CPA CHARTERED PROFESSIONAL ACCOUNTANTS CANADA

Transacting in Crypto-assets: Management Considerations and Controls for Small and Medium-sized Enterprises

DISCLAIMER

This publication was prepared by the Chartered Professional Accountants of Canada (CPA Canada) as non-authoritative guidance.

CPA Canada and the authors do not accept any responsibility or liability that might occur directly or indirectly as a consequence of the use, application or reliance on this material.

Table of Contents

Preface

Have you heard of Bitcoin? At its peak, one bitcoin was valued at approximately US$20,089.[1] Bitcoin is an example of a crypto-asset. Crypto-assets rely on blockchain technology to enable individuals and businesses to transact directly with each other without an intermediary such as a bank or other financial institution. If your business is thinking of using or accepting crypto-assets as a form of payment, this publication will provide an overview of crypto-assets used as a medium of exchange and highlight some important business considerations and controls for your business.

By the end of 2018, the previous hype around crypto-assets had declined significantly, but some businesses are still investing in and transacting with crypto-assets. However, many industry professionals supporting small and medium-sized enterprises may have little or no experience with crypto-assets and therefore may not fully appreciate the risks associated with crypto-asset transactions. With US$1.7 billion of crypto-assets stolen in 2018 alone,[2] it is paramount that businesses implement strong security practices to prevent theft of crypto-assets from their organizations.

Businesses also need to be aware that crypto-assets are not backed by government fiat and should be considered a highly speculative asset class. Unlike the tech companies that went bankrupt in the early 2000s with the collapse of the tech bubble, crypto-assets have no mechanism for delivering tangible value to their holders or purchasers. Consequently, businesses should be aware of this reality before engaging with crypto-assets.

This non-authoritative publication is intended to provide industry professionals in small and medium-sized enterprises with guidance on some of the top crypto-asset issues organizations that are transacting with crypto-assets are facing today:

- determining the business strategy as it relates to crypto-assets
- internal control considerations when engaging in crypto-asset activities
- navigating the regulatory environment for crypto-assets.

This publication is part of a broader set of CPA Canada resources related to crypto-assets. To learn about possible approaches to accounting for crypto-assets under IFRS®, refer to *An Introduction to Accounting for Cryptocurrencies*. For guidance under ASPE, refer to *An Introduction to Accounting for Cryptocurrencies under ASPE*. As to the implications

1 According to coinmarketcap.com, high price of US$20,089 for bitcoin was reached on December 17, 2017.

2 www.reuters.com/article/us-crypto-currency-crime/cryptocurrency-thefts-scams-hit-1-7-billion-in-2018-report-idUSKCN1PN1SQ

of crypto-assets for the financial statement audit, refer to ***Audit Considerations Related to Cryptocurrency Assets and Transactions***. To learn more about the underlying blockchain technology, refer to ***An Introduction to Blockchain Technology***.

About the Authors

CPA Canada would like to express its gratitude to Malik Datardina of Auvenir and Michael Wong of CPA Canada, who authored this publication.

CPA Canada would also like to express its gratitude to the members of CPA Canada's Technology Advisory Committee for their contributions to this publication.

Comments

Please contact us with any feedback or insights that could help in the development of future publications on this topic.

Michael Wong, CPA, CA
Principal
Research, Guidance and Support
CPA Canada
277 Wellington Street West
Toronto ON M5V 3H2
Email: michaelwong@cpacanada.ca

Davinder Valeri, CPA, CA
Director
Research, Guidance and Support
CPA Canada
277 Wellington Street West
Toronto ON M5V 3H2
Email: dvaleri@cpacanada.ca

State of Crypto-assets

Five hundred million stolen overnight. The crypto-asset exchange Coincheck was hacked in January 2018 for a loss of 500 million NEM coins[3] worth about $500 million.[4] One of the main security lapses identified was that the exchange kept the customers' assets in what is known as a **hot wallet** and did not implement **multi-signature security**. This event, along with a multitude of other hacks and security breaches, highlights the importance for businesses of having strong controls for managing crypto-assets and related transactions.

A **hot wallet** is connected to external networks while a **cold wallet** is not. A **multi-signature wallet** is one that implements multi-signature security and requires multiple sign-offs before a transaction is processed. Further details on the types of wallets and when they should be used is discussed in the "**Internal Control Considerations Related to Crypto-assets**" section below.

For the purposes of this publication, we use the term crypto-assets to mean only those crypto-assets used as a medium of exchange and intended to act as an alternative to government-issued fiat currencies. For example, Bitcoin would be considered such a crypto-asset while smart contracts that do not primarily function as a general-purpose medium of exchange would not.

The Crypto-bubble

The value and popularity of crypto-assets have grown exponentially in recent years. The market capitalization of crypto-assets increased from US$18 billion on December 31, 2016, to US$613 billion on December 31, 2017, an astonishing increase of 3,406%[5] that created news headlines such as "KFC Canada starts accepting Bitcoin for a bucket of chicken, immediately sells out"[6] and "Burger King Launches Crypto-asset 'Whoppercoin' in Russia"[7].

3 NEM coin is a crypto-asset supporting the NEM blockchain and was launched on March 31, 2015.

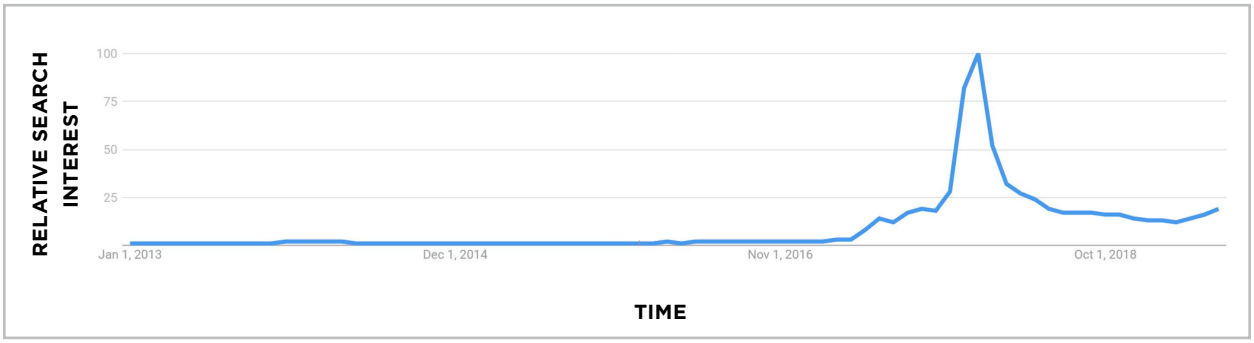
4 http://fortune.com/2018/01/31/coincheck-hack-how

