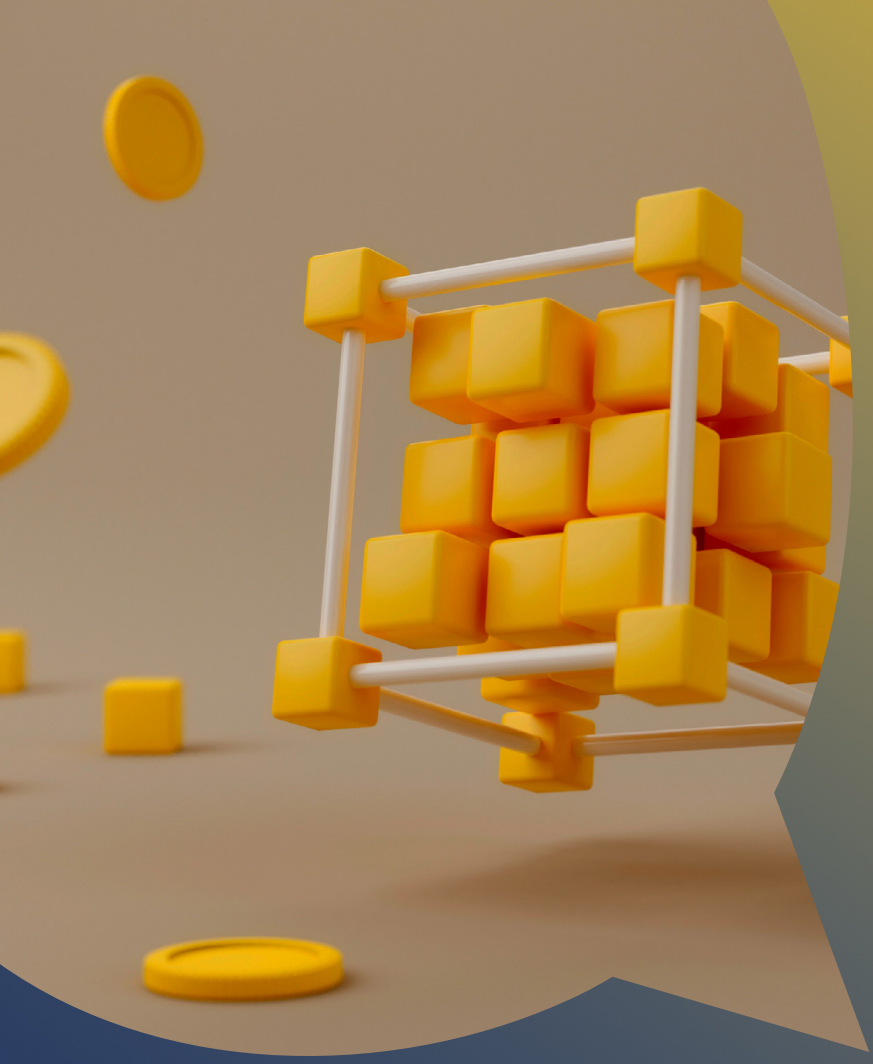


Jumpstart Your Digital Assets Journey: A Tool for Audit Committees

November 2022

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

Introduction

Public companies are increasingly engaging with digital assets[1] and blockchain technology in a variety of ways, from more straightforward investments in digital assets to exploring new opportunities to engage with customers and to improve business processes.

Digital asset activities can present new risks and considerations that public companies should bear in mind. And, audit committees have a role to play. This resource will aid audit committee members in their oversight responsibilities, providing an overview of the digital assets landscape and questions audit committees can ask to better understand company management's digital asset strategy and oversee the related risks (see **Appendix A** for a list of questions for management and your auditor).

Digital asset activities can present new risks and considerations that public companies should bear in mind. And, audit committees have a role to play.

1 A digital record made using cryptography for verification and security purposes on a digital decentralized ledger (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.

Digital assets and blockchain

Before digging into digital assets, it is important to become familiar with the underlying technology that supports them – blockchain. Blockchain relies on the use of peer-to-peer network technology[2] and cryptography[3] to execute transactions and store data immutably on a ledger distributed across several parties. These parties come to consensus on each block of transactions before it is recorded to the chain. This is different than a centralized ledger, like the type used in typical accounting software or a bank's ledger of its depositors' funds. A distributed, or decentralized, ledger is a system of record shared with other participants. In many cases, this results in participants sharing controls and relying on each other for the integrity of the information recorded on the ledger. It is like other opensource software with new and unique considerations to evaluate – like system functionality, reliability, and resilience. Companies are exploring blockchain in a broad range of business and financial applications.

Digital assets is an umbrella term for a spectrum of assets that leverage blockchain technology, including crypto assets,[4] stablecoins, and non-fungible tokens (NFTs), among others. Digital assets have a wide range of use cases and accounting for them does not fall neatly into existing accounting standards.[5] These factors present challenges to both company management and auditors as they work to appropriately account for and audit digital asset transactions, respectively, and for audit committees overseeing companies who engage with them.

