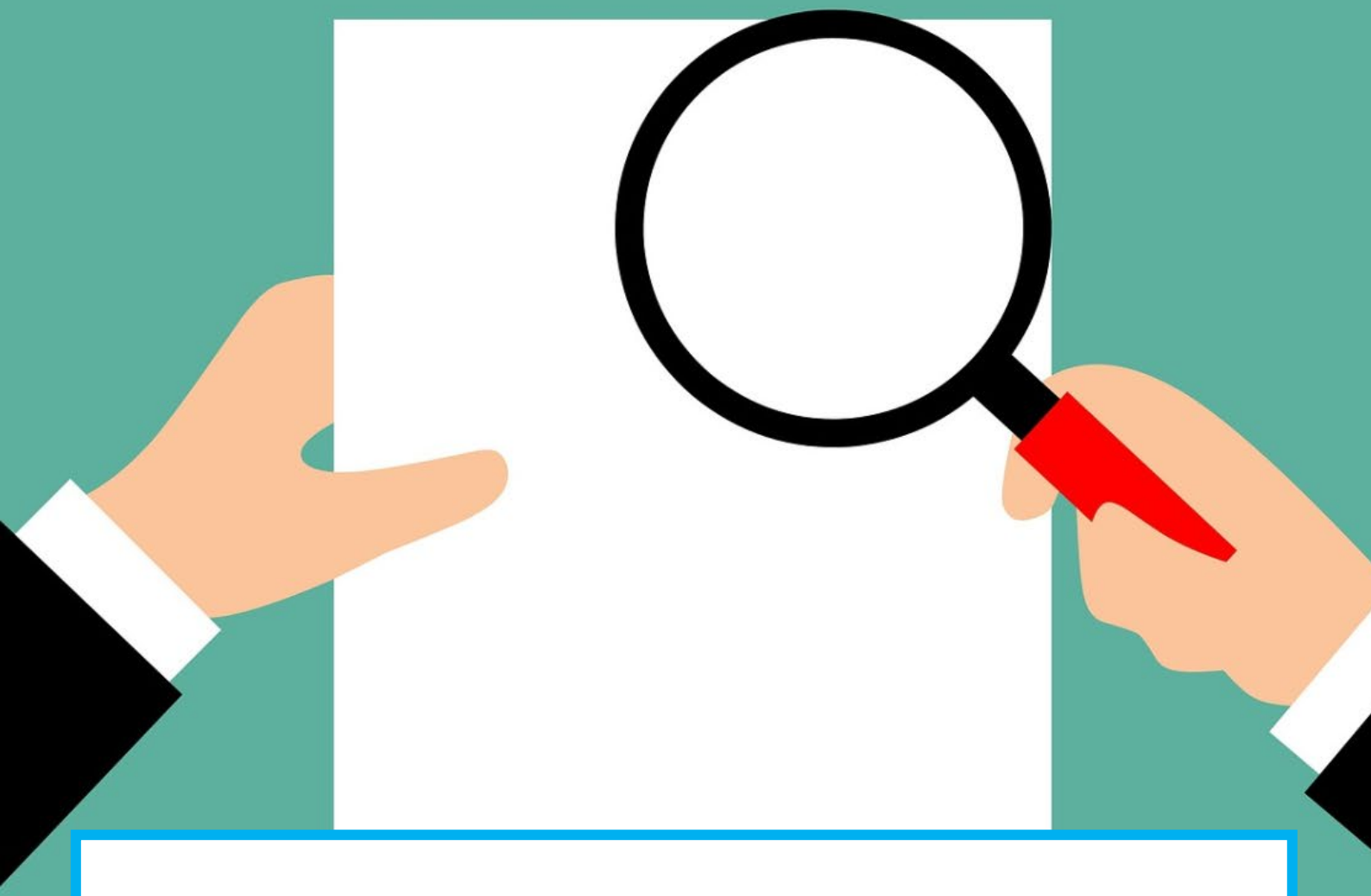

MOORE

Key Considerations for Audits with Digital Assets

Blockchain Collaboration Group
April 2019

Moore International Limited

About Moore

Moore International Limited has grown to be one of the largest international accounting and consulting groups worldwide. Today the network comprises 609 offices in 112 countries throughout the world, incorporating 30,569 people and with fees of more than US$3.06 billion.

Moore International member firms recognise the commercial importance of providing assurance on your business controls and, ultimately, satisfying regulatory requirements. However, our member firms offer much more than just a basic compliance service. They understand the need to provide advice to help you develop your business and achieve your commercial objectives.