5 https://coinmarketcap.com/charts

6 https://business.financialpost.com/news/retail-marketing/no-joke-kfc-canada-starts-accepting-bitcoin-for-a-bucket-of-chicken-immediately-sells-out

7 http://fortune.com/2017/08/25/burger-king-russia-cryptocurrency-whoppercoin

GOOGLE SEARCHES FOR "CRYPTO-ASSETS" SINCE 2013



Source: Google Trends
The popularity of "crypto-assets" surged in 2017 as evidenced by the spike in Google search interest during that period. The vertical axis represents search interest relative to the highest point on the chart since 2013. A value of 100 is the peak popularity for the term. A value of 50 means the term is half as popular.

The market capitalization of crypto-assets peaked at approximately US$829 billion in January 2018 and was followed by a drastic decline as the market capitalization of crypto-assets fell by approximately US$698 billion or 84% to US$131 billion by the end of December 2018.[8]

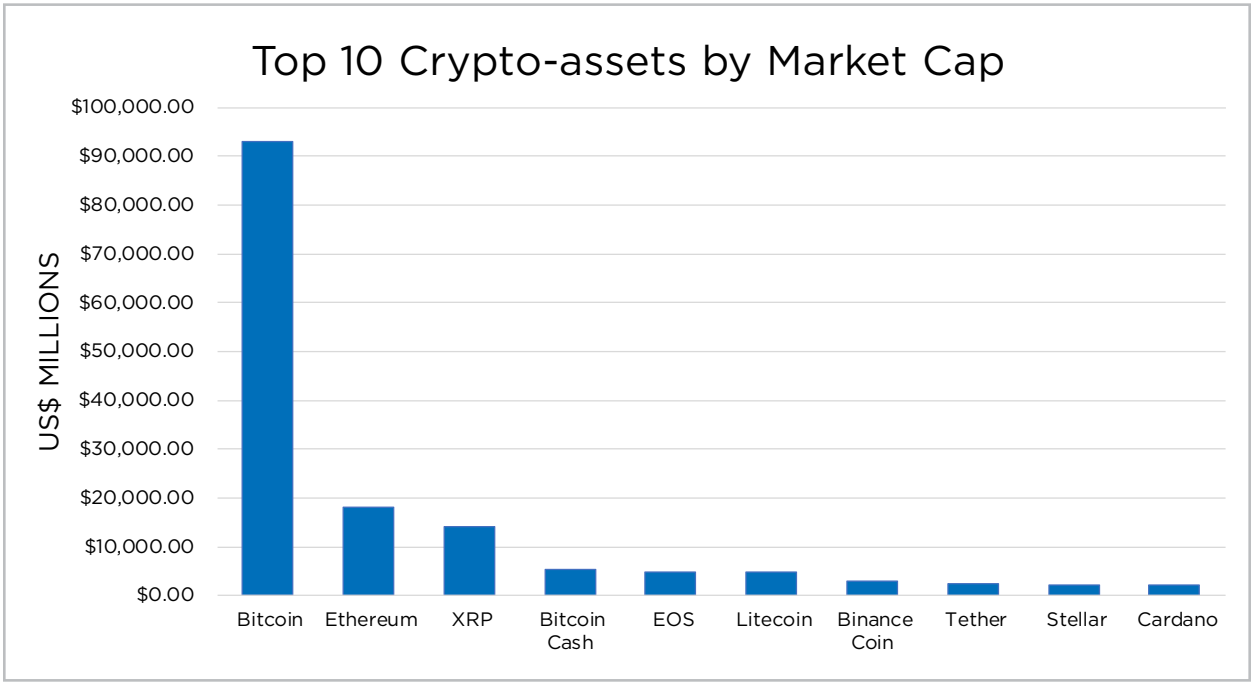
Are All Crypto-assets Equal?

There are currently over 2,100 different crypto-assets[9] and the number continues to grow as it is relatively easy to create a crypto-asset. Although at a high level, many crypto-assets share similar characteristics (e.g., decentralization and built-in security), they should not all be treated the same. Not surprisingly, a fitting analogy would be to compare a basket of crypto-assets to a basket of fiat currencies. Within the universe of crypto-assets, some like Bitcoin are widely used like the USD, and many others are treated like emerging market currencies and have lower popularity and higher risk.

8 https://coinmarketcap.com/charts

9 https://coinmarketcap.com/all/views/all as at January 16, 2019.

The most popular crypto-assets are Bitcoin and Ethereum. Bitcoin was designed as a digital payment system. Ethereum is similar but layers on smart contract capabilities and is sometimes used as a funding mechanism through a process known as an Initial Coin Offering (ICO). However, this publication focuses on crypto-assets that are used as a method of payment and store of value.



Source: coinmarketcap.com as at April 18, 2019

Evolution of Bitcoin as an Alternative Payment Method

Before the recent hype around crypto-assets and bitcoin, the ability to purchase goods with bitcoin was a novelty. Other than the few early adopters, not many individuals or companies would transact with Bitcoins. Back in 2010, one early adopter offered 10,000 Bitcoins, valued at approximately US$30 at the time, for someone to deliver him two pizzas.[10] Those 10,000 bitcoins were worth close to US$137 million at the end of 2017 — in hindsight, those were two very expensive pizzas!

