Crypto Cyber Considerations – Risk Management & Mitigation Tactics For Accounting Practitioners

Sean Stein Smith
Assistant Professor, Lehman College (CUNY)
Department of Economics and Business
Office 266, Carman Hall
Email: Sean.Steinsmith@lehman.cuny.edu

Abstract: As cryptoassets continue to experience mainstream adoption and implementation by organizations across industry lines, there has been a clear pivot and change in direction in how blockchain and cryptoassets are viewed from an institutional perspective. Following notable examples such as Tesla and Microstrategy, multiple firms and organizations have integrated these technologies to varying degrees. Even as the pace of adoption has continued to accelerate, and proliferate across economic sectors, there are several risk considerations that remain unaddressed on a widespread basis. This research seeks to identify and analyze these risks, as well as propose potential solutions to these areas. Written with an eye toward both an academic and practitioner audience, this research not only identifies and elaborates on several of the most pressing issues facing organizations looking to integrate blockchain and cryptoassets, but also provides a starting point for resolving these items.
Keywords: cryptoassets, blockchain, risk management, cybersecurity, stablecoins

Introduction

The adoption of blockchain and cryptoassets continue to accelerate across the public and private sectors, with virtually every major financial institution, payment processor, and even some governments adopting and legitimizing blockchain and cryptoasset technology. Notable examples of this include, but are not limited to, the development and implementation of crypto-enabled payment systems at organizations such as Mastercard, Visa, PayPal, and eBay, the rolling out of crypto related products and services at dozens of major financial institutions and the recognition of bitcoin as legal tender in El Salvador (Adams, 2021). Framed in this context the continued adoption and implementation of bitcoin and other cryptoassets into the mainstream financial conversation would seem all but assured.

Alongside this adoption, however, there are risks and considerations that need to be taken into account from both a cybersecurity perspective as well as an auditing and internal control angle. Blockchain and cryptoassets, as quickly as they have grown, developed, and become integrated into financial conversations, still represent a relatively new and still-emerging asset class (Yang, 2021). As individuals and organizations, across geographic, economic, and technical boundaries seek to integrate blockchain and cryptoassets into core operations, these risks and considerations will need to be reassessed. Prior to risk assessment and mitigation, however, there also needs to be a process put into place specifying how certain specific tasks and workflows will be put into place at certain firms. This piece will analyze not only how

firms should seek to integrate and implement blockchain and cryptoasset technologies within core operations, but also identify some of the most specific risks as well as outline a potential framework for addressing these potential risks.

Cyber-Specific Risks

With any technology tool and platform, but especially for those affiliated with blockchain technology, there are going to be risks and challenges linked to implementation efforts, but an extra effort must be paid to counteracting cybersecurity risks. Especially since crypto transactions and operations are, by default, a digital and cyber experience and endeavor, the emphasis on cybersecurity and control protocols is even more important than with other initiatives. Regulators have also begun to take a more active approach toward enforcement and compliance around cryptoasset trading, payments, and other activities (Hajric & Bain, 2021). There will invariably be issues linked to any new technology initiative or project, but the implementation of blockchain and cryptoasset technology represent a unique challenge to the profession. Several of the issues that will be raised as a result of this implementation certainly exist, but one issue that seems to be of paramount importance are the issues linked to interoperability. While this issue is not specifically connected to blockchain directly, it is an especially pertinent factor when assessing cyber risks connected to blockchain and cryptoassets.

Interoperability, for the purposes of this research, is the compatibility and ability to share and transmit data between network members in a manner that allows the integrity of said data to be maintained. No matter what technology underlies the application or tool itself, be it blockchain or otherwise, the ability of a technology system to interoperate with other technology platforms is an essential part of the tools ability to succeed moving forward. Specific to the accounting function this would mean that the blockchain-based system would have to connect and communicate with other blockchains, but also be able to connect and communicate other technology systems. This requirement, however, also exposes various blockchain-based applications to hacks and other risks that would not otherwise exist. Hacks and other hacking incidents have occurred related to this sector, and creates the environment where organizations need to develop specific anti-hacking policies connected to blockchain technology.