While discussing some of the risks arising from digital asset activities, this publication also examines some of the reasons companies may consider engaging with digital assets, the accounting for some digital assets, and the status of standard setting and regulation around digital assets.

2 Peer-to-peer computing or networking is based on a distributed application architecture that shares tasks among peers. All participants engage in the application to form a peer-to-peer network of nodes.

3 Modern cryptography uses mathematics, computer science and electrical engineering to enable secure communication between two parties in the presence of a third party.

4 A type of digital asset, sometimes referred to as a cryptocurrency, that function as a medium of exchange and have all the following characteristics: a) they are not issued by a jurisdictional authority (for example, a sovereign government); b) they do not give rise to a contract between the holder and another party; c) they are not considered a security under the Securities Act of 1933 or the Securities Exchange Act of 1934. These characteristics are not all-inclusive, and other facts and circumstances may need to be considered. Examples of crypto assets meeting these characteristics include bitcoin, bitcoin cash, and ether.

5 The Financial Accounting Standards Board (FASB) has an active project on its Technical Agenda, "Accounting for and Disclosure of Crypto Assets", with an objective to improve the accounting for and disclosure of certain crypto assets. The project is ongoing and may result in changes to the accounting for certain crypto assets.

Why digital assets?

Digital assets can have a wide variety of use cases, ranging from serving as a medium of exchange (e.g., crypto assets) to representing rights to use a product or service or to obtain an asset (e.g., NFTs, a utility token, or an asset token). Companies are considering ways in which they can integrate digital assets into their operations and investment portfolios. A few examples include:

+ Accepting crypto assets as a form of payment
+ Investing in digital assets
+ Buying and selling digital art
+ Selling digital memberships and access to exclusive events

Companies are also considering the opportunities digital assets and blockchain technology can provide in improving payment settlement (e.g., decreasing time to and risk associated with settlement) and lending. This publication does not discuss these applications.

Companies are considering ways in which they can integrate digital assets into their operations and investment portfolios.

TRANSACTING

Increasingly more consumer-facing businesses are accepting, or considering

accepting, crypto assets as a form of payment for goods and services. According to audit partners surveyed in the CAQ's Summer 2022 Audit Partner Pulse Survey,[6] companies in the financial services and technology, telecommunications, media, and entertainment industries were the most likely to be considering or preparing for accepting crypto assets as a form of payment (51% and 43%, respectively). Some companies accept payments directly in crypto assets which they then commonly convert into fiat currency[7] within a short period. Others permit customers to make payments in crypto assets through intermediaries who accept the crypto assets on behalf of the seller and provide the seller with the fiat currency equivalent. These models result in different risks which are discussed below.

INVESTING

There are thousands of crypto assets. Currently, the two largest crypto assets (by market capitalization) are bitcoin (BTC) and ether (ETH). Retail and institutional investors, and even some publicly traded companies, are holding crypto assets as investments. Investors hold crypto assets for various reasons – speculative investing or as a store of value to name a couple. Crypto asset markets are in early stages compared to traditional markets and can be more volatile. Crypto asset investors may self-custody their assets or have a third-party custodian hold their assets. This publication discusses some of the risks associated with these forms of custody in more detail below.

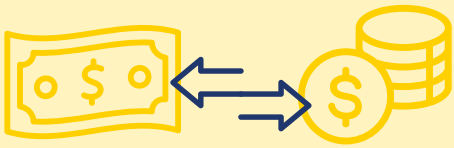
TOKENS AND NFTS

Tokenization refers to the process of digitally representing something of value, whether physical or intangible, for use on a blockchain. Tokenization has become increasingly popular with digital art, which is typically represented by NFTs. NFTs are tokens representing rights often to a one-of-a-kind or serialized digital item or sometimes to a unique physical good.

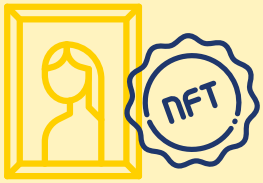
Other examples of tokenized assets include security tokens (representative of financial instruments) or asset tokens (representative of legal titles).

These are just a few use cases; however, new cases continue to arise.

FUNGIBLE VERSUS NON-FUNGIBLE ASSETS



A fungible asset is one that can be interchanged with another asset of the same type. For example, cash is fungible. A one-dollar bill can be readily interchanged for another one-dollar bill or for four quarters. The value is equivalent in each exchange. Examples of fungible tokens include bitcoin and ether.



A non-fungible asset is one that cannot be interchanged with another asset of the same type because another asset of the same type does not exist. For example, an original piece of artwork is non-fungible. It has unique qualities (e.g., originality) that change its value compared to a reprint or a different original work. Examples of non-fungible tokens include unique digital art or serialized collectibles.