Fast forward to 2018. Acceptance of Bitcoin as a method of payment has increased, particularly among online merchants and service providers. Some notable examples of organizations that accept Bitcoin include Shopify stores, Newegg, PayPal, Microsoft, and even the state of Ohio (for state taxes). In addition, the Ontario town of Innisfil has started a pilot for accepting bitcoins as payment for property taxes. While adoption by physical retailers has been slower, a service called eGifter even allows the shopper to purchase gift cards online with Bitcoins, which can then be used at popular retailers.

10 http://uk.businessinsider.com/Bitcoin-pizza-10000-100-million-2017-11

Crypto-assets in Hand: What Now?

Crypto-assets are not as widely accepted as cash or debit/credit cards, and they remain a niche market. Unless they are being held for speculative investment purposes, crypto-assets are typically converted to fiat currency. There is a number of ways for individuals and businesses to convert crypto-assets to fiat currency:

- Bitcoin ATM
- online crypto-asset exchange or over-the-counter markets
- barter exchange with another individual
- crypto-asset payment processor.

These methods of exchange all operate much like those for fiat currencies. For example, a Bitcoin ATM transaction begins with your Bitcoin wallet code (similar to the PIN for your debit card) followed by cash deposits/withdrawals directly to/from the ATM. An online crypto-asset exchange operates similarly to stock exchanges where willing market participants can buy and sell crypto-assets. As with cash, you can transact with another party directly by scanning each other's crypto-asset wallet code to facilitate an exchange of goods (i.e., the process is similar to scanning the barcode on your phone to make a payment at Starbucks). Lastly, a crypto-asset payment processor helps merchants accept payment from a customer and converts the crypto-asset into local fiat currency automatically. This is very similar to normal payment processors that facilitate the acceptance of debit/credit cards for businesses.

Business Considerations Related to Crypto-assets

The first question management should ask when deciding whether to use crypto-assets should be: what will be the primary purpose of crypto-assets for the business? Typically, the business purpose for crypto-assets will fall into two broad categories: **transactional** or **investment**. Transactional use includes facilitating and/or accepting payments in crypto-assets with minimal holding time. Investment use includes mining or storing crypto-assets, generally with a medium- to long-term holding period.[11] Business considerations will differ depending on the crypto-assets' primary use in the business.

Purpose	Business Considerations	Internal Control Considerations[12]
Transactional	• looking for a competitive advantage/differentiator • lower market risk compared to holding for speculative investment purposes • lower transaction processing fees compared to traditional payment processing • primary service provider: crypto-asset payment processor.	• Require a strong internal control environment but rely heavily on crypto-asset payment processors. • Obtain an understanding of the crypto-asset payment processor being used (more details here). • Request a service auditor's report, if available, and/or evidence of the appropriate design and operation of relevant controls from crypto-asset payment processors.
Investment	• looking for investment returns • may hold crypto-assets over a short- to long-term period with intention to earn gains on changes in value of crypto-assets • higher market risk but potential for higher investment returns when compared to traditional investment classes such as government bonds • primary service provider: crypto-asset exchange.	• Require a strong internal control environment to ensure safety of crypto-assets. • Obtain understanding of the crypto-asset exchange being used (more details here). • Request a service auditor's report, if available, and/or evidence of the appropriate design and operation of relevant controls from crypto-asset exchanges.

11 Other business purposes such as acting as custodians, exchanges, market-makers and trading platforms are out of scope for this publication.

12 Service auditor reports for crypto-asset payment processors and exchanges are not widely available at the time of publishing.

For Transactional Purposes

If a credible crypto-asset payment processor is used, businesses transacting in crypto-assets for the purposes of facilitating and/or accepting payments can expect to face risk and benefits similar to those associated with accepting credit cards. Refer to the **Internal Controls and Security** section below for what to take into consideration when assessing crypto-asset payment processors and exchanges. Many crypto-asset payment processors provide the ability to automatically convert the crypto-asset payment into fiat currency immediately, thus reducing the market risk of holding the crypto-assets. As the value of crypto-assets can be extremely volatile, immediate conversion to fiat currency is one approach to mitigating this risk.

Another consideration for crypto-assets is the speed at which transactions are confirmed on their respective blockchains. Transaction confirmation times of crypto-assets typically lag that of traditional payment processors like VISA and MasterCard. This is largely due to the way crypto-asset transactions need to be verified through a decentralized network. For example, Bitcoin typically requires six confirmation blocks before a transaction is considered complete, which could take up to an hour. This may be acceptable for online transactions but unlikely to be feasible for physical retailers. However, crypto-asset payment processors are leveraging innovative platforms such as GAP600 to help facilitate near instantaneous confirmation of Bitcoin transactions.[13]

From a cost perspective, crypto-asset payment processors generally charge lower fees than credit and debit card processors. According to a study by the Canadian Federation of Independent Business (CFIB), VISA and MasterCard merchant fees in Canada can range from 1.65% to 2.75%.[14] Merchant fees for Bitcoin processing on the other hand are typically lower. For example, fees for basic transactions at BitPay and Coingate are 1%.[15] The savings from lower transaction fees can be passed on to customers to gain a competitive advantage.

While the use of a crypto-asset payment processor will facilitate transaction processing and mitigate certain risks related to crypto-assets, it is not risk-free. Because most crypto-asset payment processors are less established than traditional payment processors, they carry a heightened credit and liquidity risk. Therefore, it is important to perform proper due diligence in selecting a credible and reputable crypto-asset payment processor.

13 GAP600 is a platform that uses data analytics to calculate the risk of double spending bitcoins. As a result, they can provide near instantaneous bitcoin transaction confirmations for payment processors.