Hacking Risks

Evidenced by the hacks and other associated data breaches at numerous blockchain and crypto adjacent organizations there are definitive risks associated with the accepting and/or holding of cryptoassets as a payment mechanism. Especially among newer exchanges, organizations, and applications of cryptoasset technology, there is ever-present risk of hacks and breaches. Specifically, one of the most interesting and fastest moving aspects of the cryptoasset space – decentralized finance (DeFi) – can be particularly vulnerable to hacks and customer theft (Graffeo, 2021). The primary reason that said risks exist is the reality that, unlike the underlying blockchain technology, the majority of payment applications and hot wallets (online portals through which investors can access crypto holdings) are not connected or secured by

blockchain technology. Rather, the majority of payment applications and portals are instead simply mobile or web-based applications that are designed with ease of use and convenience as priorities rather than data security. Such an arrangement does allow for more convenient transactions and commercial activity, but does open the door for more frequent hacking and hacking attempts.

In 2021 alone there were a five (5) hacks that totaled more than $1.2 billion in losses and customers funds being stolen which also occurred exclusively at crypto exchanges and DeFi organizations versus more well established organizations such as Coinbase or Binance (Dickens, 2021). As crypto transactions overall grew to $15.8 trillion in 2021 – a 500% increase from 2020 – the total crypto transferred to illicit addresses grew to approximately $14 billion (McAuliffe, 2022). It is true that these illicit transactions only represent a small percentage of total crypto transactions, but when combined with the continuing hacks and breaches that continue to occur this creates a significant risk that organizations and financial professionals need to safeguard against.

On top of the direct financial risks and costs associated with the possibility of hacking there is also the potential for third-party breaches, damages, and risks connected to the processing and storage of cryptoassets. Adding to these potential risks is also the fact that many of the protocols, if not all of them, are relatively new to financial markets, which can lead to dramatic price swings, outages, and other applications issues (Baker & Kharif, 2021). Specifically the regulatory risk that comes with being involved with these types of transactions is not an immaterial item, and needs to be taken into account for planning and continuity purposes. Actions taken, and statements made, in late 2021 by SEC chairperson Gary Gensler – referencing the fact that Coinbase may very well be an exchange with tokens that should be classified as securities – continue to highlight a pivot and shift toward a more aggressive and enforcement based framework for enforcing existing laws and regulations. In other words, processing and enabling crypto transactions may be higher risk than initially though, especially since the majority of institutions involved in such activities are not insured under existing regulations, nor classified as banking entities.

Counterparty Risk

Another consideration and potential risk that should be assessed as part of the cryptoasset payment and custody process is the reality of counterparty risk. Particularly as stablecoins continue to dominate the transactional side and volume of cryptoassets that are used as a medium of exchange the importance of understanding the specifics of counterparty risk cannot be overstated. For example, the following two scenarios could easily play out for organizations seeking to fully integrate stablecoins into ongoing operations.

A preliminary example of these risks can be highlighted if an organization was seeking to leverage stablecoins for transactional purposes in terms of both accepting and using stablecoins for transactions. Despite the fact that stablecoin adoption has continues to accelerate and permeate other aspects of financial markets, regulation around

stablecoins is still both ambiguous and evolving (Versprille, 2021). Assuming that the organization in question possesses the necessary technological expertise and training – whether developed internally our obtained through external consultation – there are still additional risks that need to be considered. Specifically, do all involved organizations understand the mechanics of how the stablecoin in question functions, i.e., the mechanics of stabilization and redemption process? Risks of this kind can manifest if any of the organizations involved – customers, vendors, or the organization itself – wishes to exit the stablecoin positions it had previously established. If such a risk exists or liquidations are apparently unable to be completed, or are only to be completed with significant restrictions, this could negatively impact the fair market value of said instruments. In other words, the very functionality and connection that make stablecoins so appealing could also make them ultimately unusable for transactional purposes.

An additional example of how this might ultimately manifest itself if there is an occurrence where the underlying value of the stablecoin in question becomes doubted. For instance, if there is a stablecoin that is allegedly backed and supported on a one-to-one basis by the U.S. dollar, does the coin issues actually have sufficient dollars in reserve at a FDIC insured institution? This is not merely an academic question, and has caused much of the debate and conversation around just how Tether supports the USDT token. The ongoing dialogue surrounding how USDT is supported is important for two specific reasons, namely the fact that 1) Tether and by extension USDT is the largest stablecoin in terms of market capitalization, and 2) the disclosure around reserves has been a difficult process. Specifically, and something that came as a surprise to some market participants, is that USDT is not 100% supported by U.S. dollars, but rather is backed and supported by a combination of dollars and other assets (Lopatto, 2021).