The key to a valuable compliance service is the strength of the relationship between the client and the service team. This enables our member firms' work to be thoroughly and accurately planned and tailored to each client's specific needs.

This document was put together in conjunction with our member firm, Armanino LLP, the largest independent accounting firm in California and a top 25 firm within the United States.

Global Blockchain Group

Blockchain technology is not only in vogue, it is starting to disrupt the incumbent payments industry by delivering enhanced speed, security and transparency. The days of waiting for settlement look to be numbered. Transfer of other tokenized digital asset (including derivatives) in the wider asset management industry now include stable coins, real estate, loans, letters of credit and insurance products. We share our audit and accounting observations in this rapidly evolving industry to help management plan for more seamless audit and accounting services, some of which can be delivered in near real time with the correct tools, planning and experience. Our Global Blockchain Group was established to facilitate our clients from around the world to navigate through these changing times.

If you would like to discuss how Moore Stephens network firms can support your organisation's approach to digital assets, please get in touch.

Global Blockchain Leaders

Andries Verschelden
Partner-In-Charge, Blockchain
408.240.4904
Andries.Verschelden@armaninoLLP.com

David Walker
Managing Director, Moore Stephens Cayman
david.walker@moore.ky

Table of Contents

An Introduction

In 2017, cryptocurrencies and other blockchain projects experienced rises in value. In 2018, trading prices for the top cryptocurrencies corrected downward — some would say "bottomed out." (See Figure 1.)

However, initial coin offerings (ICOs) and start-up projects abounded, almost doubling in number versus the prior year. (See Figure 2.) Venture capital and retail investor funds have continued to pour into the space, which has now gained the attention of institutional investors. With fewer viable projects (i.e. those with a demonstrated use case and a strong development team to monetize their crypto solutions) and with investor demand chasing returns, the decline in the market has moderated.

Figure 1: Global Market Cap, May 31, 2017, to December 2018

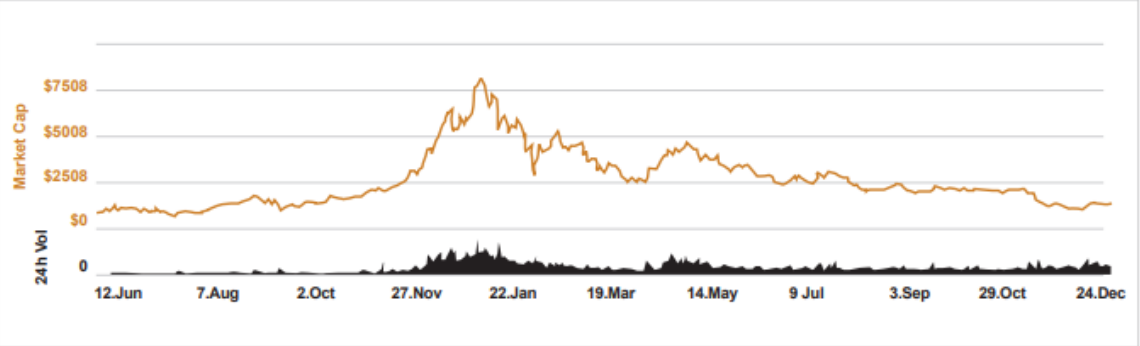

Figure 2: Summary of Initial Coin Offerings by Year

	Year of Close Date				
	2014	2015	2016	2017	2018
ICO Size ($mn)	30	9	256	5,482	16,718
Average	4	1	6	16	26
Median	2	1	1	8	10
Max.	18	5	152	262	4,200
Min.	0	0	0	0	0
Std. Dev.	7	2	23	28	173
Number of ICOs	7	7	43	343	650

With the explosion of companies venturing into the world of cryptocurrencies[i] in the last few years, auditors are being called on to apply their skills, and the attest standards, to new and unfamiliar scenarios. In applying current accounting and auditing standards in this emerging and evolving space, auditors are faced with new challenges, including: understanding the environment of internal controls and risks unique to blockchains; understanding the underlying technologies, including internally developed platforms to support blockchain transactions; and developing appropriate audit procedures over digital asset transactions and balances.

The scoping and execution challenges now extend beyond “crypto-native” companies and projects — such as exchanges and miners — to non-crypto-native organizations holding crypto, investing in crypto, or transacting in crypto. Crypto asset balances are finding their way to more balance sheets.[ii] In a few years, auditing cryptocurrency transactions and balances will be part of most auditors’ toolkits. For now, it remains the domain of those with specific technical knowledge and tools.

Practical Applications

The purpose of the following guide is twofold:

1. To help management understand the factors that play into audit scoping considerations, as well as execution. These factors will direct the time and effort it takes to sufficiently test the existence, rights and completeness of the accounts holding digital assets. Management should expect questions surrounding these topics during the proposal process and should assess potential auditors based on their knowledge of these areas.