6 Audit Partner Pulse Survey Q2 2022, Center for Audit Quality 2022
7 Generally accepted legal tender issued by a sovereign government (e.g., dollar, pound, and euro). Blockchain Universal Glossary, AICPA

QUESTIONS FOR MANAGEMENT

+ What are the company's objectives for engaging with digital assets?
+ Does the company have the requisite expertise to use, monitor, and report on digital assets?
+ Has management considered the tax, legal, regulatory, or financial reporting requirements that apply to the company related to its engagement with digital assets? Do these requirements call for external advice?

QUESTIONS FOR AUDITORS

+ What is the experience of the engagement partner and other senior engagement team members with digital assets? Would the firm be able to supplement the engagement team's expertise if necessary (e.g., by engaging qualified specialists)?
+ Does the audit firm have other similarly situated clients in the digital asset ecosystem?
+ Do the engagement partner and other senior engagement team members understand the company's objectives for engaging with digital assets?
+ Do the engagement partner and other senior engagement team members understand the applicable regulatory environment, and whether there is a risk an entity may not comply with laws and regulations?
+ What policies and procedures does the audit firm have regarding conducting and monitoring audit engagements involving digital assets, including considering the risks associated with performing such audits? Does the audit firm require some type of monitoring of these types of audits by other professionals in the firm?[8]

8 Spotlight - Audit Committee Resource, August 2022, PCAOB

Digital assets and risk

Given the inherent complexities associated with digital assets and blockchain technology, many risks arise. Some of the more common risks are addressed below, though these are not exhaustive. The risks associated with digital assets vary depending on use case and design decisions.

SAFEGUARDING PRIVATE KEYS AND CUSTODY

Cryptographic key pairs are the public and private keys needed to encode and decode encrypted messages on a blockchain network. Digital asset holders use their private keys to transfer their digital assets. Without the private key, the holder loses their ability to transfer their digital assets, perhaps permanently. If a private key is compromised, unauthorized parties could gain access to the related digital asset. This makes private key storage and safeguarding important to maintain the confidentiality, availability, and integrity of private keys and by extension the related digital assets.

Digital asset holders generally store their private keys and the associated public keys or blockchain addresses in a cryptographic wallet. These solutions range in ease of use and level of security in private key management (e.g., preventing destruction or misplacement, access, cybersecurity). It is important that companies develop effective processes and controls related to the safeguarding, storage, and use of their private keys. This can be complex and, in part, depends on the type(s) of cryptographic wallet the company uses and how the company custodies its digital assets.

Holders can store their private keys using self-custody or through a third-party custodian, exchange, or other service provider. With self-custody, it is the responsibility of the holder to ensure the safeguarding of their private keys.

A few questions to consider related to private key management using self-custody include:

+ How are the company's private keys generated and what are controls in place surrounding private key generation?

+ How are the company's private keys stored and backed up?

+ Who has access to or the ability to use the company's private keys?

+ Are multiple signatories required to use a private key?

+ Has the company ensured appropriate segregation of duties throughout the private key lifecycle?

+ How would the company address misplaced or misappropriated private keys?

On the other hand, third-party custodians can provide customers with a variety of financial services, most notably the safeguarding of their digital assets – similar to custody in traditional capital markets. Custodians often have significant technological expertise and can aid their customers in transacting with digital assets. However, the use of a third-party custodian gives rise to various risks such as counterparty risk (e.g., ability to effectively safeguard the company's digital assets or risk of default) and cybersecurity risk. The services provided by third-party custodians generally have defined features and controls in place to safeguard their customers' digital assets – sometimes supported by system and organization controls (SOC) reports; however, it is incumbent on users to perform due diligence over their relationship with the third-party custodian, including putting in place complementary user entity controls, if needed. If the third-party custodian cannot provide a SOC report, users should put in place controls to address the risks arising from use of the custodial service. Other risks arise depending on if a third-party custodian segregates or commingles customer accounts with those of other customers.[9]

A few questions to consider related to private key arrangements using a third-party custodian include:

+ Has the company performed due diligence in selecting a third-party custodian?

+ Can the third-party custodian initiate transactions on behalf of the company?

+ Does the third-party custodian commingle the company's digital assets with those of other depositors? If so, does it maintain records of the company's digital assets outside of the blockchain?

+ Does the third-party custodian have control of the company's digital assets?[10]

EXAMPLES OF CRYPTOGRAPHIC WALLETS[11]

Cold storage wallet. A wallet that is not connected to the internet, also referred to as an offline wallet.

Hardware wallet. A hardware (physical) device that generates private keys instead of software.

Hot storage wallet. A wallet that is accessible to the internet. This is the most common implementation of a wallet, which may be referred to as just a wallet.

Mobile wallet. A wallet that is accessed via a mobile app.

