ALAN BRILL

Senior Managing Director
Cyber Risk
Secaucus, NJ, US
abrill@kroll.com

HUGO HOYLAND

Associate Manager
Business Intelligence and Investigations
London, UK
hugo.hoyland@kroll.com

KEN C. JOSEPH

Managing Director, Global Head
Disputes
New York, NY, US
ken.joseph@duffandphelps.com

JOSHUA MCDOUGALL

Director
Cyber Risk
Denver, CO, US
joshua.mcdougall@kroll.com

Proceed with Caution: Using Controls to Manage Risk in Digital Currency Transactions

A case study of cryptocurrency theft provides a primer on some of the risks that can accompany digital assets, as well as possible mitigations.

More and more organizations, from governments to the private sector, are capitalizing on the benefits and efficiencies of digital currency in their payments and settlements systems. Indeed, 28 percent of respondents to this year's *Global Fraud and Risk Report* survey confirmed that they already use cryptocurrency in some way. Facebook's announcement of the Libra initiative, involving several major financial services institutions, provides further evidence of the gathering momentum behind digital currency.

However, venturing into digital currency is not without peril for organizations. The threats include fraud, theft, money laundering, terrorist financing, tax evasion, manipulation and illiquidity—all encased in a wrapper of regulatory uncertainty. Enterprises need to respond with a coherent risk-based strategy that identifies the unique challenges faced by each organization and then mitigates and controls those risks across a range of environments, including legal, regulatory and operational compliance; risk management; information technology; data privacy and security; financial crime; and fraud. Putting compliance and controls at the center of technology adoption is crucial to managing the risk of new and complex ventures.

Proceed with Caution:

THE CASE OF THE MISSING MILLIONS

Recent investigations conducted by Kroll have highlighted some of the risks, threats and costs that an organization may face as a result of an ineffective system of compliance and controls in the use of digital currency. A number of cryptocurrency exchanges, for example, have contacted us after suffering losses from criminals who have exploited weaknesses in the exchanges' know your customer (KYC) and payment processes. In this work, we have found that traditional techniques can be quite effective when conducting investigations in the digital world of cryptocurrency. These techniques include constructing fictional digital personas to communicate with suspected thieves and mapping corporate structures, internet traffic and social media activity to reveal hidden relationships between actors. In one case, for example, Kroll was contacted by a cryptocurrency payment-processing company claiming it had to refund millions of dollars to several customers whose bitcoin accounts had been hacked. Kroll was able to uncover suspiciously close ties between the purported victims and the payment-processing company; the matter is now being investigated by law enforcement.

REGULATION AND TRANSPARENCY

Several observations can be gleaned from the matters we have investigated. First, tracking the transactions frequently proves to be a major obstacle. Cryptocurrency is often touted for its transparency; in theory, anyone with access to the underlying blockchain can trace the path of a cryptocurrency block from its origin to each transaction it has touched. The reality, however, is not so straightforward. Tracking crypto transactions can be time-consuming and inconclusive due to the anonymity of the parties in each transaction. Indeed, some cryptocurrencies seek to differentiate themselves from their competitors by promoting the strength of their anonymity. Hopefully, the draft guidance issued in June by the Financial Action Task Force (FATF), which recommends that virtual asset service providers adopt KYC safeguards and share customer information, will be a first step toward true transparency.

The new FATF guidance underscores the importance of cryptocurrency's global regulatory and enforcement framework, which at the moment is very much in flux. This situation is partly due to the usual lag that occurs when regulation has to catch up to technological innovation. So it is that countries with weak or no cryptocurrency regulations have the potential to become safe havens for perpetrators who wish to obscure their transactions and operate away from regulatory scrutiny.

But regulating crypto requires confronting an even deeper challenge. Cryptocurrency was developed precisely to facilitate transactions outside the frameworks established by government agencies and the financial services industry. In fact, crypto constitutes a direct challenge to the state's heretofore exclusive right to issue currency. The market's desire for crypto's benefits, however, is forcing the crypto industry and governments to create regulations for an entity that was designed to be unregulated. Not surprisingly, that task has been an arduous one.

Meanwhile, as that framework emerges, other risks loom beyond those related to fraud and theft. Unfortunate timing is one: Organizations that are early adopters may develop extensive procedures only to have to change them in the wake of evolving regulation (as, for example, the European Union's General Data Protection Regulation, California's Consumer Privacy Act and similar legislation from other jurisdictions are forcing organizations to do with respect to data privacy). The lack of adequate regulation can also delay broader public confidence in crypto, leading to adoption rates that fall short of what the organization anticipated when management decided to invest in a cryptocurrency system. Enterprises need to account for variables of this sort when devising their crypto strategies.