2. To provide some insight into how an audit approach to digital assets can be applied, share best practices used to streamline our audit from management's perspective, and share our expertise in this industry as professional guidance and standards continue to catch up.

A major takeaway is that all companies with a balance sheet or income statement containing digital assets cannot be treated equally. In fact, the level of risk, as well as the execution and delivery efforts of the auditor, can increase or decrease significantly depending on the considerations discussed below.

Note: This white paper focuses on the scoping considerations related to digital assets stored on public blockchains, and it does not necessarily include all potential technical accounting considerations (e.g., classification, exchange rates, disclosures). This white paper does not cover considerations for traditional audit cycles, impacts of information technology and application controls, regulatory and legal considerations, or security controls and measures.

Scoping Considerations

Financial Statement Composition

Financial Statement Accounts	Segregated vs. Commingled Accounts	On vs. Off Balance Sheet
How many balance sheet accounts hold digital assets and how material are the dollar amounts?	Do the financial statement accounts hold multiple digital assets within a single account?	Does the company hold all digital assets on the balance sheet?
What income statement accounts are affected by digital asset transactions and how material are the dollar amounts?	Do the financial statement accounts hold a single wallet, multiple wallets, and/or a hierarchical deterministic (HD) wallet[iii] within a single account?	Does the company act as a custodian for third parties?

Audit Impact. As with all audits, gaining a general understanding of the makeup of the financial statements is of utmost importance. When a company holds digital assets, there is an added complexity that should be considered and documented.

It is key to understand the breakdown of accounts that are composed of or transact in digital assets, including the currencies and wallets making up these accounts. Similar procedures should be performed for digital assets that are held off balance sheet. Another key insight from the financial statements is determining materiality and scoping from an account perspective. Once audit considerations and scoping mechanisms are applied, auditors will have a general outline for scope. However, until the underlying blockchains, wallets and third-party custodians (see sections 2-4) are noted, the full scoping picture will not be apparent.

MANAGEMENT INSIGHT: If possible, segregate financial statement accounts by currency and use case. Along with simplifying internal accounting processes, segregated accounts disperse risk among the financial statement accounts. Segregated accounts also ease the auditing process for both external auditors and a company's internal finance team (as the finance team will be providing the related supporting documentation).

Scoping Considerations

Blockchain & Digital Assets

Network Currency vs. dAppiv Token vs. Other

Are the digital assets native to the given network and used to incentivize participating nodes? For example: bitcoins (BTC) on the Bitcoin network, ether (ETH) on the Ethereum network.

What are the crypto assets' intended uses or utility (other than speculation)?

Are the assets "built on top" of an existing network? For example: ERC-20 tokens built on the Ethereum network, NEP-5 tokens on the NEO network.

Do the digital assets in scope include non-fungible tokens (NFTs) or other "tokenized assets"?

Blockchain Security

What is the consensus mechanism used to govern the underlying in-scope blockchains?

How much hash power is currently supporting the in-scope blockchains?

Audit Impact. From an auditor's perspective, it is key to understand the underlying blockchains that the crypto assets are native to. Along with gaining comfort over the network security considerations of each blockchain,[v] the auditor will use the list of in-scope blockchains to determine what type of node explorers or external tools will be needed.

MANAGEMENT INSIGHT: Building "on top" of – or acquiring digital currencies or tokens built "on top" of – blockchains is advised. During an audit, the benefits of this are twofold. Network security is typically greater (hash rates and network participants/nodes), and the data and tools available are much more robust. If tools are unavailable for smaller blockchains to verify transactions or ownership, the auditor may have to qualify the audit opinion.

Scoping Considerations

Wallet Structure

Hierarchical Deterministic (HD) vs. "Just a Bunch of Keys" (JBOK)	Single-Signature vs. Multi-Signature & Multifactor Authentication (MFA)	Single-Use vs. Multi-Use	Key Storage and Transaction Broadcast
Are keys generated in a deterministic fashion stemming from a master key set? Are keys generated individually?	Do transactions require a single signer or multiple signers to send funds? What is the M of N "secret-sharing scheme"? Do online custodial or other wallets require an MFA code or password?	Are key sets used for multiple transaction sends or discontinued after a single spend?	What is the digital asset breakdown between cold and hot wallets? How are private keys managed and stored (e.g., paper, hardware wallet)? Are third-party tools used to create and manage keys and sign transactions (Electrum, Litecoin Core)? Is management willing to send funds or use digital signatures as part of the audit procedures?