Multisig (multisignature) wallet. A wallet that requires two or more signatures to transfer a digital asset from a wallet address.

Physical wallet. Any medium used to store keys offline in physical form (e.g., paper wallet).

Software wallet. Refers to anything other than a hardware or physical wallet.

Third-party hosted wallet service. A third-party service provider who holds an entity's digital assets, also referred to as custodial wallet.

9 See Q&A 10 in the AICPA's 'Accounting for and auditing of Digital Assets practice aid' for additional questions to consider in risks arising from and evaluating control over digital assets when using a third-party custodian.
10 Ibid.
11 Blockchain Universal Glossary, AICPA

- Does the third-party custodian perform a reconciliation of its independent records to the blockchain?

- Can the third-party custodian provide a SOC report that contains control objectives relating to generation, security, and monitoring of the keys used? For example,
  - Has the company obtained and reviewed it and implemented relevant complementary user entities controls?
  - How has the company evaluated the controls over the safeguarding of assets held by the third-party custodian?

- Does the third-party custodian engage a sub-custodian to safeguard the company's assets?

CYBERSECURITY

While blockchains storing digital assets instill a degree of confidence between transacting parties, the digital nature of the blockchain and digital asset ecosystem makes it a target for bad actors. Cybersecurity is interrelated with safeguarding private keys and is applicable whether a company self-custodies its digital assets or uses a third-party custodian. Companies must prevent cyber attackers from accessing and misappropriating their private keys, and consequently their digital assets. However, considerations for cybersecurity go a step further.

The way blockchain protocols and digital exchanges or platforms are set up, and how holders interact with them, can create opportunities for bad actors. For example, there have been recent instances of blockchain code being exploited to misappropriate crypto assets. Similarly, for cryptographic wallets that are accessible to the internet (a hot storage wallet), cyber attackers may be able to take advantage of that connection if not securely designed and maintained. Companies should establish cybersecurity protocols related to how they store and use their private keys and obtain an understanding of and comfort over cybersecurity at the exchanges or platforms on which they transact, and on the cryptographic wallets and third-party custodians they use, among others.

ANTI-MONEY LAUNDERING AND KNOW YOUR CUSTOMER

Certain blockchains provide pseudo-anonymity to their users. Some use this pseudo-anonymity to engage in illicit activities. To stay compliant with relevant laws and regulations, companies engaging with digital assets should consider establishing know-your-counter party (KYC) and anti-money-laundering (AML) processes and controls. Companies may also need to evaluate how the digital asset exchanges or platforms on which they transact address these laws and regulations, among others.

ACCOUNTING

The words cryptocurrency and stablecoins (discussed below) include the words 'currency' and 'coins' and can be used to transact or invest. Therefore, some conflate these digital assets with traditional currency, like coins or paper money – just in a digital format. Contrary to conventional thinking, these types of digital assets are different from traditional currency in the US.[12] Digital assets are not backed by the US government as an official currency, nor are they widely accepted as a medium of exchange (i.e., they are not legal tender). This means that digital assets like these are not accounted for as cash and, at present, are most often accounted for as intangible assets.

Digital assets have unique features that can result in complex accounting treatments under existing standards. These standards did not originally contemplate such assets, and their application may result in accounting conclusions that do not reflect the economics of a transaction. Read on for examples of accounting treatments that those who engage with digital assets might encounter.

Companies should understand all the details of the digital assets transactions into which they enter and develop robust accounting policies. Companies should also consider if they have the

12 The U.S. Department of the Treasury defines "currency" as, "[t]he coin and paper money of the United States or of any other country that is designated as legal tender and that circulates and is customarily used and accepted as a medium of exchange in the country of issuance", Title 31 CFR § 1010.100.

appropriate skill sets to determine the proper accounting treatment for these transactions. Advanced consideration, including discussion with your external auditor, can save time, effort, and risk exposure down the line.

VALUATION

Digital asset markets operate differently from traditional capital markets, not to mention some crypto assets are highly volatile. These and other factors give rise to certain challenges in the valuation of digital assets. In most cases, digital asset markets are always open, and the same digital asset may trade in multiple markets to which a company has access. Companies engaging with digital assets should consider how they determine market close (e.g., local close of business, midnight in a certain time zone), how they monitor pricing of their digital assets, and which is a given digital asset's principal market. Similarly, companies should also consider the consequences that the volatility of crypto assets may have on the value of their transactions and holdings over time.

Other digital assets, like NFTs, are one-of-a-kind. Conventional approaches to valuation may be difficult to apply. Consider an NFT collectible, like digital art. NFTs like these sometimes sell at auctions or through online marketplaces; however, the price for which an NFT collectible last sold does not necessarily reflect the current value for which a willing buyer and seller would transact. Factors that may influence NFT fair value, like rarity, utility, liquidity premiums, and others, are difficult to quantify.