THE IMPORTANCE OF CONTROLS

Recent thefts at cryptocurrency exchanges highlight the need to maintain proper controls—not just at exchanges but at any organization using cryptocurrency. In one investigation, Kroll discovered that the exchange could not access information about how the payment service provider settled transactions and moved cash; further, the exchange released uncollateralized bitcoin to buyers before payment had been received—a practice very much at odds with standard procedures for exchanging tangible goods for fiat currency. This anomaly helps illustrate a key principle: Fundamentally, any transaction involving cryptocurrency should be handled as it would be if it involved fiat currency. For example, if a transaction in excess of $10,000 requires the approval of two corporate officers, the same controls should apply whether the transaction is in fiat or cryptocurrency—just as they should apply whether the transaction is in dollars or euros. The onboarding process for new customers should involve the same level of due diligence, whether those customers are paying in crypto or fiat currency. In fact, due diligence of a client's cryptocurrency transactions should be integrated into

the organization's existing KYC procedures to deliver a single panoramic view of customer risk.

Insufficient crypto controls often come about because organizations view cryptocurrency as an IT or cybersecurity issue and fail to include the perspective of compliance, internal audit and other key functions. Under these conditions, not only are controls inadequate, but important internal information regarding cryptocurrency transactions also goes uncollected, making it difficult to fully reconstruct fraud or theft involving crypto.

When imposing controls on crypto-based transactions, organizations will need to adapt the rules somewhat to account for the mechanics behind digital currency. In one recent case, the perpetrators used "bitcoin blenders" to scramble transactions and hobble the tracing of activity on the blockchain ledger. Other fraud techniques seek to take advantage of the time lag—usually between 10 minutes and one hour—that occurs before a transaction is authenticated on the cryptocurrency's underlying blockchain. This vulnerability can be mitigated, however, by altering the transaction process: Rather than releasing the acquired goods immediately, a company could impose a short waiting period to allow the transaction to be confirmed by the required number of users on the blockchain.

Sometimes the necessary changes to controls are not immediately apparent. Suppose, for example, that both the CEO and the CFO must approve certain transactions, whether executed in fiat or cryptocurrency. In a disaster scenario such as a plane crash involving those two officers, the board of directors and the general counsel could pass the appropriate resolutions and, with the company's financial institutions, implement the necessary transition so that the company could retain full access to its capital. With crypto, however, the company would have to anticipate the problem, perhaps by storing credentials in "virtual escrow" to allow continuing access in case of such an emergency.

A similar risk is that of cryptocurrency becoming inaccessible due to a ransomware attack that locks users out of the organization's computer network. Cryptocurrency has all the same vulnerabilities as other digital files, so an organization's crypto-assets are only as safe as the cybersecurity protecting them. Organizations thus should consider using offline ("cold") cryptocurrency wallets and incorporating crypto-specific security guidelines such as the CryptoCurrency Security Standard (CCSS) into their overall cybersecurity framework.

Insufficient crypto controls often come about because organizations view cryptocurrency as an IT or cybersecurity issue and fail to include the perspective of other key functions.

MAINTAINING A HEALTHY SKEPTICISM

Given the various risks associated with crypto, organizations are well advised to maintain a healthy skepticism when evaluating their level of adoption. This entails making sure crypto proponents are not the only ones involved in the discussion. In addition, at each decision point, risk analysis should involve not just IT and cybersecurity but also legal, treasury, corporate compliance and internal audit functions. As the organization's use of crypto deepens, enterprises need to ensure that key players, such as the chief information security officer, have adequate experience to accurately evaluate crypto's costs and benefits. When it comes to establishing sufficient cryptocurrency controls, corporations do not want to find themselves in the vulnerable position of learning as they go along.

When incidents do occur, it is important that they be approached with the same expertise in investigations that would be brought to a traditional fraud or theft. In the exchange case discussed at the beginning of this article, for example, the evidence that established the likelihood of collusion came about through the same process of gathering information and testing hypotheses that is used to solve analog crimes.

Cryptocurrency undoubtedly offers benefits in a world that places a premium on speed and efficiency. But it will be some time before regulators, law enforcement and industry have fully established foundational safeguards. In the interim, organizations that embrace crypto must take it upon themselves to ensure that digital currency's risks are thoroughly identified and mitigated.