Forensic bites series
June 2022

Safeguarding crypto holdings – considerations for private businesses

China markets briefing for risk, legal and compliance professionals

Since 2020, markets for digital assets such as cryptocurrencies and non-fungible tokens (NFTs) have seen remarkable development and growth. Recent months have seen these markets cool dramatically, but many businesses that chose to begin to hold digital assets continue to do so.

Like any other asset, digital assets can be vulnerable to wrongdoing unless appropriate steps are taken to keep them safe. Are there specific considerations for private businesses that have purchased crypto or that are considering doing so? Price volatility is probably the best understood risk around digital assets but safeguarding these assets from fraud and theft is just as important.

This article seeks to highlight steps that non-crypto specialist organisations should ask themselves as they consider whether their business and investments are well protected from fraud and economic crime.

pwc

Questions to ask

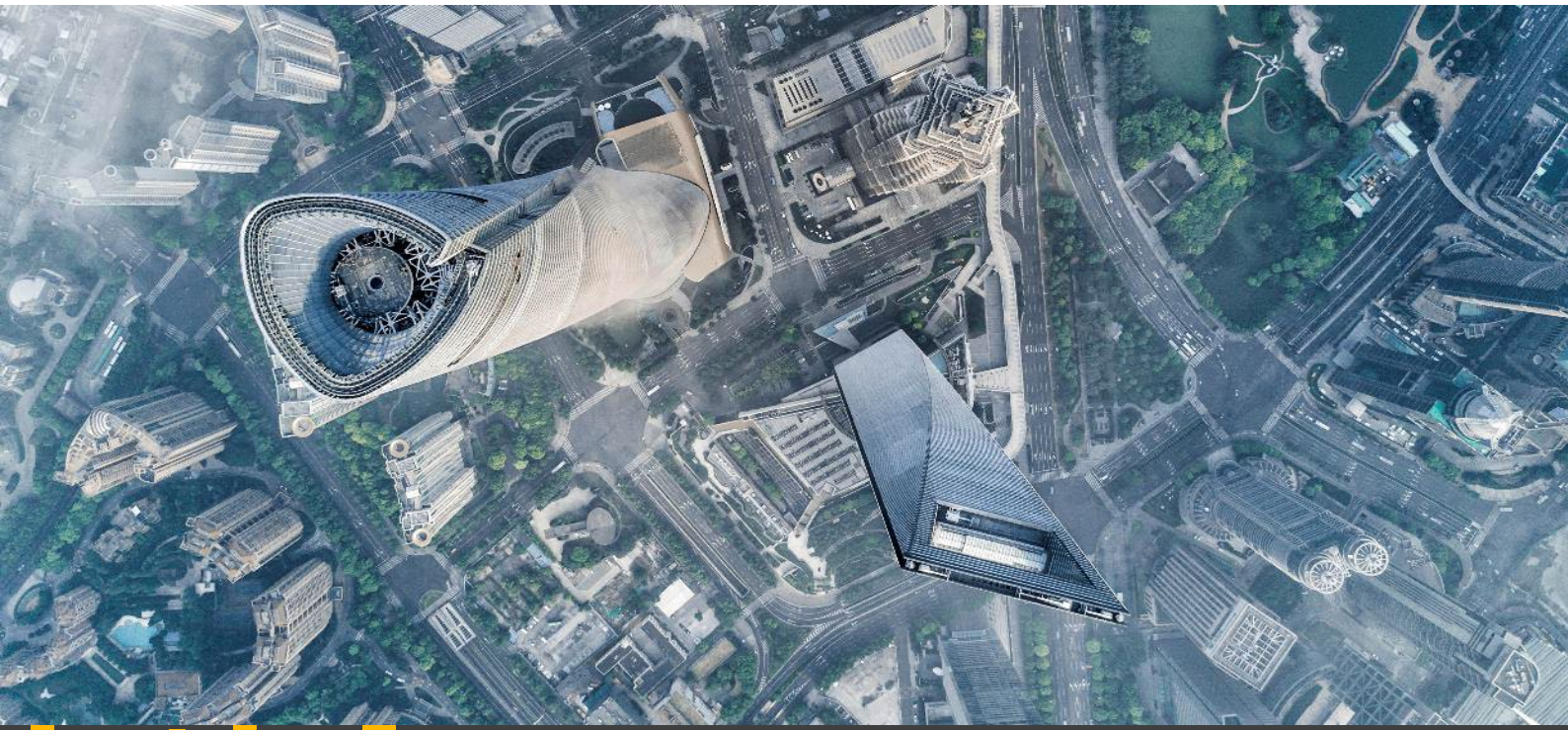
How well do we know our business partners and counterparties?