DIGITAL ASSETS ACCOUNTING RESOURCES

In response to the complexities associated with the accounting for digital assets, accounting experts have published non-authoritative guidance and thought leadership on how to apply existing accounting rules to digital assets in various circumstances. A useful example is the AICPA's 'Accounting for and auditing of digital assets' practice aid.[13]

REGULATORY ENVIRONMENT

Congress and regulators, like the SEC, CTFC, and others, are paying close attention to digital assets. Given how new the digital assets market is, there is a lack of clarity regarding digital assets regulation and which regulatory bodies have jurisdiction over which digital assets. This regulatory uncertainty poses risks to those engaging with digital assets and changes to the existing regulatory landscape could have large impacts on companies holding or otherwise engaging with digital assets. Later, the publication discusses the regulatory state of play at a high level.

13 Accounting for and auditing of Digital Assets practice aid, AICPA

Digital assets in the financial reporting ecosystem

CRYPTO ASSETS

Most commonly, companies use crypto assets as investments. Examples of crypto asset investments include:

- Investments in crypto assets or digital assets held in a cryptographic wallet owned and managed by the company.
- Investments in crypto assets or digital assets held in a cryptographic wallet managed by a third-party service provider.
- Exposure to crypto assets or digital assets through derivatives.

In most cases, crypto assets held by a company are recorded as an indefinite-lived intangible asset pursuant to the guidance in Accounting Standards Codification (ASC) 350, *Intangibles – Goodwill and Other* (ASC 350). Such assets are assessed at least annually for impairment and must be written down between annual assessments if a triggering event indicates they more likely than not impaired. Under ASC 350, assets are not written back up to fair value.

Crypto assets received as consideration for goods or services may result in complex revenue

Consider the following simplified example:

On April 5, 202X, Company A purchases ten units of Crypto X, a crypto asset, for $200 per unit (total fair value of $2,000). Company A analyzes the features of Crypto X and determines Crypto X should be accounted for as an indefinite-lived intangible asset.

On May 10, 202X, the fair value of Crypto X falls to $150 per unit, and Company A concludes Crypto X is impaired. Company A writes down the value of Crypto X on its balance sheet to $1,500 (10 units at $150 per unit) and records a $500 loss on its statement of operations. Assume there are no other decreases to the fair value of Crypto X.

On June 15, 202X, the fair value of Crypto X increases to $300 per unit.

As part of its quarterly close, the Company considers the value of its ten units of Crypto X as of June 30, 202X. Given Crypto X is an indefinite-lived intangible asset under ASC 350, Company A must value Crypto X at $1,500 (the impaired value) even though there was a subsequent increase in fair value during the period.

accounting under ASC 606, *Revenue from Contracts with Customers* (ASC 606). Other transactions involving crypto assets may trigger nonmonetary transaction accounting, derivative accounting, or other specialized guidance.

MAKING AND ACCEPTING PAYMENTS IN CRYPTO ASSETS

There are some companies who accept or make payments in crypto assets, including compensating employees in crypto assets. There are several ways companies can facilitate purchases or payments in crypto assets with varying degrees of accounting and operational impacts. One key aspect is whether a company custodies crypto assets at any point during the purchase or payment process.

Consider a few examples:

+ *Company A elects to pay some of its employees in Crypto X, a crypto asset. Company A purchases and holds Crypto X which it then uses to make payroll payments to its employees by direct deposit into their cryptographic wallets. This example introduces a host of accounting considerations and operational/financial risks for Company A given that Company A has taken custody of a crypto asset. See discussion of some risks below.*

+ *Assume the same facts as above, except Company A does not purchase Crypto X. Rather, Company A pays a third-party service provider in cash to make payroll deposits to its employees in Crypto X. While there are still certain complexities associated with this model, Company A does not interact directly with Crypto X which mitigates some of the custodial and other risks associated with holding and making payments in Crypto X.*

A few risks to consider related to accepting and making payments in crypto assets include:

+ **Price volatility** – Changes in fair value between transaction execution and settlement of payment or receipt may impact the value of the exchange. For products or compensation denominated in crypto assets, price volatility and settlement timing may impact the ultimate value of fiat currency exchanged for goods and services.

+ **Compatibility with existing systems** – Typical enterprise reporting systems (ERPs) are not set up for crypto assets. For example, traditional ERPs allow for recording transactions with up to two decimal places. Bitcoin is denominated in eight decimal places, and ether is denominated in eighteen decimal places. The truncation of these decimal places under a traditional ERP could result in significant differences in value depending on the quantity of tokens in a transaction. So, making or accepting accurate payments in crypto assets may require additional IT systems. The implementation of new IT systems creates risks related to how it interfaces with existing systems and how systems are reconciled, among others.

+ **Regulatory and tax uncertainty** – Changes to regulations and tax laws may impact, or hinder, making or accepting payments in crypto assets.

