CURRENT ISSUES IN AUDITING
Vol. 16, No. 2
Fall 2022
pp. A10–A17

American Accounting Association
DOI: 10.2308/CIIA-2020-038

Determining the Inherent Risks of Cryptocurrency: A Survey Analysis

Steven A. Harrast
Debra McGilsky
Yan (Tricia) Sun
Central Michigan University

SUMMARY: Cryptocurrencies pose several risks that impact the inherent risk assessments of auditors. The SEC has issued warnings about the risks (Clayton 2017), and the PCAOB lists virtual assets as a key focus area in future inspections (Vincent and Wilkins 2020). This study examines how accounting professionals perceive the inherent risks associated with cryptocurrency based on their likelihood of occurrence and expected impact on financial statements. We find the risk of determining cryptocurrency value is perceived as having the highest likelihood of occurrence, and unauthorized private key access has the highest impact. Combining the evaluations of likelihood and impact, we rank the risk of ineffective exchange-level controls as having the highest inherent risk. We also find that inherent risk judgments are negatively correlated with cryptocurrency experience. Professionals with prior cryptocurrency experience, or who work for a company planning to process cryptocurrency transactions, rate inherent risk lower than those with less experience.

Keywords: cryptocurrency; risk; inherent risk; exchange risk; risk rankings; cryptocurrency risk judgments; accounting risk judgments; ineffective exchange controls.

I. INTRODUCTION

The concept of a privately minted (or mined) cryptocurrency has garnered significant attention and financial resources ever since Bitcoin first appeared in 2009 (Clayton 2017; Marr 2017). Part of the attention is likely due to the novelty of a currency outside the traditional banking system and the symbolism of modern information technology challenging, and perhaps undermining, long-established and powerful institutions. Cryptocurrencies rely on an

The authors thank Denise Dickins (editor) and two anonymous reviewers, as well as the support of a research grant from the School of Accounting at Central Michigan University.

Steven A. Harrast, Debra McGilsky, and Yan (Tricia) Sun, Central Michigan University, College of Business Administration, Department of Accounting, Mt. Pleasant, MI, USA.

Editor's note: Accepted by Denise Dickins.

Submitted: November 2020
Accepted: May 2021
Published Online: June 2021

informal network of peer computers to validate and record transactions rather than a formal banking system. They are available to anyone with a credit card and can be purchased without any form of identification using apps, websites, or kiosks in hotels. Cryptocurrency is being accepted for payment by a growing list of companies (Hopkins 2020), including criminal enterprises demanding extortion payments for ransomware attacks (Popper 2015).

Cryptocurrencies can experience significant price volatility since the amount in circulation cannot be quickly manipulated, unlike in a presumed low-risk central bank monetary system. In September 2020, for example, a single Bitcoin was trading around $11,000; by February 2021 it traded at over $50,000.

Due to these characteristics, cryptocurrencies look more like securities than stable currencies. However, regulation of cryptocurrencies has proved slippery as exchanges transcend national borders, and trades are conducted in cyberspace using anonymous key values that lack biographical or company identifiers. Cryptocurrencies have been able to mostly circumvent registration as securities, and as of 2017 the Securities and Exchange Commission (SEC) had not registered a single initial coin offering (ICO) (Clayton 2017). More recently, the SEC has challenged the failure of companies to register ICOs as securities (SEC 2020), and at least one company claims to have registered (IPX 2021). The Internal Revenue Service (IRS) has found no formal way to track cryptocurrency gains and losses, although it did recently obtain account holder information from exchanges which it used to alert about 10,000 account holders of their obligation to report taxable events (Erb 2019).

The SEC has warned investors to be cautious with cryptocurrencies (Clayton 2017). According to SEC public statements regarding cryptocurrency "*there is substantially less investor protection than in our traditional securities markets, with correspondingly greater opportunities for fraud and manipulation*" (Clayton 2017, emphasis in the original). The PCAOB recently announced it has added virtual assets as a key area for future inspections (Vincent and Wilkins 2020). This raises the stakes for auditors and makes risk identification a critical task.

