles—Goodwill and Other—Crypto Assets (Subtopic 350-60) Accounting for and Disclosure of Crypto Assets), the FASB outlines six criteria for a digital asset to fall within the scope of the project: (1) Meet the definition of intangible assets as defined in the Codification Master Glossary; (2) Do not provide the asset holder with enforceable rights to, or claims on, underlying goods, services, or other assets; (3) Are created or reside on a distributed ledger based on blockchain technology; (4) Are secured through cryptography; (5) Are fungible; and, (6) Are not created or issued by the reporting entity or its related parties.

assets within the scope of the project should be measured at fair value each reporting period. In December 2022, the FASB decided on certain presentation and disclosure matters, including that gains and losses on crypto assets within the scope of the project should be presented in net income. Lastly, in February 2023, the FASB refined certain scope and transition matters. The exposure draft (Proposed ASU) was published in March 2023. The project is ongoing and will have a significant impact on the accounting for crypto assets within the scope of the Proposed ASU. Management and audit committees should follow the progress of this project.[28]

OTHER ACCOUNTING TOPICS

Other accounting topics that may be of interest to audit committees are:

- *Cost basis of digital assets* – Companies should have processes and controls, including supporting systems capabilities, to track the cost basis of units of digital assets obtained at different times. The cost basis is used to calculate the gain or loss recorded in the financial statements and for tax purposes when digital assets are sold.[29]

- *Derecognition of digital assets* – Because digital assets need to be derecognized at their cost basis, companies need to develop accounting policies, such as applying a first-in, first-out method, for derecognition. This is particularly important for fungible digital assets.[30]

- *Accounting for third-party custody (for the digital asset owner)* – For companies that utilize third-party custodians, understanding if the company has control of those digital assets impacts how the company accounts for them in the financial statements. This may require the company to perform a legal analysis of the custody agreement.[31]

As use cases for digital assets are rapidly evolving, new accounting and auditing questions are arising as well. Additionally, existing accounting interpretations continue to evolve. We recommend that companies facing emerging questions work with their legal counsel and professional service providers to address such matters.

As use cases for digital assets are rapidly evolving, new accounting and auditing questions are arising as well.

28 Refer to updates on the FASB website.
29 See also AICPA's Accounting for and Auditing of Digital Assets Practice Aid Question 8.
30 See also AICPA's Accounting for and Auditing of Digital Assets Practice Aid Question 8.
31 See also AICPA's Accounting for and Auditing of Digital Assets Practice Aid Question 10.

Other current regulation

REGULATORS IN THE DIGITAL ASSET SPACE

There are a number of different regulators and lawmakers that are active in overseeing and monitoring digital assets (beyond the SEC and CFTC), including state and federal banking and treasury regulators, New York Department of Financial Services (NYDFS), Consumer Finance Protection Bureau, Financial Crimes Enforcement Network (FinCEN), and other state legislatures. Following recent high-profile incidents in the digital asset ecosystem, many of these regulators have been active - proposing new rules and regulations and focusing on enforcement in some cases. While the impacts may mostly be felt by crypto native companies, some regulation and enforcement actions may have broader implications for digital asset holders as well. For example, enforcement actions by the SEC against certain crypto native companies may impact a digital asset holder if trading of the asset is halted. Enforcement actions related to digital assets are published on the SEC website.[32]

The SEC has also been actively reminding publicly traded companies of disclosure obligations. In December 2022, the SEC published a Sample Letter to Companies Regarding Recent Developments in Crypto Asset Markets. The letter focuses on disclosures related to a company's exposure to counterparties and other market participants, risks related to a company's liquidity and ability to obtain financing, and risks related to legal proceedings, investigations, or regulatory impacts in the crypto asset markets.[33]

Additionally, in February 2023, the SEC proposed an Enhanced Safeguarding Rule for Registered Investment Advisors. The proposed rule, among other updates, would (1) expand the types of assets (to include all crypto assets) that are subject to the rule and (2) expand the requirement for qualified custodians to segregate customer assets to include all asset types (including all crypto assets).[34] This proposed rule demonstrates that custody practices related to digital assets are a focus of the SEC.