STABLECOINS AND CENTRAL BANK DIGITAL CURRENCIES

Some crypto assets were originally designed to function like traditional currency, specifically as a digital store of value, medium of exchange, and unit of account. However, enterprise adoption of crypto assets has not picked up, in part due to price volatility. Recently, stablecoins have emerged as a type of digital asset seeking to mitigate volatility concerns. To do this, a stablecoin issuer attempts to 'peg' (or link) the value of the stablecoin to that of a fiat currency (typically, the US Dollar). In many cases, a stablecoin is backed by its peg. For example, USD Coin (USDC) is a stablecoin that is pegged to the US dollar and backed with high-quality liquid assets. A well-designed and appropriately managed stablecoin effectively acts as a fiat proxy on a blockchain. However, a stablecoin's success relies heavily on the ability of its issuer to maintain the peg.

The accounting for stablecoins is dependent on the features of the coin, which can differ from those of crypto assets (e.g., redemption rights, legal form debt or equity, or other rights and obligations). In some circumstances, stablecoins may meet the definition of a financial asset and be accounted for under ASC 310, *Receivables* (ASC 310), or ASC 320, *Investments – Debt Securities (Topic 320)* (ASC 320).

Some countries are exploring or have already established central bank digital currencies, or

CBDCs. While some stablecoins are pegged to fiat currencies, CBDCs differ in that they represent a digital version of legal tender (i.e., cash) issued by a central monetary authority. For example, the Peoples Bank of China is currently piloting its digital yuan (e-CNY).[14]

NFTS

Recently, NFTs have received significant attention – particularly in the gaming industry and creative communities with the development of digital games and art. NonFungible.com and L'Atelier BNP Paribas released a study in March 2022 which found that NFT sales reached $17.7 billion in 2021, up from $82.5 million in 2020.[15] Others have begun to develop NFTs representing digital sports collectibles, club memberships, and event tickets. NFTs can also be used, albeit less often at present, in provenance applications (e.g., supply chain) or for the storage of personal data (e.g., healthcare, or personal identification information).

Issuers and sellers of NFTs must focus carefully on the nature of their NFTs. Often, the sale of an NFT will be recorded under ASC 606; however, even under ASC 606 careful consideration is required to appropriately account for the sale of an NFT to a customer. A few questions to consider related to NFTs which ultimately impact the accounting conclusion may include:

+ What rights does the NFT confer to the buyer?
+ What obligations are borne by the issuer?
+ Are there any licensing features to consider by either the issuer or buyer?
+ Are there any fractional ownership rights conferred to the buyer?

For example, a seller may retain ownership of digital art and grant a purchaser of an NFT an exclusive license to use and display such digital art. In this circumstance, the company should consider the supplemental guidance in ASC 606 that addresses the licensing of IP.[16]

The introduction of third parties like custodians or exchanges means that companies will need to perform robust due diligence.

IMPACT ON ACCOUNTING AND AUDITING

The nature of transactions on the blockchain may involve third parties that companies must consider. The introduction of third parties like custodians or exchanges means that companies will need to perform robust due diligence and other third-party risk management activities to ensure their assets are secure. Other third-party service providers, like digital asset accounting platforms, may also be involved in the financial reporting process. These third parties help companies with digital asset-specific needs in financial reporting and analysis. In some cases, these third parties may provide SOC reports or other service auditor reports to support due diligence and internal controls over financial reporting. In other cases, such information may not be available. Companies and their auditors should be prepared for these potential outcomes.

Technological intricacies introduced by blockchain give rise to additional complexities. Both the companies and their auditors should be aware of the types of data and reporting a blockchain can

14 Behind the Scenes of Central Bank Digital Currency, IMF 2022
15 Yearly NFT Market Report – 2021, Nonfungible.com 2022
16 The Metaverse — Accounting Considerations Related to Nonfungible Tokens, Deloitte 2022

produce and whether it is suitable for financial reporting, maintaining effective internal controls, and providing sufficient and appropriate audit evidence. When a blockchain is developed, its coding is agreed upon and difficult to change. Users are subject to the protocols established by the code which can be less than optimal if not carefully developed. Companies should evaluate the blockchains they interact with to ensure they are technologically sound. A failure of the blockchain itself presents risks like a lack of data availability or reliability which are integral for companies to maintain their books and records.[17]

COSTS OF ENGAGING WITH DIGITAL ASSETS

Transacting on a blockchain is not without cost. Like transaction costs companies pay in the form of bank fees and other service costs, many blockchains require users to make payments to transact. For example, transacting on the Ethereum blockchain requires transaction fees to be paid in ether, referred to as 'gas' fees. Other blockchains have similar mechanisms that are used to compensate others on the blockchain for 'mining' blocks (i.e., recording transactions).

Gas and similar fees are often variable, dependent on transaction traffic among other things. The more traffic, the higher the fees.

