COMPLIANCE WEEK
FOR THE WELL-INFORMED CHIEF COMPLIANCE OFFICER AND AUDIT EXECUTIVE

Internal control best practices for blockchain technology



By Jaclyn Jaeger | Thu, Nov 14, 2019 11:19 AM

Those in the accounting profession who want to understand better the inherent risks, threats and vulnerabilities, *and* internal control best practices associated with the use of blockchain technology now have a first-of-its-kind framework to follow, thanks to the Accounting Blockchain Coalition.

The Accounting Blockchain Coalition, made up of a group of accounting and tax professionals, was **established** last year to educate the accounting profession on digital assets and distributed ledger technology, including blockchain, and its accounting and audit implications. Recently, the coalition's Internal Control Working Group released its **first framework**, providing guidance on how to mitigate the threats and vulnerabilities of digital assets and blockchain technology.

"The purpose of this document is to assist readers who are considering a risk assessment of certain common processes associated with the use of blockchain technology," Bennett Moore, co-chair of the Internal Control Working Group, said during a recent **Webinar**. It is not intended to be an authoritative risk framework. The framework was adapted using concepts and principles from the National Institute of Standards and Technology's (NIST) Special Publication 800-30.

At a high level, the type of inherent risks common to the various types of blockchain technologies are collusion, lack of authorization, hacks and malware, IT security practices, and a strong reliance on third-party platforms—whether associated with the use of cryptocurrencies, wallets, stablecoins, privacy coins, and more.

Below, we take a deeper dive into some of the various blockchain technologies highlighted in the framework, as well as a discussion about some of the inherent risks, threats and vulnerabilities, and internal control best practices for each.

"The purpose of this document is to assist readers who are considering a risk assessment of certain common processes associated with the use of blockchain technology."

Bennett Moore, Co-chair, Internal Control Working Group

Stablecoins

Stablecoins are cryptocurrencies designed to be pegged to an asset that has a stable value, such as the U.S. dollar (fiat stablecoins) or to the price of a precious metal, like gold or silver. Fiat stablecoins, for example, are generally stabilized by paying the value one-to-one, backed by assets held in a reserve. Put simply, for every stablecoin issued, one dollar is held in a reserve by a central custodian, such as a bank.

With stablecoins, however, volatility and liquidity are an inherent risk. "Most stablecoins are not actually stable at one dollar but fluctuate within a few cents above or below a single dollar," Moore explained. Thus, if using stablecoins to pay an invoice, for example, and you're paying that invoice over 20 days from an accounts/receivable perspective, one day it could be three cents above the dollar, meaning you'd be paying a three percent premium just for using that stablecoin, he said. The availability, potential time delays, and administrative burden associated with liquidation are additional areas of vulnerability created with the use of stablecoins.

One suggested internal control is to evaluate the market for stablecoins to see if there has been a price fluctuation. "You can look at the historical price fluctuations and the stablecoins that are out there," Moore said. You can see how often it fluctuates above and below a dollar based on trading. Another internal control is to evaluate terms of use to understand how stability is achieved.

The coalition also highlighted in its framework the high likelihood and high impact of non-compliance risks associated with the use of stablecoins—whether that be monitoring requirements from an anti-money laundering or know-your-customer perspective or a failure to have a disaster recovery plan in place in the event of a full liquidation.

With this form of cryptocurrency, it's advisable, first and foremost, to evaluate a stablecoin's compliance with regulations, including areas such as AML/KYC, disaster recovery. "Most stablecoins out there are being audited by different accounting firms on a

biweekly or monthly or quarterly basis," Moore said. "You can review those reports. They are publicly available."

Asset-backed tokens

Asset-backed tokens are a type of digital asset designed to represent physical product or goods. Here, auditability is an inherent risk. "Most of the physical assets that are represented in the virtual world by asset-backed tokens are high value," said Deniz Appelbaum, assistant professor of accounting and finance at Montclair State University.

Take diamonds as an example. From a risk-management standpoint, a company will want to track this physical asset to the blockchain to show the diamonds sold on the commercial market that are represented on the blockchain as real are, in fact, real—that they did not come from a blood mine or were manufactured artificially.