TAX IMPLICATIONS

It is important for management to be aware of the tax implications of the digital asset transactions that they engage in. The IRS has published guidance[35] on the consequences of digital asset transactions, specifically the tax treatment of virtual currencies.[36] Virtual currencies are currently treated as property for federal tax purposes and therefore tax principles applicable to property transactions apply to transactions involving virtual currencies. Companies are encouraged to engage legal counsel and their professional service provider to navigate the tax implications of their digital asset transactions.

It is important for management to be aware of the tax implications of the digital asset transactions that they engage in.

32 Refer to the SEC Crypto Assets and Cyber Enforcement Actions website.
33 See the SEC's Sample Letter to Companies Regarding Recent Developments in Crypto Asset Markets.
34 SEC Proposes Enhanced Safeguarding Rule for Registered Investment Advisers
35 IRS Notice 2014-21
36 The IRS has defined virtual currency as "a digital asset that has an equivalent value in real currency, or acts as a substitute for real currency, has been referred to as convertible virtual currency. A cryptocurrency is an example of a convertible virtual currency that can be used as payment for goods and services, digitally traded between users, and exchanged for or into real currencies or digital assets."

Conclusion

Audit committee oversight in areas such as compliance with applicable laws and regulations, identification and assessment of risks, and financial reporting, is essential as the digital assets landscape continues to evolve. An understanding of key digital assets topics as well as the questions to ask management and the auditor will help audit committees effectively exercise their oversight responsibilities.

Appendix A

This appendix lists questions audit committees may consider asking management and the external auditor related to digital assets. It includes questions from throughout the publication and additional questions that audit committees may find relevant (denoted with an asterisk*).

REGULATORY AND LEGAL

Questions for management

+ Has management involved appropriate internal resources or external advisors to understand the digital asset legal and regulatory environment?

+ Does management, or external advisors engaged by management, have appropriate knowledge of and experience with the digital asset regulatory frameworks to which the company's digital assets are subject?

+ Has management considered any new compliance or regulatory risks that are introduced by engaging with digital assets?

+ How does management monitor changes in regulatory risks or emerging risks related to digital assets? How has management responded to any changes in the risk assessment related to digital assets?

+ Does management have a process in place to analyze whether a specific digital asset is a security under SEC rules?

+ Has management considered how the company's business strategy related to digital assets may be impacted by future regulation?

+ *How has management considered the legal and regulatory implications of its digital asset-related activities?

Questions for auditors

+ What is the auditor's understanding of the legal and regulatory framework to which the company is subject?

+ How does the auditor monitor emerging risks and developments in the digital asset regulatory environment?

+ Does the auditor, including external specialists employed or engaged by the auditor, have appropriate knowledge of and experience with the digital asset regulatory frameworks to which the company's digital assets are subject?

RISK ASSESSMENT AND CONSIDERATION OF FRAUD

Questions for management

+ What is management's process for evaluating risks related to digital asset transactions?

+ Does management, or external advisors engaged by management, have appropriate knowledge of and experience with digital asset and blockchain technology to understand the risks arising from the company's digital asset transactions and to design and implement corresponding controls to address such risks?

+ What fraud risks associated with digital assets has management identified and how have they been addressed?

+ Has management evaluated how relationships with service providers or other external parties may give rise to risks that the company may be a victim of fraud perpetrated by an external party?

+ What policies and controls has management implemented to address the fraud risks related to digital assets?

+ *How has management considered engaging internal audit related to digital assets?

Questions for auditors

+ What risks impacting the financial statements has the auditor identified based on how the company has structured their digital asset holdings and transactions?

+ Has the auditor identified any deficiencies or lack of internal controls to mitigate against risks?

+ Has the auditor identified any fraud risks related to the company's digital assets? How has the auditor addressed such risks in the audit?

SAFEGUARDING DIGITAL ASSETS

Questions for management

+ What are some of the key risks and responses that management has considered related to the company's safeguarding and custody practices?

+ How has management evaluated the sufficiency of existing policies and procedures related to the safeguarding of digital assets?

+ What custody model has management selected to safeguard the company's digital assets and why?