Audit Impact. Along with general considerations of volume, wallet structure will most likely have the largest impact on the scope of the digital assets audit. HD wallets will be easier to manage than an assortment of JBOK (independently generated) wallets. The number of key signers (multi-sig)[vii] also tends to increase the time needed to perform audit procedures. In general, the easier the digital assets are to transfer (e.g., single signature, hot wallets), the easier it will be to perform the audit procedures. However, this trade-off for ease of use is accompanied by an increase in security risk. The auditor should also understand the tools used by the company to create the keys, as well as the process to sign and broadcast transactions. Depending on the complexity of the wallet schema, the auditor should be prepared to use node explorers, QR code technologies and various client software.

The scoping and execution challenges now extend beyond "crypto-native" companies and projects — such as exchanges and miners — to non-crypto-native organizations holding crypto, investing in crypto, or transacting in crypto. Crypto asset balances are finding their way to more balance sheets.[ii] In a few years, auditing cryptocurrency transactions and balances will be part of most auditors' toolkits. For now, it remains the domain of those with specific technical knowledge and tools.

MANAGEMENT INSIGHT: As security is of utmost importance, the company should not take measures detrimental to security for the sake of an "easier" audit. However, management can ensure a smooth audit by documenting policies and procedures related to key creation and transaction signing/broadcasting. Management should also be willing to prove ownership of wallets, either via sending funds or digital signatures. Management should also keep all keys for any wallets that held crypto assets for three or more years!

If a company's operations will support the use of HD wallets, they significantly reduce the number of procedures performed by an auditor to ensure proper ownership of those wallets.

And a note on standard security measures: Following the Cryptocurrency Security Standard (https://cryptoconsortium.org/standards/CCSS) is always highly encouraged; however, most items outlined by the C4 fall outside the standard financial statement audit scoping considerations.

Scoping Considerations

Exchange or Third-Party Custodial Wallets and Accounts

Access	Confirmation & Custody
Does management have access to current and historical account data?	Are the exchanges available to perform account balance confirmations (if necessary)?
Does management use two-factor authentication (2FA) or a multi-signature account?	Is the exchange reputable? Has it had a material breach in its operating history?

Audit Impact. The auditor will need to ensure that access to the exchange account (and underlying wallets), as well as transaction data, is sufficient and appropriate to perform audit procedures. If the exchange account is no longer accessible, the auditor should be assured a balance confirmation (comparable to a bank confirmation) is attainable.

MANAGEMENT INSIGHT: Keep access passwords and 2FA for the associated exchange accounts, even if no longer in use. Historical data may be needed from these accounts during an audit. Developing relationships with reputable exchanges that may be able to provide historical account balance confirmations is an added safety net.

Scoping Considerations

Overall Volume

Transaction	Wallets
What is the transaction volume by currency, wallet and account?	How many wallets held digital assets at any point during the fiscal year?

Audit Impact. The number of wallets and transactions can have a significant impact on the scope of an audit. The auditor should ask about the overall volume of the operation, in conjunction with other significant items (e.g., wallets, blockchains)

MANAGEMENT INSIGHT: In terms of audit preparation, management typically does not have much control over operational aspects that affect the audit scope. However, management should be aware that increases in wallet number and structure, transaction volume, in-scope blockchains, and reporting mechanisms have a material and varying effect on audit scope.

Scoping Considerations

Reporting Capabilities

Customized Accounting Systems vs. Third-Party Solutions

Are third-party tools used to track digital assets?

Are internally developed tools used to track digital assets?

Does the company rely on manual compilations or manual uploads for tracking?

Are custom or “out-of-the-box” integration packages used for digital asset data transfers?

Does the system provide a sufficient audit trail?

Customized Accounting Systems vs. Third-Party Solutions

Do the reporting or inventory tools offer third-party assurance reporting, such as a SOC 1 and/or SOC 2 report, that management and auditors can rely on?

Has the underlying report logic been tested and validated? For custom reports and queries, can management provide raw queries for review, and rerun key reports for completeness and accuracy checks?

Does the homegrown software or database, third-party software, or other reporting mechanism have the necessary fields (schema) to perform the testing over digital assets (e.g., timestamp, transaction ID, amount)?

Does the homegrown software or database, third-party software, or other reporting mechanism have the ability to track the cost basis for digital assets?