Especially as the FDIC continues to map out potential regulation and rule-making, and potentially modify rules that it had made prior, it should be clear that thee are not idle concerns (McGrath, 2021). Regulation and rule-making is coming to cryptoassets, and the complication around these issues continues to prove a challenge for rule-making efforts. In other words, as the United States and other countries seek to create a hospitable and innovative environment for cryptoassets, the sometimes conflicting existing guidance only further complicates this conversation (Muzinich, 2021).

Regulatory and Reporting Risk

The cryptoasset sector continues to evolve and mature in a number of innovative and creative ways, but even with this growth the accounting profession remains without crypto-specific guidance. While there is no shortage of opinions and perspectives around how these cryptoassets should be accounted for, there are several more general areas that ideally would be treated as priority issues. These more general areas are not presented to address and raise every potential crypto-specific accounting issue, but rather should be used as a starting point for wider discussion and potential development.

Firstly, the consideration that should be raised as it pertains to crypto accounting is the potential impact of differentiating the accounting treatment for the different cryptoassets that have emerged into the marketplace. Specifically, the question should be raised if it is appropriate for every type of cryptoasset - ranging from bitcoin to privately issued stablecoins to central bank digital currencies to non-fungible tokens - should be treated the exact same way? Building on this, the continued inconsistency with regards to crypto tax treatment further complicates the reporting and valuation issues that can expose organizations to significant reporting risk (Sundaravelue, 2021). Considering the fact that these previously listed cryptoassets are all designed to operate differently, have different valuation and trading implications, and are most likely going to be used for different purposes it would seem illogical to lump them all together in one accounting bracket.

It might make more sense for cryptoassets to be classified and treated as it is linked to the use cases and applications derived from them. Such treatment would not only reflect economic realities on the ground, but would also help enable more transparent and comparable financial information to be published and reported to the marketplace. Such a private market solution and endeavor is seemingly increasing in popularity, as well as reflecting the fast moving cryptoasset sector. In other words, the conversation around crypto regulation and reporting treatment might best be addressed via a combination of public-private research, versus a top-down regulatory approach (Light, 2021). This approach has already been approached and utilized in several jurisdictions, and seems to make sense given the rapid expansion of the sector.

Secondly, the rise of the decentralized finance (DeFi) sector of the blockchain and cryptoasset sector also has created a number of accounting questions. Since regulatory and policy actions are normally taken against organizations in question rather than the end users of these products and services, this is potentially a more complicated question than it might otherwise appear to be. That said, financial operations connected to DeFi include an array of cryptoasset developments that move fay beyond simply transacting in a single cryptoasset.

Staking, block rewards, and the rise of wrapped tokens raise two distinct issues connected to accounting and reporting principles. For example, if a bitcoin is wrapped and - for all intents and purposes - becomes an ERC-20 token (running on the Ethereum blockchain) has the cryptoasset itself actually changed? Crypto staking and block rewards have already raised significant tax related issues, but also create financial accounting and reporting questions as well. Specifically, which of the counterparties involved should be allowed to recognize these coins or tokens, and what criteria should be utilized to establish which entity can recognize these coins or tokens?

Central Bank Digital Currency Risks

One other area of potential risk for organizations seeking to integrate crypto payments and other aspects of crypto within core operations is the continuing investment and focus being allocated to the concept of central bank digital currencies (CBDCs). For the

purposes of this research a CBDC can be defined as a cryptoasset that is developed, issued, and governed by either a central government, nation-state, or other form of centralized governmental agency. In almost every instance the goal of a CBDC is to either augment or entirely replace the current fiat currencies wherever these currencies are presently used. The specifics of the CBDC itself will, of course, vary depending on the jurisdiction in question, but generally speaking the aim is to render the present currency obsolete. Appealing as this might be, as nations capture and leverage the benefits of blockchain-based payments, the risks are clear whereas the benefits remain – to this point – more conceptual than applied (Torres, 2021). The development and implementation of a CBDC is no small task, nor is the utilization of these crypto for payment purposes something that should be undertaken lightly.