The digital assets world thrives on the race to be first to launch with a new innovation or the lore of large investments being made immediately after nothing but a brief pitch meeting. In the rush to do things fast and first, some digital asset firms bristle at the idea of conducting formal due diligence or counterparty background checks.

In bountiful times, such measures may seem to be nothing but trouble – making things slower, more expensive, more of a hassle. In lean times, the results of these exercises can make a big difference in safeguarding your funds.

Unlike traditional banks and investment brokers, most crypto exchanges are not backed by government deposit/investment protection programs, such as Hong Kong's Deposit Protection Scheme. Consequently, it is important to understand whether the party holding your crypto assets is reputable or whether there are red flags that you should be aware of. One recent example is the Hong Kong-based exchange Coinsuper, where users have indicated that they have been unable to withdraw funds since the end of last year. Some users have reportedly filed police reports; however, given that Coinsuper is not a regulated exchange, it is unclear whether users' funds can be retrieved.

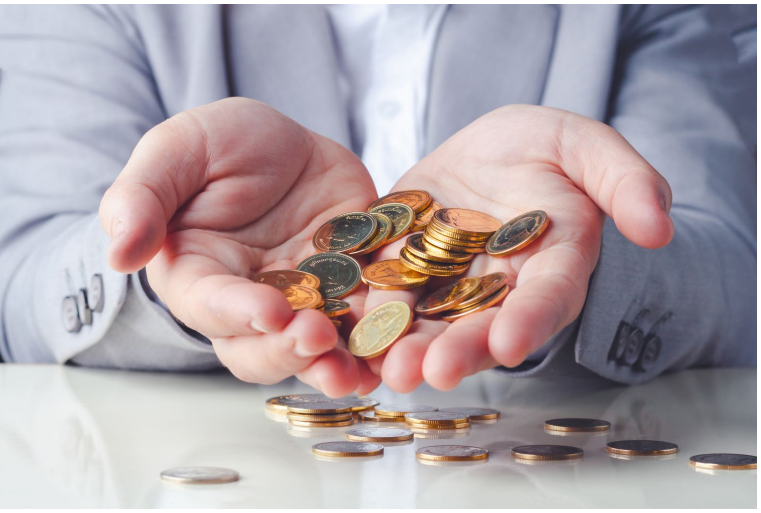
What are some things to look for? Diligence on the identities and integrity of business parties and counterparties can help to identify red flags among questionable actors, validate the bona fides of good ones and can help to identify other facts that can make for better informed decision making. Specific factors to consider are the regulatory status of the exchange (whether this is in Hong Kong or another reputable jurisdiction), its history of regulatory investigations, litigation history and association with negative news.



Do we have sound controls around treasury and digital asset holdings?

All companies have some degree of internal control protecting bank accounts and physical cash holdings. Although crypto assets are technologically advanced, maintaining robust controls around your holdings is always advisable. For example, if your company holds the assets in its own wallets, the use of multisig wallets (requiring multi-user authentication of transactions) is sensible for most organisations. As a control, this can be thought of as being analogous to having multiple signatories required for large-value cheque payments. A high-profile example of insufficient controls is the cryptocurrency exchange QuadrigaCX: up to USD 190 million in cryptocurrency owed to customers was missing or inaccessible after the death of the CEO and founder, who had sole control of the company's key wallets and was alleged to have misappropriated funds prior to his death.

Ensuring that appropriate access rights are given to move and control assets held with third parties such as exchanges or custodians is also advisable. This is similar to having controls around electronic funds transfers for bank accounts.



If a fraud or theft occurred, are we prepared to react?