QUESTIONS FOR MANAGEMENT

- Has management considered the risks associated with the use of digital assets?
- Has management considered what internal controls it will need to design and implement for reporting and safeguarding digital assets?
- Will third-party involvement be required for management to engage in digital asset transactions?
- Has management considered all potential impacts to the financial statements arising from the company's involvement with digital assets?

QUESTIONS FOR AUDITORS

- What is the auditor's understanding of the financial reporting implications of the company's planned activities related to digital assets?[18]
- Does the auditor have access to specialized technology-based audit tools needed to identify, assess, and respond to risks of material misstatement?
- Has the auditor considered the challenges that may arise in obtaining sufficient appropriate audit evidence for the company's digital assets?
- How does the audit firm monitor auditor independence considerations associated with audit engagements involving digital assets (e.g., monitoring whether its staff invests in digital assets, holds an account on an exchange or with a third-party custodian, or engages in crypto asset mining activity)?

17 Blockchain Risk Considerations for Professionals, ISACA and AICPA & CIMA 2021
18 Spotlight - Audit Committee Resource, August 2022, PCAOB 2022

Digital assets: Regulation and standard setting

While there are some similarities and some fundamental differences between digital assets and existing assets classes in today's financial markets, regulators in the US are taking a step back to consider the original intent behind existing rules and regulations over the capital markets and determine how those may apply to or perhaps can be modified or supplemented for digital assets.

ON THE HILL

In March 2022, President Joe Biden signed an 'Executive Order on Ensuring Responsible Development of Digital Assets' (the Executive Order). In essence, it is a directive to government agencies to form committees to research and form a regulatory framework for digital assets. The White House framed this as, "the first ever, whole-of-government approach to addressing the risks and harnessing the potential benefits of digital assets and their underlying technology."[19] In July 2022, Department of the Treasury's Office of Financial Research released white paper regarding a 'digital dollar', a CBDC, in response to this Executive Order.

Congress is also exploring bills related to the regulation of digital assets, particularly crypto assets and stablecoins.

AT THE SEC AND CTFC

Facts and circumstances dictate that some digital assets are securities and others are commodities. This is important as securities and commodities fall under different regulatory jurisdictions in the United States. The Securities and Exchange Commission (SEC) has authority over securities, while the Commodities and Futures Trading Commission (CFTC) has authority over the commodities markets.

In August 2022, Senators Debbie Stabenow (D-MI) and John Boozman (R-AR) introduced the Digital Commodities Consumer Protection Act of 2022. It seeks to clarify primary regulatory jurisdiction over crypto assets at the federal level, giving the CFTC authority over digital commodities, a newly defined asset class that would encompass crypto assets that are not defined as securities, for example BTC and ETH.

Companies must understand the nature of the digital assets with which they engage and how they are transacting with them. Slight differences could result in different jurisdictional regimes and regulatory frameworks. Similar agencies at the state level and around the world are also monitoring developments in their markets and

19 President Biden to Sign Executive Order on Ensuring Responsible Development of Digital Assets, White House 2022

establishing regulations and frameworks of their own to address digital assets.

The enforcement arms of both the SEC and CFTC have been active in the digital asset ecosystem, issuing enforcement actions for alleged unregistered securities offerings, failures to register trading platforms, AML violations, and misrepresentations related to coin offerings to name a few. Some companies have received comment letters from the SEC related to their engagement with digital assets. To date there have been forty-nine comment letters discussing digital assets in Form 10-K filings, focusing on topics ranging from MD&A disclosure, fair value measurement, revenue recognition, and non-GAAP disclosures.[20]

As another example, in March 2022, the SEC issued Standards Accounting Bulletin (SAB) No. 121. The SAB provides interpretive guidance for companies that have an obligation to safeguard their customers' "crypto-assets." This results in those who custody "crypto-assets" recording a safeguarding liability for those assets regardless of whether they control them, a big change from how custodians typically reflect custodial arrangements.

AT THE FASB AND PCAOB

In May 2022, Financial Accounting Standards Board (FASB) added a project to its technical agenda seeking to improve the accounting for and disclosure of certain digital assets. The project is in early stages, and in August 2022, the FASB narrowed the scope of the project to focus on fungible tokens. Additionally, the Public Company Accounting Oversight Board (PCAOB) released a spotlight, 'Audits Involving Cryptoassets',[21] addressing certain responsibilities under PCAOB standards for auditors of issuers transacting in or holding crypto assets.

There were thirty-two critical audit matters (CAMs) related to digital assets for twenty-one distinct companies in Form 10-K and 20-F filings for fiscal year 2021.[22] This is up from eighteen such CAMs[23] in similar filings for fiscal year 2020. We have summarized some common CAM themes to the right.