For risks and risks management associated with organizations seeking to use and implement a CBDC there are several that can be applied and referenced across the board. Lack of interoperability and refusal to accept these coins as a legitimate medium of payment represent real and tangible risks to the continued roll-out of such a currency. Put simply for a CBDC to operate as advertised and effectively these cryptoassets must interoperate with every single payment channel or platform in use in those areas, and must do so on a continuous basis. On top of this technical risk there is also the possibility – that depending on the credit worthiness of the issuing nation – that not every counterparty or related entity will accept these CBDCs are an acceptable medium of exchange.

Framework for Implementation

While there are certainly risks and challenges that are embedded with the growing implementation and onboarding of blockchain and cryptoassets in the mainstream economy that does not mean the pace of adoption is going to diminish. Rather, and taking into account both the rapid adoption of blockchain and crypto by individuals and institutions alike, the number of organizations seeking to integrate cryptoassets are going to increase. That said, and acknowledging that every organization is going to be different, there are several key factors and considerations that should be incorporated into a policy framework.

The first thing that an organization should seek to plan out and understand is what specific types of crypto should be accepted and held as a payment tool. Specific risks and factors that are linked to this decision include, but are not limited to, whether or not the organization in question is looking to process and hold stablecoins, decentralized cryptocurrencies such as bitcoin, or some other form of cryptoasset. Each of these cryptoassets brings with it distinct factors and items with regards to reporting, custody, and other disclosure requirements.

After deciding what types of cryptoassets are to be accepted there needs to be a discussion around what third party service provider will be used in order to process and record payments correctly with the existing accounting and finance software. While there are numerous such organizations in the marketplace, there is an additional

question that needs to be asked; how straight-forward is it to convert these cryptoassets into fiat currencies? Will the company attempt to partner with a third-party service provider, or will the company seek to develop an in-house wallet storage solution? Building on this question there are additional considerations that should be taken into account that include, but are not limited to, the following. Firstly, will the cryptoassets stored and managed on behalf of customers be held in a hot or cold wallet, and with that sub-decision there are other factors such as cyber-security or physical access policies that should be outlined.

Secondly, and directly related to the wallet decisions is how customers will be able to access funds on their behalf. Especially for incumbent financial institutions that are seeking to expand product and service offerings into the blockchain and cryptoasset sector there is going to be the need to update controls and workflows within the organization. Put simply the ability to lend and extend financing to individual and institutional customers is going to be constrained if indeed an institution wants to be involved in the issuance and active management of specific cryptoassets without making the necessary updates to existing policies and controls.

Lastly, there is also a consideration that needs to be taken into account around the reality that not every organization will want to receive and hold cryptoassets on the balance sheet of the organization. In other words, and building on an earlier point, does it make sense for the entity in question to store and hold cryptoassets, or should they immediately convert them back into fiat currencies? While this might make sense from a risk management perspective, and reduce some risks linked to holding cryptoassets, such an approach also does increase the number of taxable transactions that will need to be handled by the organization in question. This is due to the fact that in the United States every transactions involving crypto is a taxable transaction, and that global crypto tax regulations are inconsistent in terms of terminology and enforcement.

Stablecoin Banking Risks

During the last few months of 2021 in the United States there was conversation around the potential for regulating stablecoin issuers as banking institutions, and with this comes several considerations that need to be integrated into how this might move forward. First and foremost it is important to note that while on the surface increasing the regulation around stablecoin issuers might not make certain actors in the cryptoasset sector feel incredibly enthusiastic going forward, it is a necessary part of the maturation of the space. Put another, the regulation and constructing of compliance mechanisms around stablecoin issuers and other cryptoasset organizations means that – far from banning or outlawing crypto and blockchain applications – cryptoasset applications are increasingly becoming mainstream.

Secondly, this is reflective of the understanding and acknowledgment by both private sector actors and regulators that the banking sector itself will have to evolve in order to keep pace with the rapidly developing cryptoasset sector. Banks and other financial institutions may have initially not been fans or supporters of cryptoassets, but have

increasingly begun offering services in these areas. While this has been emerging, a parallel trend has emerged in crypto-native organizations; a realization that combative or adversarial relationships with policymakers is not conducive to long-term sector growth. Framed in an alternative light, as banking institutions have pivoted toward crypto offerings, cryptoasset organizations have pivoted toward offering banking services.