14 www.cfib-fcei.ca/sites/default/files/pdf/5513.pdf

15 BitPay: https://bitpay.com/pricing
Coingate: https://coingate.com/accept-Bitcoin

For Investment Purposes

Businesses also use crypto-assets for "investment purposes," with the goal of generating investment returns. In contrast to businesses engaged in crypto-assets for transactional purposes, businesses that focus on investment will generally hold crypto-assets over a longer period thus subjecting themselves to significantly higher market risk. Holding crypto-assets can also lead to higher risk of both internal and external theft. Therefore, these businesses will need stronger internal controls and security to ensure the safety of their crypto-wallets and private keys. More information can be found in the Internal Controls and Security section below.

The main costs related to trading and holding crypto-assets are transaction fees charged by crypto-asset exchanges both for conversion to/from fiat currency and for each purchase and sale transaction of crypto-assets on the exchange. The costs involved would be similar to brokerage costs incurred when transacting on the equity markets. Selecting a credible and reputable crypto-asset exchange is difficult, but it is important to reduce risk and ensure the best pricing. Aside from cost, other important considerations when selecting an exchange are the liquidity of the exchange as well as its security.

Regardless of whether your business uses crypto-assets for transactions or investment, it is highly advisable first to:

- understand the risks and benefits associated with crypto-assets
- set up a strong internal control environment to ensure security of crypto-wallets and private keys as well as the integrity of underlying transactions
- consult with subject matter experts on the appropriate accounting and tax treatments
- discuss the implications for the audit engagement with your auditors.

Internal Control Considerations Related to Crypto-assets

Internal Controls and Security

When looking at risks associated with crypto-assets, security must be top of mind — and for good reason. Unlike funds in a bank account where ownership is tied to the person whose name is on the account, ownership of crypto-assets is tied to a set of public and private keys represented only by an alphanumeric string of characters. Anyone with access to the public key and the corresponding private key can access crypto-assets. Typically, a crypto-asset wallet is used to store the public address for a specific crypto-asset and is used to send and receive the crypto-asset. Furthermore, when it comes to crypto-assets such as bitcoin and ether, they can easily be converted to cash because of the liquidity available in their respective markets, which makes them highly susceptible to theft. Can a bitcoin thief be tracked through the open ledger? Yes, it is possible since bitcoin transactions are only pseudonymous and not anonymous. Services like Chainanalysis can help businesses and law enforcement investigate fraud and other criminal violations. However, the process remains a game of cat and mouse. Careful criminals can leverage the pseudonymity to launder the money through the use of mixers/tumblers "that crisscross [stolen] bitcoins with other users' bitcoins so that [the thieves] get a clean address that the blockchain cannot connect with any of the addresses from which the coins were stolen."[16] With the lack of registered ownership, pseudonymity, and ease of conversion to cash for some crypto-assets, they are comparable to bearer bonds where anyone with access to the private key essentially has full control and use of the crypto-assets.

It is therefore not surprising numerous hacks have stolen and defrauded crypto-assets from businesses. Appendix I summarizes several hacks that have occurred recently. By analyzing the recent hacks to understand what went wrong, it became apparent that some of them were related to IT security issues that were not specific only to crypto-assets.

- **Inadequate understanding of the technology**
  The Mybitcoins hack occurred because of a "misunderstanding of how Bitcoin secures transactions into the next block." Such an issue exists with any nascent technology and is a good illustration of how using technology can put you on the "bleeding edge" instead of the "leading edge." Therefore, it is important to understand the underlying blockchain protocol used for the crypto-asset since not all crypto-assets are designed equally.

16 www.theverge.com/2013/12/19/5183356/how-to-steal-bitcoin-in-three-easy-steps

- **Incorrect risk analysis**
  Implementing controls requires an understanding of the underlying risk equation. In both the Linode hack and Bitfloor hack, the hackers compromised systems that were thought to be lower risk. For example, the Bitfloor hack occurred because of the misbelief that a non-public-facing computer carried a lower risk and did not require extensive security controls.
- **Improper configuration of controls**
  Security controls such as multi-factor authentication (MFA) requirements are effective when properly set up. MFA is a security practice requiring a user to present at least two credentials when logging into an account (e.g., password and fingerprint). However, in the case of the Inputs.io hack, hackers were able to exploit old email accounts that did not have a proper secondary authentication (e.g., phone numbers) attached to them to properly enable MFA.

Before delving into the controls around Bitcoin, it is important to remember that crypto-assets are in their infancy. The definitive set of best practices on how to secure such assets is yet to be developed. However, experts such as Andreas Antonopoulos and others offer several considerations when it comes to securing crypto-assets:[17]

- **Understand the crypto-asset payment processor and/or exchange being used**
  Not all crypto-asset exchanges are created equal. Some may keep crypto-assets for each user in a common wallet rather than individualized hot wallets. Some may attempt to save transaction fees by creating a system that keeps track of transactions *instead* of relying on the actual blockchain. These types of transaction are typically referred to as "off-chain transactions." Consequently, the information held on a system that tracks only off-chain transactions does not benefit from the consensus mechanism or other security protocols of the blockchain. It is important to perform adequate research prior to selecting an appropriate exchange.
- **Choose an appropriate wallet type**
  Because hot wallets are connected to the Internet, hackers are able to compromise the wallet provider more easily and to access the stored crypto-assets. Therefore, it is not recommended to keep all your crypto-assets in a hot wallet. Cold wallets are generally a better option for long-term storage. Although they may be less convenient than hot wallets, cold wallets are generally more secure because they are not connected to external networks. There are generally two types of cold wallets — paper wallets and hardware wallets:
  — *Paper wallets*

17 Andreas M. Antonopoulos. 2017. *Mastering Bitcoin: Programming the Open Blockchain* (2nd ed.). O'Reilly Media, Inc.

It is a bit ironic, but a safe way to protect your digital currency may be to print out the private key and store it in a safe and secure place. However, this method is subject to the risk of destruction and deterioration over time.

— *Hardware wallets*
Unlike cellphones or computers, hardware wallets are devices dedicated solely to storing the private keys securely on the device for accessing crypto-assets. Examples of hardware wallets on the consumer market include Trezor One, Ledger Nano S, and KeepKey. Major advantages of hardware wallets over software wallets are that private keys:

- are stored securely in protected microcontrollers and cannot be transferred off the device in plain text
- do not interact with potentially vulnerable software and are less susceptible to malware such as trojans.