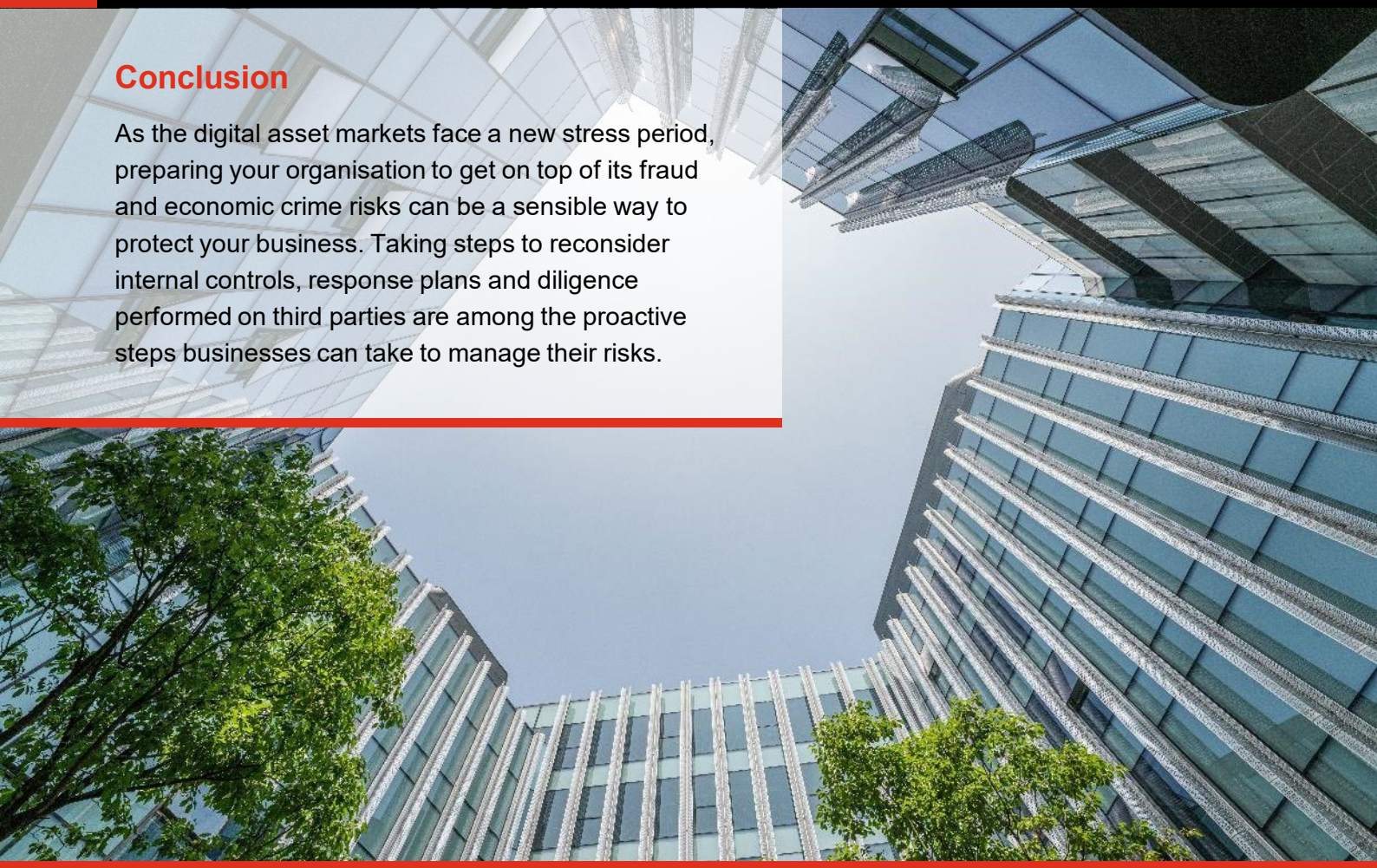
If something were to happen to your crypto assets, would you be able to respond in order to track down and, hopefully, recover the funds? Depending on how significant your digital asset holdings are, it may be appropriate to develop a pre-planned investigation response framework for the possibility of theft or fraud occurring. During the Polygon hack in August 2021, cryptocurrency valued at over USD 600 million was stolen. The Poly Network team published impacted addresses and publicly called on miners and exchanges to blacklist tokens coming from these addresses. By quickly doing so before the funds had moved through untraceable channels, the hacker was unable to move the funds and ultimately returned them.

Such a framework should clearly assign responsibilities internally and set out when to involve specialist investigations support and lawyers who will be able to advise on strategy and findings. This will help to ensure that the findings of the investigation form sound evidence that will support the companies' recovery efforts, whether through civil legal action, law enforcement or insurance.

A cost-benefit analysis may determine that a formal investigation plan is not proportionate to the size of your company's crypto asset holdings; however, would you know who to contact if an issue were to arise? Making sure to identify key contacts could help to protect you in the future from the consequences of unforeseen issues with theft or fraud.

Conclusion

As the digital asset markets face a new stress period, preparing your organisation to get on top of its fraud and economic crime risks can be a sensible way to protect your business. Taking steps to reconsider internal controls, response plans and diligence performed on third parties are among the proactive steps businesses can take to manage their risks.



Contact us

Brian McGinley

Partner, Forensic Services Leader
PwC Mainland China and Hong Kong
brian.mcginley@hk.pwc.com

Brent Sellors

Associate Director, Forensic Services
PwC Hong Kong
brent.sellors@hk.pwc.com

Bryoni Tse

Senior Manager, Forensic Services
PwC Hong Kong
bryoni.bt.tse@hk.pwc.com