Either way, and no matter how the conversation continues to develop it is imperative that these regulatory conversations involve an iterative process that involve all interested counterparties. There are several examples of regulatory approaches and frameworks that have been developed and implemented in states like Wyoming, this might involve the creation of a new form of banking entity, or simply the integration of cryptoasset services into existing financial institutions. As these developments occur, however, there are several policy considerations that need to be integrated into how risk is managed and reported about moving forward.

Financial stability and systemic risk, and outlined below in the conversation around the Fall 2021 President's Working Group, a primary risk around the rapid introduction of stablecoins into the financial services space is the potential for such a dramatic change in how financial payments processed. Specifically, the issues around the redemption risk and conversion risk must be reasonably acknowledged and accounted for. Simply stating that the odds of this are low is not enough; frameworks and policies must be implemented to help ensure that as cryptoassets become increasingly mainstream and integrated into financial transactions that these tools operate as advertised.

U.S. President's Working Group Report

An additional, and somewhat complementary regulatory update that was issued toward the very end of 2021 was the report published by the President's Working Group that focused almost exclusively on stablecoins, and the role of stablecoins in the payments marketplace. Despite the bias against stablecoins and stablecoin utilization, there are several key facts that this document does illustrate effectively (Rinearson, 2021). During 2020-2021, as referenced in the report itself, the utilization of stablecoins for transactional purposes has increased by approximately 500%. Market capitalization and nominal trading value has increased as nearly as fast a rate, and this highlights the two distinct facts. Firstly, the value and dramatic run-up in valuations serves a prime example of just how much external value the marketplace – and organizations therein – are placing on these assets. Secondly, as these individual assets and part of the marketplace continue to become more integrated within incumbent financial institutions and payment rails the controls and processes surrounding these instruments are going to become more important.

Clearly the implications of this report, and the suggestions contained therein, are going to be difficult to determine until such a time that the market is more matured and readily prepared for this report. That said, it is reasonable to expect the suggestions and recommendations included in this document are going to have a significant influence on

the broader regulatory conversation. It is also worth noting that the tone and approach to the stablecoin marketplace by the authors of this document – granted incumbent financial institutions – was not universally negative, the slant in this piece did tend to be more negative in nature.

Several of the core considerations that need to be taken into account as this plan becomes implemented, which it realistically will eventually become either directly or indirectly, is the fact that these measures will need to evolve over time. Given the fact that this report was focused on U.S. markets it makes sense that the conversation and regulatory focus would center around U.S. markets. Interestingly enough this report also overtly documented the fact that the vast majority of stablecoin transactions are indeed connected to a small handful of stablecoins backed and supported by the U.S. dollar. Even though the tone and focus of this whitepaper tended to focus on potential future regulation, this does not seem to be having any kind of chilling effect on the sector at large. Rather, and especially among the larger players in the space, the opinion was that more transparent and consistent regulation is a good thing for the future development of the space (Crosman, 2021). This may indeed represent the current state of the current stablecoin marketplace, but is no guarantee that this trend will continue into the future. As of this writing there are well approximately 100 nations across the world that are actively working on developing some form of either state-supported stablecoin or a central bank digital currency.

As the marketplace continues to evolve and mature the odds of a small handful of U.S. dollar supported stablecoins continuing to dominate the marketplace on an almost exclusive basis will most assuredly decrease over time. Such a development reflects both the increasing economic leadership of non-U.S. markets as well as a traditional precedent including the rotating nature of reserve currency leadership on an international basis. That said, it is important to recognize that other nations might have lessons to teach U.S. policymakers with regards to currency development and implementation issues, with experience both with the benefits and risks linked to currency changes (Gillespie, 2021). As organizations implement, whether voluntarily or not, certain types of state backed stablecoins or other central bank digital currencies, the need for interoperability to be addressed and addressed will continue to increase. Put another way the increased diversification of the cryptoasset and stablecoin sector is bound to increase moving forward.