- **Maintain control of the private key**
Crypto-asset transactions rely on private and public keys. The public "address" of your wallet is created from a hash of your public key and allows others to transact with you. The public key is derived from the private key. The private key is essentially the "key" to your home at your public "address". If you lose control of your private key, you lose control of your crypto-assets. Therefore, private keys need to be kept secure throughout the ownership of the crypto-asset wallet, starting from key generation. It is not recommended to share the private key with others.

- **Maintain physical security of private key**
Cold wallets are only more secure than hot wallets if there are adequate controls around the physical security of the private keys. Therefore, despite the digital nature of crypto-assets, physical security is equally important. Physical security over private keys should be as sophisticated and strong as one would have for other high value assets. Examples of potential storage places could include safety deposit boxes or vaults where access is controlled.

- **Ensuring proper management of private-key backups**
Antonopoulos notes in his book that "a well-known bitcoin awareness and education project lost almost 7,000 bitcoin. In their effort to prevent theft, the owners had implemented a complex series of encrypted backups. In the end they accidentally lost the encryption keys, making the backups worthless and losing a fortune." Similar to other IT systems, appropriate backup processes (including ensuring access to backups) should be in place to protect your private keys.

- **Diversify storage approach**
  Keeping all crypto-assets in a single wallet is a high risk since all the crypto-assets will be lost if that wallet is compromised. Consider using a combination of multiple wallet types and providers to reduce the impact of an individual compromised wallet.
- **Consider multi-signature (multi-sig) wallets**
  The concept of multi-sig wallets is not new. One of the best practices in managing encryption keys is "split knowledge" (i.e., no one person has the full key). Multi-sig wallets "secure funds by requiring more than one signature to make a payment. The signing keys should be stored in several different locations and under the control of different people. In a corporate environment, for example, the keys should be generated independently and held by several company executives, to ensure no single person can compromise the funds." (Antonopoulos, 2017). Private key ceremonies are one way of generating new keys. Refer to the example below from Coinbase's private key ceremonies for more details.

Private Key Ceremonies – A Coinbase Example[18]

Coinbase is a crypto-asset exchange regarded as one of the more popular consumer-facing exchanges in the U.S. The company processes transactions and stores crypto-assets globally. So how does a company like Coinbase generate its private keys?

The first step of the process is to setup a Faraday tent. A Faraday tent is designed to block electromagnetic signals from escaping or being intercepted by hackers. Inside the Faraday tent is where the private key ceremony happens. Inside the tent, a Linux-based laptop is chosen randomly through a coin toss and then used to generate the private key. The printed private keys are then safely stored in a secure vault. After the ceremony is complete, the laptop used to generate the key is destroyed to prevent data leaks.

While some of the steps taken by Coinbase may seem extreme, they do highlight the importance of protecting private keys from inception. Businesses should consult with subject matter experts when designing their private key ceremonies.

Auditor Expectations

While the above control considerations are helpful in improving the security of crypto-assets for business operations, auditors may require additional audit evidence (including control design and implementation) to address specific risks unique to crypto-assets. Auditors may also need to perform independent evaluations to understand the relevance and reliability of the information received from the underlying blockchain technology.

18 www.wired.com/story/coinbase-physical-vault-to-secure-a-virtual-currency

When it comes to the security of access to private keys, auditors may ask to attend private key ceremonies to get evidence of a strong control environment, to make sure the keys are generated in a cryptographically secure manner, and that no unauthorized copies have been made. For crypto-assets held at an exchange or payment processor, auditors may request a service auditor's report from the exchange or payment processor and, if one is not available or if the scope of the service auditor's report is not appropriate for the auditor's purposes, the auditor may consider directly testing internal controls at the exchange or payment processor.

Another area where additional scrutiny may be necessary is around related-party transactions. Due to the pseudonymous nature of crypto-assets, it can be difficult to associate crypto-asset wallets (consisting of strings of characters and numbers) with real-world entities. To overcome this problem, establish an effective control environment within the organization. Create policies and procedures for getting sufficient knowledge about the parties with whom your business will be entering into crypto-asset transactions. Assign responsibilities within your organization for identifying, recording and disclosing related-party transactions.

For more information on the implications of crypto-assets for the audit, refer to CPA Canada's ***Audit Considerations Related to Cryptocurrency Assets and Transactions*** publication.

Crypto-assets are still considered new territory for many businesses. Therefore, it is necessary to be extra careful working with this type of asset. When in doubt, seek guidance from subject matter experts and advisors to determine the controls required to secure your crypto-assets.

Regulatory Environment

Regulators and supervisors around the world are showing great interest in crypto-assets. In the U.S., the Financial Stability Board (FSB) in collaboration with the Committee on Payments and Market Infrastructures (CPMI) has developed a framework to monitor the financial stability of crypto-asset markets. The FSB noted in a recent report that although "crypto-assets do not pose a material risk to global financial stability at this time, it [the FSB] recognises the need for vigilant monitoring in light of the speed of market developments."[19] While there are no global rules for crypto-assets yet, governments around the world have taken differing approaches to monitor and regulate them at the national level. These regulations also continue to evolve and change along with the development of crypto-assets. Therefore, businesses looking to expand into the crypto-asset space should carefully assess the regulatory environments of the jurisdictions in which the business plans to operate.

While there are legitimate business uses for crypto-assets, crypto-assets have also been used by criminals to engage in illicit activity as well as orchestrate ransomware. Unfortunately, it is often after a ransomware attack that companies (and their IT consultants) are forced to learn about crypto-assets because the company has had to pay the hacker in bitcoin or other crypto-assets to regain access to their system and data. Crypto-assets also represent a way to disrupt the conventional order. Satoshi Nakamoto (whose identity is not truly known[20]) released bitcoin in the aftermath of the 2008 financial crisis in which the centralized trust model had taken a reputational hit because of excessive risk-taking by financial institutions. Furthermore, bitcoin was not the first attempt for cyber-activists to create a digital currency that would grant individuals independence from both the state and corporations. These factors are often the reasons governments around the world attempt to regulate crypto-assets.