Audit Impact. The availability of clean, accurate and sufficient data is key to validating transaction histories. Often, companies dealing in digital assets create internally developed custom software to fit their needs. The auditor should understand how these systems derive and compile data (e.g., from internally hosted platforms, or even hosted nodes) and examine the underlying logic. The availability of transaction and wallet identifiers (i.e., public addresses and transaction IDs) from the data downloads is also important when reconciling transaction histories. Basis and transaction tracking are also key for tax purposes. Auditors relying on reporting from homegrown software tools and databases will need to place increased emphasis on IT general controls, specifically change management and privileged logical access.

MANAGEMENT INSIGHT: Management should determine the most effective method for their company to track digital assets. Management may opt to develop in-house reporting tools. If so, management should document policies and standard operating procedures to govern logical access and change management, as well as preserve evidence of management's testing of the functionality and underlying report logic.

Management may also opt to use a third-party crypto accounting tool. Some of the ones we have seen in the field include Ledgible, Libra, SoftLedger, Balanc3 and Blox. Each tool has pros and cons that management should weigh against organisational objectives.

Ask the financial statement auditor to provide you a set of illustrative IT general controls that management can review against existing internal policies and procedures. While the chosen auditor cannot implement these controls for you, they should spend the time to share best practices and examples with you to facilitate management's success in implementing controls.

Conclusion

As shown by the considerations above, each audit that includes digital assets is unique, with its own set of dynamics and challenges. Management and potential auditors should engage in transparent discussions regarding the audit environment to ensure a distinct audit scope and delineated audit plan.

Audit Impact. The auditor should be prepared to encounter brand-new situations for which clear guidance from governing bodies is not always available. As always, the auditor should use his or her best professional judgment. Part of that judgment includes gaining a sufficient understanding of the underlying technologies involved in the audit before accepting or continuing an audit engagement. Experience transacting in digital assets, researching from authoritative sources in the space, and a general interest are the building blocks for developing expertise. Certifications such as the Certified Bitcoin Professional (CBP) designation, which indicate a certain level of subject matter competence, are also available to audit professionals.

MANAGEMENT INSIGHT: The inherently technical nature of digital assets raises the difficulty of engaging competent auditors. Knowledge and familiarity of the crypto space by the audit team can dramatically decrease the time and effort needed to perform procedures for both management and the external auditors. While more auditors are expanding their knowledge in this space, UTXOs, HD wallets and asymmetric cryptography are still not in the typical audit plan.
To ensure a smooth audit, management can use some of the pointers above. Generally, these include documenting policies and procedures for processes surrounding digital assets (and all processes, for that matter), keeping all wallet keys and exchange information for seven or more years, employing HD wallets where appropriate and ensuring robust reporting mechanisms.

References

i) For the purposes of this article, we use the terms “cryptocurrency,” “crypto,” “digital assets” and “crypto assets” interchangeably. In practice, digital assets encompass more than just cryptocurrencies. Examples would include non-fungible tokens (e.g., CryptoKitties, Decentraland plots) and potentially some tokenized assets.

ii) In our view, the “crypto winter” has been a pruning of sorts, separating the weaker projects within the space from those with more promising viability. The overall trend line of increased adoption and increased use will continue. As the underlying fundamentals (i.e., transactions per day, hash rate, wallet activity) rise, we expect a steady rise in the occurrences of crypto assets appearing on company (both crypto-native and non-crypto-native) balance sheets.

iii) HD wallets use a one-way hashing algorithm to produce a tree of keys from a single set of seed words. Therefore, use of the primary key can back up all associated addresses and can also be used to show proof of ownership for a large number of wallets in a single confirmation procedure.

iv) DApps typically have an associated fungible token (cryptocurrency) used to reward and incentivize users for using the decentralization application. A decentralized application (DApp) is a computer program or application run by multiple users on a decentralized network using a trustless cryptographic protocol.

v) Network security of underlying blockchains is outside the scope of this white paper but should always be considered. One of the key considerations is the hash rate of a given network. This is the power of the network to make guesses at the solution to the cryptographic problem (e.g., solving or mining a block in Bitcoin’s Proof of Work consensus algorithm). The hash power of the Bitcoin network at the time of this writing is approximately 60 Equihash, which is 60 × 1018 guesses per second. Therefore, a 51% attack (a powerful miner changing the ledger to suit their wants) would have to have 51% of that computing power.

vi) Shamir, Adi (1979). “How to share a secret.” Communications of the ACM 22 (11): 612–613.

vii) vii) Multi-signatures are a form of “Sharding” or “Shamir’s Secret Sharing,” which is a method in cryptography created by Adi Shamir. It is a form of secret sharing, where a secret is divided into parts, giving each participant its own unique part. To reconstruct the original secret (or cryptographic key), a minimum number of parts is required. Sharding keys can create a segregation-of-duties control in the same way a safety deposit box can be secured with two or more keys necessary to open it.