Cyber Insurance Risks

The issues connected to insurance and cyber insurance are by no means unique or differentiated specifically to the blockchain and cryptoasset sector. Alongside the rise and proliferation of technology tools such as artificial intelligence, robotic process automation, data analytics, blockchain, and cryptoassets are the risks connected to such operations. Risks connected to data storage and management are well known, and have been documented across a variety of industries; blockchain and cryptoassets are no exception to this trend.

Where the balance of power can change and pivot, however, is where the dialogue around blockchain and cryptoassets are concerned. As the cryptoasset class continues to increase in size and variety, with a collective valuation of nearly $3 trillion, the risks connected to hacks and breaches will only increase (Ossinger, 2021). Specifically, the risks and potential risks linked directly to implementation of said tools and applications will need to be embedded in insurance policies. Such policies will need to be updated for the accounting firms as well as the clients who are actively investing in these technologies. Breaking down some of the core cyber-security risks that can arise over time include, but are not limited to, the following:

Coverage for certain activities. Perhaps the most obvious place to start the analysis of blockchain and crypto cyber insurance policies would be whether or not the specific activities entered into by an organization will be covered. Errors and omissions insurance is a commonplace insurance policy used at organizations, but is not broad enough to guarantee coverage of activities connected to blockchain and cryptoassets. Prior to any specific type of activity being entered into, the management team of the organization should try to ensure that these activities will not expose the organization to unnecessary risk.

Coverage for holding assets. Offering crypto custodial services is a fast-growing aspect and area of the blockchain and cryptoasset sector, but how exactly does these activities impact the risk profile of organization at large? It would be safe to say that – generally speaking – that entering into the blockchain and crypto spaces do increase the risk profile of the underlying operations. Building on that, and especially as organizations offer custodial services, it makes sense that insurance coverage will have to reflect this development.

Sector specific risks. On top of the risks that are often connected and linked to cryptoassets on their own there are also the regulatory and policy risks that are directly connected to certain economic sectors. For example an insurance organization might seek to implement blockchain to facilitate the speed and accuracy of payments, but might not be able to share all pertinent information across organizational lines

These specific risks and issues often lead organizations, looking to integrate blockchain and cryptoassets into operations, to instead start this journey at a simpler point in the organization hierarchy, oftentimes via payments and payment processing. Even if these less complicated areas are where implementation starts, however, there are factors that need to be integrated into said implementation plan.

Payment Strategy Considerations

Something that is often overlooked when discussing the potential risks and opportunities connected to the implementation of cryptoassets of any kind are the risks and cyber considerations that should be incorporated into the establishing of a payment system. Even well established and mass market payment processors such as Mastercard collaborate with crypto-native organizations for payment purposes

(Fitzgerald, 2021). Outside of the previously stated and analyzed risks there are also several factors that need to be assessed when and if an organization is going actively establish a crypto-denominated payment system. Every organization is going to operate differently, and so the specifics of a payment system will differ depending on the criteria required. That said, there are several factors that should be integrated into any conversation regarding this initiative.

Firstly, what specific cryptoassets are going to be accepted for payment and transactional purposes? Wharton, for example, has begun accepting crypto as tuition payments for blockchain course, specifying bitcoin as the cryptoasset that will be taken in lieu of normal (dollar-based) tuition payments (Kharif, 2021). This might seem like a technical question, but is one that can appear overly simplistic upon initial review, as every individual cryptoassets operates differently and has different risks linked to it. For example, accepting bitcoin for payment at this point is a relatively straight-forward matter as this point, with numerous payment processors and credit card organizations offering such services. Conversely, if non-fungible tokens (NFTs) are to be accepted for compensatory purposes this can bring with it a whole array of different risks and opportunities, such as how the value of these tokens as established, the functionality of these tokens, and the potential use cases for said tokens.

Secondly, after the criteria for crypto payments has been established there needs to be an additional choice made as to whether or not the crypto that had been accepted for payment will be converted immediately to fiat or held over the longer term. There are risks involved in both strategies, clearly, but they are distinct and unique risks that should be assessed on their own due to the significant differences. For example if an organization seeks to hold onto cryptoassets that have been receive for payment or other transactional purposes, how will these cryptoassets be held and secured? Hacks continue to occur at exchanges and other organizations whose primary business model is conducting cryptoasset transactions, and non-crypto native organizations will also face these exact same risks (Yang, 2021). Questions around securing and safeguarding cryptoassets generally bifurcate along two separate tracks; utilizing a hot wallet platform or cold wallet hardware.