19 www.fsb.org/wp-content/uploads/P160718-1.pdf

20 Satoshi Nakamoto is the named used by the unknown individual or group who developed bitcoin and authored the bitcoin white paper.

In Canada

Crypto-assets are not considered legal tender in Canada and are characterized as a commodity under Canadian law. However, payments in crypto-assets are still subject to taxation under the *Income Tax Act*.[21] For details on accounting under IFRS and tax implications related to crypto-assets in Canada, refer to CPA Canada's ***An Introduction to Accounting for Cryptocurrencies*** publication.

While the Canadian federal government is still finalizing regulation of crypto-assets at the time of writing (June 2019), this has not stopped federal agencies and regulators from acting (see to **Appendix III** for a list of select guidance issued by regulatory bodies in Canada and the U.S.). For example, it has been reported that the Canada Revenue Agency (CRA) is looking closely at auditing crypto-asset holders and has sent them "comprehensive questionnaires to fill out regarding their bitcoin-related activity over the past years."[22] In addition, agencies like the Canadian Securities Administrators (CSA) have issued staff notices on crypto-asset offerings that could be considered a distribution of securities.[23] Therefore, businesses must stay abreast of regulatory developments in order to ensure compliance with Canadian laws and regulations.

Internationally

Nations around the world differ in their approach to crypto-assets. There are nations like Venezuela that have embraced crypto-assets and created their own digital currency; other nations such as China have reined in the use of crypto-assets by its citizens.

"Beijing's crackdown on bitcoin is part of a broader effort to root out risks to the country's financial system. Officials earlier this year [2017] circulated a draft of anti-money-laundering rules for bitcoin exchanges, a powerful warning, even though the regulations were never formalized, according to people familiar with the matter.... Virtual currencies in theory allow holders to bypass China's traditional banking system to move money outside its capital-controlled borders. That could make it more difficult for Chinese regulators to maintain a tight grip on the yuan."[24]

While enacted regulations around the use of crypto-assets are minimal in the U.S., certain U.S. government agencies, such as the Federal Deposit Insurance Corporation (FDIC) and the U.S. Department of Justice (DOJ), have taken key regulatory action against organizations that use bitcoin. For example, the FDIC reportedly pressured bank compliance officers

21 www.loc.gov/law/help/cryptocurrency/canada.php

22 www.forbes.com/sites/ktorpey/2019/03/06/bitcoin-investors-targeted-with-audits-by-canadas-federal-tax-agency/#133439e1656e

23 http://research.osc.gov.on.ca/ld.php?content_id=34149486

24 www.wsj.com/articles/china-to-shut-bitcoin-exchanges-sources-1505100862

to not work with organizations that use bitcoin. The DOJ launched an initiative in 2013 known as Operation Choke Point to investigate banks dealing with businesses that were not necessarily illegal but were considered a high risk for fraud and money laundering. The businesses under investigation included legal providers of bitcoin services. The operation achieved the intended result of cutting off banking and financial services for those businesses under investigation because the risk of an audit from the DOJ was enough to dissuade financial institutions from working with those businesses.[25]

In the European Union, the financial authorities have highlighted the risks associated with crypto-assets but have not yet advanced significant regulations. In January 2019, the European Banking Authority (EBA) issued a report advising the European Commission to perform a thorough assessment of whether regulatory action is needed to achieve a common EU approach to crypto-assets.

While crypto-assets are generally designed to be borderless and globally accessible, current regulatory actions and regulation under development may reduce that accessibility. However, development of crypto-assets continues to rage ahead while regulatory frameworks try to catch up. Therefore, regulatory uncertainty is a real risk. It is important then to understand how a regulator views crypto-asset activity to better assess and anticipate the regulatory risks in a specific jurisdiction.

Regulatory clarity for crypto-assets will arrive eventually. Despite the early hype, crypto-assets are still in their infancy. Similar to anti-money laundering and know-your-customer requirements, which are now the norm in financial institutions, controls and standard procedures for crypto-assets will be developed in due course. Until then, the nascent crypto-assets will lack regulatory clarity in most jurisdictions. This, combined with the differing regulatory views around the world, makes it difficult for businesses to properly leverage crypto-assets in their operations. For now, crypto-assets will remain a niche tool for enthusiasts.

25 Vigna, Paul. *The Age of Cryptocurrency: How Bitcoin and Digital Money Are Challenging the Global Economic Order* (p. 258-259). St. Martin's Press. Kindle Edition.

Appendix I: Analysis of Crypto-asset Hacks

Hack	Date	Size of Loss	Incident Summary	What Went Wrong
allinvain	June 2011	25,000 bitcoins worth US$500,000	This attack was one of the first reported incidents of bitcoin being stolen.[26]	Malware that compromised wallet security enabled the hacker to transfer coins to another wallet.
Mybitcoins[27]	August 2011	154,406 bitcoins worth US$2 million	Mybitcoins was a wallet service that maintained wallets for their users. They kept half their bitcoins in cold storage. According to a message Mybitcoins posted to their users, they were intending to refund what they had to the users. However, it was unclear as to how they would send the bitcoins back, given their systems were compromised.	Improper interface controls between the system and the blockchain ledger were exploited by a hacker. The site noted that "it appears to be human error combined with a misunderstanding of how Bitcoin secures transactions into the next block."
Linode	March 2012	46,703 bitcoins worth US$228,845	More than 43,000 of the stolen bitcoins belonged to a bitcoin trading platform known as Bitcoinica. Another 3,094 bitcoins were lifted from the virtual purse of Marek Palatinus, a freelance programmer from the Czech Republic. He said in an interview that a separate bitcoin user he had been in contact with lost 50 bitcoins to the same attackers. And Gavin Andresen, the lead bitcoin programmer, lost all five bitcoins he had stored in one online account.[28]	A hacker targeted Bitcoin wallets stored on Linode's servers after compromising a customer service portal.