Theme	Number of CAMs
Revenue from contracts with customers	14
Existence, valuation, and/or control of digital assets	10
Overall accounting and disclosure of digital assets	6
Other	2
Total	32

OTHER REGULATORS

Numerous other regulatory and legislative bodies in the US have taken an interest in the digital asset space. A few of the other regulators and some of their areas of interest include:

+ **Banking and treasury regulators** (e.g., the Federal Reserve, the Federal Deposit Insurance Corporation, the Office of Foreign Assets Control, and the Office of the Comptroller of the Currency): Evaluation of the risks and opportunities crypto assets and other digital assets present in the banking and treasury spaces
+ **Consumer Finance Protection Bureau:** Consumer protection issues
+ **Financial Crimes Enforcement Network:** AML and Bank Secrecy Act matters, among others
+ **State legislatures:** Regulation of crypto assets and other digital assets at the state level

20 Audit Analytics Comment Letter database as of July 14, 2022 (Search terms: cryptocurr*, Bitcoin, "digital asset")
21 Spotlight - Audits Involving Cryptoassets, Information for Auditors and Audit Committees, PCAOB
22 Audit Analytics CAM database as of July 14, 2022 (Search terms: "digital asset", crypto*, "blockchain", NFT for Fiscal Year 2021)
23 Audit Analytics CAM database as of July 14, 2022 (Search terms: "digital asset", crypto*, "blockchain", NFT for Fiscal Year 2020)

Conclusion

As the digital assets landscape continues to develop, the related risks will evolve, and audit committee oversight will be at the forefront. An understanding of digital assets, an awareness of the risks they present to financial reporting and inquiring with management and the auditor are essential tools for audit committees to discharge their responsibilities.

Appendix A:
Questions for auditors and management

OVERALL
Questions for management

+ What are the company's objectives for engaging with digital assets?
+ Does the company have the requisite expertise to use, monitor, and report on digital assets?
+ Has management considered the tax, legal, regulatory, or financial reporting requirements that apply to the company related to its engagement with digital assets? Do these requirements call for external advice?
+ Has management considered the risks associated with the use of digital assets?
+ Has management considered what internal controls it will need to design and implement for reporting and safeguarding digital assets?
+ Will third-party involvement be required for management to engage in digital asset transactions?
+ Has management considered all potential impacts to the financial statements arising from the company's involvement with digital assets?

Questions for auditors

+ What is the experience of the engagement partner and other senior engagement team members with digital assets? Would the firm be able to supplement the engagement team's expertise if necessary (e.g., by engaging qualified specialists)?
+ Does the audit firm have other similarly situated clients in the digital asset ecosystem?
+ Do the engagement partner and other senior engagement team members understand the company's objectives for engaging with digital assets?
+ Do the engagement partner and other senior engagement team members understand the applicable regulatory environment, and whether there is a risk an entity may not comply with laws and regulations?

+ What policies and procedures does the audit firm have regarding conducting and monitoring audit engagements involving digital assets, including considering the risks associated with performing such audits? Does the audit firm require some type of monitoring of these types of audits by other professionals in the firm?

+ What is the auditor's understanding of the financial reporting implications of the company's planned activities related to digital assets?

+ Does the auditor have access to specialized technology-based audit tools needed to identify, assess, and respond to risks of material misstatement?

+ Can the auditor obtain sufficient appropriate audit evidence related to the company's financial reporting and internal controls over financial reporting related to the company's digital assets?

+ How does the audit firm monitor auditor independence considerations associated with audit engagements involving digital assets (e.g., monitoring whether its staff invests in digital assets, holds an account on an exchange or with a third-party custodian, or engages in crypto asset mining activity)?

SELF-CUSTODY

Questions for management

+ How are the company's private keys generated and what are controls in place surrounding private key generation?

+ How are the company's private keys stored and backed up?

+ Who has access to or the ability to use the company's private keys?

+ Are multiple signatories required to use a private key?

+ How would the company address misplaced or misappropriated private keys?

THIRD-PARTY CUSTODY

Questions for management

+ Has the company performed due diligence in selecting a third-party custodian?

+ Can the third-party custodian initiate transactions on behalf of the company?

+ Does the third-party custodian commingle the company's digital assets with those of other depositors? If so, does it maintain records of the company's digital assets outside of the blockchain?

+ Does the third-party custodian have control of the company's digital assets?

+ Can the third-party custodian provide a SOC report that contains control objectives relating to generation, security, and monitoring of the keys used?

  - If so, has the company obtained and reviewed it and implemented relevant complementary user entities controls?

  - If not, how has the company evaluated the controls over the safeguarding of assets held by the third-party custodian?

Does the third-party custodian engage a sub-custodian to safeguard the company's assets?

NFTs

Questions for management

+ What rights does the NFT confer to the buyer?

+ What obligations are borne by the issuer?

+ Are there any licensing features to consider by either the issuer or buyer?

+ Are there any fractional ownership rights conferred to the buyer?

CAQ

www.thecaq.org

We welcome your feedback!

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