Hot wallets can be best summarized as an online portal that allows real-time, instantaneous, and easily accessible options for individuals and institutions. That said, it is also worth noting that these hot wallets do not have any significant blockchain enabled encryption or security, and must instead rely on traditional web-based security or password protocols. Building on this fact, it is worth noting that many of the high profile hacks associated with the blockchain and cryptoasset sector does not have to do with the specific blockchains in question, but instead are caused by the vulnerabilities of hot wallets.

Cold wallets are specialized hardware devices that are customized and designed exclusively for holding and storing cryptoasset information. These devices are hardware, not continuously connected to the internet or any online portal, and are generally thought of as a more secure option versus hot wallets. On a technical basis

this is correct, hacking or gaining access is going to require increased effort with lower successful results for hackers or other bad actors. This does not mean that a cold wallet will necessarily always be safer (Alexander, 2019), but does add an additional layer of security due to the disconnected nature of the tool.

Either way, implementing a crypto payment strategy will incur some sort of potential risk and upside regardless of what specifics are incorporated into the payment plan itself. One other area that should be assessed is how the training and education related to blockchain and cryptoassets will be incorporated into ongoing operations. Trainings and education related to any one specific tool can include specific task related applications, but also need to touch on how these tools will change the current tasks and jobs of employees. The technological aspects of blockchain and cryptoassets have bee proven to work time and again; that is beyond dispute. What still needs to be addressed, however, is how the leadership team will actively encourage the staff and middle management to effectively utilize these tools. Oftentimes, as with virtually every other technology tool or upgrade, the most difficult part is usually the human facet of the conversation.

Cyber Risk Mitigation

After analyzing and examining the array of risks and potential risk connected to blockchain and cryptoassets it might seem difficult to effectively integrate these tools into core business operations. It is correct that, due to cost, risk, and technical complexity, the implementation of blockchain and cryptoassets remains a technically and financial challenging endeavor. Setting that aside, however, there are numerous examples illustrating just how this exact event has occurred at organizations across multiple economic sectors. In other words there are multiple examples of firms and countries that have embraced cryptoassets successfully, and established crypto payment systems on a wide ranging basis (Co, Sidiropoulos & Kalogirou, 2021). While every organization is going to operate differently, and will need to assess the risks and opportunities on a case-by-case basis, there are several common guidelines that can – and should – drive the implementation conversation moving forward.

1. Conduct exploratory research within the organization. Prior to the budgeting, purchasing, and implementing of any specific blockchain and cryptoasset issue there must be research conducted as to both the appropriateness and reasonableness of this project. Questions that should be asked at this juncture include 1) does it make sense for the organization to develop an in-house solution or purchase with an external third-party, 2) is this initiative going to include blockchain or blockchain and cryptoassets, and 3) what will be done with the information stored on the underlying blockchain?
2. Develop a specific plan. Mentioned previously in this piece, a common pitfall and obstacle toward successful implementation is the lack of planning and preparation on the side of the organization? The blockchain and cryptoasset sector is rapidly growing, widely differentiated, and lacking in virtually any standardization so it falls to the organization to develop a plan that reflects not

only the blockchain and cryptoasset space, but how the organization will implement and utilize these assets moving forward.

3. Implementation via iteration. As tempting as it is for management professionals to seek implementation across the board at the organization a more practical and realistic approach would seem to be to gradually integrate blockchain and cryptoassets into operations. In other words, simply because non-fungible tokens or other new applications of cryptoassets may be trendy or hot topics, there is no need for an organization to operationalize these specific tools immediately. Rather, it would be more reasonable experiment and stress test the implementation around these tools as the business evolves over time.

The above mentioned steps and factors should be integrated alongside other technology best practices such as employee training, ensuring that the technology tools used at the organization are both up-to-date, and the most current version available, and that interoperability issues are proactively addressed. Interoperability might seem like a technical topic that is not the concern of non-technical experts or users of these tools, but is an area that needs to be effectively addressed and resolved in order to realize the benefits of blockchain and cryptoassets. If these tools are unable to effectively communicate and work with each other it is unrealistic to expect that risk will be lower as a result.