26 www.forbes.com/sites/timworstall/2011/06/17/bitcoin-the-first-500000-theft/#74c5604d29b3

27 https://observer.com/2011/08/mybitcoin-spokesman-finally-comes-forward-what-did-you-think-we-did-after-the-hack-we-got-shitfaced

28 https://arstechnica.com/information-technology/2012/03/bitcoins-worth-228000-stolen-from-customers-of-hacked-webhost

Hack	Date	Size of Loss	Incident Summary	What Went Wrong
Bitfloor	September 2012	24,000 bitcoins worth around US$250,000	Servers were compromised allowing the attacker to gain access and transfer the coins. The vast majority of the coins on the exchange were taken during this attack.[29]	Backup of the wallet was accessed because Bitfloor assumed there was a low risk of being compromised since the machine used for the backup was not public facing.
Inputs.io[30]	October 2013	4,100 bitcoins, worth over US$1 million	Inputs.io, which was run by a developer known as TradeFortress in the bitcoin community, was hacked. The company also operated a bitcoin bank, CoinLenders as well as a chatroom Coin-Chat. The developer was intending to repay users from the bitcoins stored in cold storage as well as "from his own personal account."	The attacker circumvented the multi-factor authentication by using compromised email accounts that were "easy to reset" due to the lack of phone numbers attached to those accounts. This was "due to a flaw on the server host side."
BIPS [31]	November 2013	1,295 bitcoins worth US$650,000	Europe's largest payment processor and online wallet holder lost 1,295 bitcoins. According to the Copenhagen-based company, the funds stolen belonged to the company.[32]	The company was targeted by two successive attacks, which the company believed were related. The first was a large Distributed Denial of Service attack and the second attack "disabled the site and overloaded our managed switches and disconnected the iSCSI connection to the SAN on BIPS servers."

29 www.nbcnews.com/technology/250-000-worth-Bitcoins-stolen-net-heist-980871

30 www.theguardian.com/technology/2013/nov/08/hackers-steal-1m-from-Bitcoin-tradefortress-site

31 www.theguardian.com/technology/2014/mar/18/history-of-Bitcoin-hacks-alternative-currency

32 www.coindesk.com/Bitcoin-payment-processor-bips-attacked-1m-stolen

Hack	Date	Size of Loss	Incident Summary	What Went Wrong
Pico-Stocks[33]	June and November 2013	1,300 bitcoins in June and 5,896 bitcoins in November	According to Wired magazine, PicoStocks was an "unregulated stock market denominated in Bitcoins, and supposedly incorporated in the Marshall Islands. PicoStocks attempted to circumvent federal securities regulations by operating as if PicoStocks itself owned the assets and traders merely purchased dividend streams."	Wired also noted that the June 2013 hack was a result of improper security. "PicoStocks used duplicate passwords for multiple accounts – a practice the founder himself described as 'just extremely stupid' and 'clearly our fault.'" Wired noted the second hack in November included "both its 'hot' and 'cold' wallets. Because cold wallets can't be accessed in online attacks, the theft may have been an inside job."
Mt. Gox[34]	February 2014	850,000 bitcoins worth US$450 million	A Russian named Alexander Vinnik was the owner and operator of a competing bitcoin exchange called Bitcoins-e. The U.S. Federal Bureau of Investigation alleged he knowingly accepted stolen Bitcoins from Mt. Gox and laundered them through his own bitcoin exchange.	In June 2011, it is believed that an auditor's laptop was compromised that allowed hackers to "artificially alter the nominal value of bitcoin to one cent and then transfer an estimated 2,000 bitcoins from customer accounts on the exchange, which were then sold." The second hack is believed to have started prior to September 2011, when "the Mt. Gox private key was unencrypted and it would appear that it was stolen via a copied wallet.dat file, either by hacking or perhaps through an insider."

33 www.theguardian.com/technology/2014/mar/18/history-of-bitcoin-hacks-alternative-currency

34 https://blockonomi.com/mt-gox-hack

Hack	Date	Size of Loss	Incident Summary	What Went Wrong
Bitstamp	January 2015	19,000 bitcoins worth US$5.2 million	UK-based Bitstamp, the second largest bitcoin exchange for US dollars, suspended operations following evidence that online thieves had stolen up to 19,000 bitcoins – approximately $5.2 million – from its operational store of bitcoins. The company alerted its users of the possible attack and warned against transferring any bitcoins to the service's old bitcoin deposit addresses. Bitstamp later revealed the attack affected fewer than 19,000 bitcoins. The actual attack appeared to have compromised the company's operational funds, also known as the "hot wallet." "To restate: the bulk of our bitcoin are in cold storage, and remains completely safe."[35]	Bitstamp's operational funds were stored in a hot wallet, which was compromised by hackers. The primary issue was the number of bitcoins stored in the hot wallet as hot wallets should not be used to store large amounts of bitcoins. The bitcoins stored in cold wallets were not compromised.
Bitfinex	August 2016	120,000 bitcoins worth US$77 million	According to comments by Zane Tackett, Director of Community & Product Development at Bitfinex, on Reddit, a total of 119,756 bitcoins were stolen. At an average value of $650 per bitcoin, that amounts to more than $77 million.[36]	The challenge of the Bitfinex hack is that the exchange used BitGo a multi-sig approach to security (i.e., more than one signature is required to execute the transaction). According to an article that references an infographic from Bloomberg, it speculates the automation required to get the second signature was exploited. However, nothing is confirmed with respect to what actually happened.