+ If the company self-custodies their digital assets, has management evaluated the sufficiency of technological resources and skills of those responsible for custody?

+ How has management assigned roles and authorities around private key generation and private key safeguarding and custody practices?

+ When a third party is used to assist with safeguarding assets, does management have a comprehensive due diligence and monitoring framework in place which considers the custody model used and the unique risks associated with safeguarding the assets? Is a SOC 1 Type 2 report available?

+ *Does management have the appropriate knowledge and training to understand the digital assets the company is engaging with, and the risks associated with safeguarding those digital assets?

Questions for auditors

+ What risks has the auditor identified related to the custody model selected by management?

+ If the company self-custodies their digital assets, has the auditor identified any risks related to management's skills and technological resources?

+ If the company self-custodies their digital assets, does the auditor believe that management has implemented the appropriate processes and controls to address the risks?

+ If a third-party custodian is used, does the auditor have any concerns about management's due diligence or oversight of the third-party custodian?

+ If a third-party custodian is used, does the auditor believe the SOC 1 Type 2 report covers the necessary processes and controls to address the relevant risks?

DUE DILIGENCE AND THIRD PARTY MONITORING

Questions for management

+ What blockchain(s) is the company interacting with?

+ What due diligence procedures has management performed to assess the reliability of the blockchain(s) the company uses?

+ What is management's process for monitoring the reliability of the blockchain(s) the company uses?

+ Has management identified any issues with the blockchain(s) it interacts with? How is management mitigating those risks?

+ What third parties has management identified related to its digital asset transactions?

+ How does management perform due diligence on third parties? Based on due diligence procedures, what risks or concerns were identified?

+ Is management able to obtain a SOC 1 Type 2 report for service providers including custodians? If not, what alternative procedures will management perform?

+ If available, has management reviewed the SOC 1 Type 2 report(s) and established any necessary complimentary user entity controls? Is the scope of the SOC 1 Type 2 report sufficient for management's needs?

+ Does management have any concerns about custodians or other service providers based on the SOC 1 Type 2 report or any alternative procedures performed?

+ Is management relying on a proof of reserve report? If so, how has management considered the inherent limitations of such reports?

+ *Are current third-party risk management practices sufficient to adequately address risks arising from digital asset engagement?

Questions for Auditors

+ What is the auditor's understanding of the blockchain technology underlying the company's digital asset-related activities?
+ Does the auditor have experience and expertise dealing with the digital assets and blockchain(s) management engages with?
+ How does the auditor evaluate reliability of information obtained from blockchain that is used as audit evidence?
+ Has the auditor identified any financial reporting risks related to the company's interactions with third parties related to its digital asset transactions?
+ Is the auditor able to obtain sufficient appropriate audit evidence (through SOC 1 Type 2 report or alternative procedures) about the company's digital asset transactions with, or digital assets held at third parties?
+ Has the auditor evaluated the company's complimentary user entity controls?

ACCOUNTING AND AUDITING

Questions for management

+ How does management obtain and record digital asset transaction information in the general ledger? Does the company have appropriate systems and technology to support recording digital asset transactions?
+ Does management rely on third-party or other external data to record digital asset transactions? How does management evaluate the reliability of external data?
+ Does management have processes to reconcile its books and records to third-party data and the blockchain?
+ What procedures and controls has management implemented to identify related party transactions?
+ What additional transparency-related risks (e.g., risks related to the identification of related parties and illegal acts) has management considered? How does management plan to address these risks?
+ *What controls has management implemented to support the completeness and accuracy of data and appropriate recording of digital asset transactions?

Questions for auditors

+ Has the auditor identified any risks related to the systems and controls that support recording digital asset transactions?
+ Has the auditor identified any risks related to the reliability of internal or external data used to record digital asset transactions?
+ Has the auditor identified any risks to the financial statements related to related party transactions?
+ Is the auditor able to obtain sufficient evidence about any related party transactions?
+ Has the auditor identified any CAMs related to digital assets? How did the auditor reach their conclusion?
+ If the auditor identified any CAMs related to digital assets, how has the auditor addressed the CAM(s)?

CAQ

www.thecaq.org

We welcome your feedback!

Please send your comments or questions to info@thecaq.org