One vulnerability with the use of asset-backed tokens, however, is whether the information associated with it can be audited—for example, ensuring the diamonds have no connection to a blood mine or being able to verify third-party government agents in that mining country were not bribed in violation of the Foreign Corrupt Practices Act. "So, there are quite a few threats and vulnerabilities that present themselves trying to represent a physical asset in a virtual world," Appelbaum said.

What makes this information particularly difficult to prove or validate is the remote conditions of many of these high-value products—for example, an office in New York relying on blockchain from South Africa to verify these are not blood diamonds.

With these inherent risks in mind, recommended internal controls activities and procedures include the evaluation of compliance with regulations and laws and an audit report or attestation report from a third party concerning the existence and condition of the physical asset. It's also important to ensure the token has the required features available for an audit, such as a block explorer or wallet activity.

Utility tokens

Utility tokens are a type of digital asset designed to be exchanged or received for a product or service. They're typically used as a marketing tool to raise money and, generally, don't have value. Consider, for example, that some platforms are in the business of selling excess storage space on computers. In that case, a research university may be interested in buying that blockchain and using the utility token to purchase that excess storage space.



The inherent risk there is in the usability of them. Thus, from an internal controls perspective, it's incumbent upon the entity or person using the utility token to understand exactly what the utility token can be used for and when and how it can be used, said Graham Gal, associate professor of accounting at the Isenberg School of Management.

Other blockchain threats

Of all the threats and vulnerabilities and inherent risks associated with the use of blockchain technology, one common thread is people—whether it's an executive, manager, or trader. For example, with multi-signature (multi-sig) wallets—which require multiple keys to authorize a transaction—collusion is an inherent risk. The framework cites an example of management and IT personnel who each hold a private key to the multi-sig wallet working together to authorize and execute a transaction to their own personal wallet, effectively stealing the digital assets.

"While the likelihood of this happening may be low, the impact is high because sending value over a blockchain is irreversible," Moore said. Thus, one internal control activity would be to "segregate asset and execution duties between multiple IT managers, trade floor managers, and executives rotating every single withdrawal," he said.

Another internal control is to implement supervisory review by trade floor manager to ensure value, designation, frequency, and approval prior to execution. Beyond this, other internal controls include IT training related to phishing, as well as reviewing up-to-date publications by wallet software developers to ensure code is up to date and safe.

Cyber-hackers and malware are another people-related inherent risk with multi-sig wallets. “The hack points are occurring at the touchpoint of *individuals* in the blockchain, not the blockchain itself,” Moore said. Thus, when using a specific Website to transfer value, as is common practice, understand what to look for to ensure the site is secure. “That supervisory review aspect is going to be really important when you think about some of the threats and vulnerabilities associated with hacks and malware,” he said.

Specific examples of internal control activities and procedures around the use of multi-sig wallets may include implementing supervisory review by trade floor managers to ensure value, destination, frequency, and approval prior to execution; standard IT related to training; and reviewing up to-date publication by wallet and blockchain developers to ensure employee knowledge of identity hacks and malware. “It’s a matter of being educated, aware, and up-to-date of the fact that we are dealing with constant flooding of security attacks and phishing attacks and hacking attacks,” Appelbaum said.

Another people-related inherent risk associated with blockchain technology is lack of authorization. With multi-sig wallets, for example, it may be that the authorization of execution of a transaction was made in error. “Lack of authorization can cause serious problems,” Graham said.

To mitigate this vulnerability, the framework suggests segregating access and execution duties with rotation of roles every six months; implementing supervisory review and approval before execution, such as based on transaction amounts; and using two-factor authentication on all exchange accounts and e-mail accounts associated with exchange accounts, to cite just a few examples of internal controls.

The Accounting Blockchain Coalition said it plans to add more processes to its framework moving forward. But for the time being, the Coalition said, the framework can serve as an effective tool at board meetings with management to frame a discussion around the use blockchain of technology.

RATE THIS RESOURCE

Select your rating