35 https://arstechnica.com/information-technology/2015/01/Bitcoin-exchange-bitstamp-claims-hack-siphoned-up-to-5-2-million

36 https://arstechnica.com/information-technology/2016/08/Bitcoin-value-falls-off-cliff-after-58m-in-btc-stolen-in-hong-kong-exchange-hack

Hack	Date	Size of Loss	Incident Summary	What Went Wrong
Quad-rigaCX	February 2019	Crypto-assets worth ~$180 million	According to the BBC, the crypto-assets are believed to have been lost due to the death of the company's CEO, who was the only one with access to the crypto-assets kept in cold storage.[37]	The crypto-assets were lost due to the lack of adequate succession planning (i.e., there was no secondary person(s) who could access the crypto-assets in the extended absence of the primary founder). Furthermore, the overall unregulated nature of crypto-exchanges exposes purchasers of crypto-assets to such risks since there is currently no regulation that requires crypto-asset exchanges to have independent audits or be subjected to regulatory scrutiny.

37 www.bbc.com/news/world-us-canada-47203706

Appendix II: Ten Questions to Ask When Considering Crypto-assets for Your Small and Medium-sized Enterprises

1. What is the primary purpose of crypto-assets for my business?
2. Has my business consulted with subject matter experts on any accounting, tax, legal, and regulatory implications of engaging in crypto-asset transactions? Do the people in my business understand all the risks?
3. Will my business leverage a crypto-asset service provider? If so, does that provider have a service auditor's report or alternative sources of assurance that demonstrate the adequacy of the relevant internal controls within their organization?
4. Has my business done other forms of due diligence on the crypto-asset service provider to ensure their security, reliability and integrity meet the standards of my organization?
5. Has my business selected the appropriate crypto-asset wallet type and are there appropriate access controls around those wallets?
6. Are my business's private keys secure? Are they securely backed up and can they be accessed in the absence of the primary key holder? Has my business performed a private key ceremony and implemented appropriate controls to prove ownership of the private key?
7. Has my business developed and documented appropriate accounting policies related to crypto-assets?
8. Has my business discussed with the auditors the implications of crypto-assets for my audit engagement? What additional audit evidence (including internal controls) may they require to address the unique risks of crypto-assets?
9. Does my business understand the local legal obligations and regulatory requirements for crypto-asset transactions? Does my business also understand the differences in treatment of crypto-asset transactions in the other jurisdictions in which we operate?
10. After understanding the risks of engaging in crypto-assets and implementing the appropriate internal controls, is my business comfortable with the residual risks to the organization?

Appendix III: Select Regulatory Guidance

Canadian Securities Administrators (CSA) / Ontario Securities Commission (OSC) / Investment Industry Regulatory Organization of Canada (IIROC)

- August 24, 2017 – CSA Staff Notice 46-307 – *Cryptocurrency Offerings*
- June 6, 2018 – CSA Investor Alert: *Caution urged for Canadians investing with crypto-asset trading platforms*
- June 25, 2018 – IIROC Administrative Notice 18-0119 – *IIROC Priorities for 2019*
  - announces formation of blockchain working group to recommend potential regulatory response.
  - completing industry consultation (Accenture) to better understand regulatory issues relating to innovation, technology and changing client demands.
- July 5, 2018 – OSC Notice 11-781 – *Notice of Statement of Priorities for 2018-2019*
  - supports fintech innovation through OSC LaunchPad; identifies opportunities to modernize regulation; continues to identify regulatory gaps arising from cryptocurrency, initial coin offerings and blockchain developments
- July 10, 2018 – CSA 2017/18 Enforcement Report – *Securities Enforcement in a Connected World*
  - notes creation of Investment Fraud Task Force; co-ordination with global digital platforms to ban advertising of cryptocurrencies and ICOs; first prosecution in Quebec.
- March 14, 2019 – Canada Consultation Paper 21-402 *Proposed Framework for Crypto-Asset Trading Platforms.*

U.S. Securities and Exchange Commission (SEC)

- December 11, 2017 – Statement on Cryptocurrencies and Initial Coin Offerings (SEC Chairman Jay Clayton)
- January 19, 2018 – Joint statement by SEC / Commodity Futures Trading Commission (CFTC) Directors of Enforcement on virtual currency enforcement actions
- January 22, 2018 – SEC Chairman issued warning to companies that change their name to incorporate bitcoin or blockchain

- January 24, 2018 – SEC / CFTC Chairs issued *Wall Street Journal* op-ed that they are closely monitoring cryptocurrency activities; will take action when warranted
- March 7, 2018 – Statement by Divisions of Enforcement and Trading and Markets on potentially unlawful online platforms for trading digital assets
- June 6, 2018 – SEC Chairman Jay Clayton suggests to CNBC that bitcoin is not a security
- November 16, 2018 – Statement on Digital Asset Securities Issuance and Trading
- November 29, 2018 – Two Celebrities Charged With Unlawfully Touting Coin Offerings
- December 12, 2018 – Executives Settle ICO Scam Charges
- February 20, 2019 – Company Settles Unregistered ICO Charges After Self-Reporting to SEC
- April 3, 2019 – Statement on "Framework for 'Investment Contract' Analysis of Digital Assets"

U.S. Financial Industry Regulatory Authority (FINRA)

- December 21, 2017 – "FINRA Warns Investors: Don't Fall for Cryptocurrency-Related Stock Scams"
- May 31, 2018 – Issued an article on "Getting a Handle on Virtual Currencies"
- August 16, 2018 – Investor Alert: Initial Coin Offerings (ICOs) – What to Know Now and Time-Tested Tips for Investors
- September 6, 2018 – Issued an article on "Here's How to Avoid Crypto Stock Scams"
- September 11, 2018 – FINRA Charges Broker with Fraud and Unlawful Distribution of Unregistered Cryptocurrency Securities
- November 29, 2018 – Issued an article on "Storing and Securing Cryptocurrencies"

North American Securities Administrators Association (NASAA)

- January 4, 2018 – Statement on NASAA Statement regarding approaching cryptocurrencies, ICOs and other crypto-related investment products with caution (SEC companion statement)

CHARTERED
PROFESSIONAL
ACCOUNTANTS
CANADA

277 WELLINGTON STREET WEST
TORONTO, ON CANADA M5V 3H2
T. 416 977.3222 F. 416 977.8585
WWW.CPACANADA.CA