Conclusions and Action Steps

It should be clear to any and all market participants that blockchain and cryptoassets have absolutely achieved mainstream understanding, but that wider adoption is not an easy or quick step away. The specifics of how these tools will be implemented will clearly vary from organization to organization, and while this is true it is also worth pointing out that there are several commonalities that can and should be understood and taken into account by management teams across the board. Setting aside the promise and potential of cryptoassets, of which there is not an insignificant amount, there are also risks that management professionals must take into account. Risks and risk factors connected to insurance items, operational issues, and the difficulties associated with even designing a robust crypto payment system all represent significant items that need to be assessed and accounted for moving forward. That said, these and other risks are no reason to avoid, or put off, blockchain and cryptoasset adoption. Instead, organizations across different economic sectors should take the lessons learned from other areas, modify and tweak them as necessary, and implement them within organizations. Action steps, including those outlined in this research, should not be viewed as an authoritative nor exhaustive listing of factors, but rather an effective starting point for further conversation and analysis.

References

Adams, J. (2021). Mastercard’s buy-in a turning point for crypto payments. *American Banker*, *186*(31), 5–6.

Alexander, D. (2019). Quadriga Crypto Mystery Deepens With “Cold Wallets” Found Empty. *Bloomberg.Com*, N.PAG

Baker, N., & Kharif, O. (2021). Crypto Keeps Breaking. *Bloomberg Businessweek*, *4725*, 35–36.

Co, E. N. &, Sidiropoulos, I., & Kalogirou, X. (2021). Fintech and the payment ecosystem: Cyprus and the world. *International Financial Law Review*, N.PAG.

Crosman, P. (2021). Stablecoin issuers say they’re unafraid of regulation. *American Banker*, *186*(192), 5.

Dickens, S. (2021). The five biggest cryptocurrency hacks of the year. *Yahoo Finance.* N.PAG.

Fitzgerald, K. (2021). Mastercard, Bakkt team up for crypto card payments. *American Banker*, *186*(206), 11.

Gillespie, P. (2021). Argentina, Land of Currency Crises, Warns About Crypto Risks. *Bloomberg.Com*, N.PAG.

Graffeo, E. (2021). DeFi Protocol Cream Finance Loses $130 Million in Latest Crypto Hack. *Bloomberg.Com*, N.PAG.

Hajric, V., & Bain, B. (2021). The SEC Is On the Prowl For Crypto. *Bloomberg Businessweek*, *4713*, 27–29.

Kharif, O. (2021). Wharton to Accept Crypto as Tuition Payment for Blockchain Class. *Bloomberg.Com*, N.PAG.

Light, J. (2021). Crypto’s Regulation Fix: We’ll Handle It. *Bloomberg Businessweek*, *4721*, 34–35.

Lopatto, E. (2021). The Tether Controversy, Explained. *The Verge.* N.PAG.

McAuliffe, Z. (2022). Cryptocurrency crime hit a record $14B in 2021, report says. *CNET.* N.PAG.

McGrath, L. (2021). FDIC Is Preparing Guidance on Banks and Crypto. *Bloomberg.Com*, 416.

Muzinich, J. (2021). America’s Crypto Conundrum. *Foreign Affairs*, *100*(6), 129–141.

Ossinger, J. (2021). Crypto World Hits $3 Trillion Market Cap as Ether, Bitcoin Gain. *Bloomberg.Com*, N.PAG.

Rinearson, J. (2021). What the President's Working Group got wrong about stablecoins. *American Banker*, *186*(225), 10–11.

Sundaravelu, A. (2021). US tax regulation still too ambiguous on classifying crypto assets. *International Tax Review*, N.PAG.

Torres, C. (2021). Quarles Says Fed Digital Dollar Poses Risks With Unclear Benefit. *Bloomberg.Com*, N.PAG.

Versprille, A. (2021). Stablecoin Issuers Should Choose Rule Model, Key Lawmaker Says. *Bloomberg.Com*, 1.

Yang, Y. (2021). NYC, Miami Seen Facing "Ponzi Scheme" Risks With Crypto Push. *Bloomberg.Com*, N.PAG.

Yang, Y. (2021). Crypto Exchange BitMart Vows Compensate for $150 Million Hack. *Bloomberg.Com*, N.PAG.