The Digital Assets Working Group (DAWG) of the American Institute of Certified Public Accountants (AICPA) recently issued a Practice Aid providing guidance on accounting for and auditing digital assets (AICPA 2020). It states cryptocurrencies should be reported as intangible assets and tested for impairment. It also provides four areas auditors need to assess before accepting or continuing an engagement with entities in the digital asset ecosystem. They are: (1) auditor skill sets and competencies, (2) management skill sets and competencies, (3) management integrity and the entity's overall business strategy, and (4) processes and controls, including information technology systems. Each area presents unique risks and challenges.

Vincent and Wilkins (2020) discuss audit risks and challenges imposed by the novelty, ambiguity, and lack of official guidance surrounding cryptocurrency transactions. Sterley (2019) and Smith and Castonguay (2019) agree the accounting profession lacks formal guidance on accounting for and auditing cryptocurrency. Vincent and Wilkins (2020) present a client acceptance model based on firm competency and resources as well as a cryptocurrency risk framework. The framework summarizes commonly used financial assertions, current audit procedures, and additional risks and challenges inherent in cryptocurrencies for auditors to consider when planning and performing an audit.

Our research complements the work of Vincent and Wilkins (2020) by focusing on understanding the inherent risks of cryptocurrency in an audit context and addresses the AICPA's guidance on assessing auditors' knowledge and expertise in digital assets. The assessment of the inherent risk of cryptocurrency is necessary to mitigate the risk of accepting an engagement the auditor is not capable of effectively performing. Specifically, we asked accounting professionals to evaluate the qualitative components of the inherent risk of cryptocurrency, the likelihood of

occurrence and the expected impact on the financial statements.[1] Combining these risks enables us to rank the inherent risks of cryptocurrency. We also explore the correlation between characteristics of accounting professionals (e.g., professional experience, cryptocurrency experience) and their inherent risk judgments.

II. THE SURVEY

Both the Chartered Professional Accountants Canada (CPAC) and the DAWG published audit considerations related to cryptocurrencies (CPAC 2018; AICPA 2020). The AICPA (2020) suggests that firms should "[b]uild general awareness among firm personnel of the risks inherent in the digital asset ecosystem, so that current auditors understand such risks and what resources are available for existing client engagements." The CPAC (2018) published a list of nine specific cryptocurrency risks to consider when planning engagements or when deciding whether an auditor possesses sufficient cryptocurrency expertise to accept an engagement. These risks are:

1. The entity chooses to use a cryptocurrency exchange that does not have effective controls over the transactions it enters into on behalf of the entity or over the balances of cryptocurrency maintained in the entity's accounts.
2. The entity has a cryptocurrency wallet that has not been accounted for.
3. The entity loses a private key and therefore can no longer access the related cryptocurrency.
4. An unauthorized party obtains access to the entity's private key and steals the entity's cryptocurrency.
5. The entity misrepresents ownership of a private key and therefore of the related cryptocurrency.
6. The entity sends cryptocurrency to an incorrect address and the cryptocurrency cannot be recovered.
7. The entity enters into and records a cryptocurrency transaction with a related party that cannot be identified because of the anonymity of parties to blockchain transactions.
8. There are significant delays in processing cryptocurrency transactions at the end of a period.
9. Events or conditions make it difficult to determine the value at which a cryptocurrency should be recorded for financial reporting purposes.

Some risks have a higher likelihood or impact than others. For example, a private key is a secret number known only to the person who generated it that allows the holder to access funds on a blockchain. The loss of a private key would prevent access or use of the cryptocurrency making this a high-impact risk. Conversely, delays in processing cryptocurrency at the end of a reporting period may have a high likelihood of occurrence, but for private enterprises its impact could be small.

The participants are told:

> For this section of the survey, you are assessing **risk of material misstatement** of financial statements similar to what an auditor might do in the planning stages of an audit. Please read the ten **risk** scenarios and then assess the **likelihood** of occurrence and the **impact** of the occurrence on the financial statements. Please assume in all scenarios: (1) the company is currently engaging in cryptocurrency transactions and/or mining and (2) all cryptocurrency transactions and balances are **material** (i.e., greater than 5 percent of total assets).

[1] Institutional Review Board exemption was granted by Central Michigan University.

TABLE 1

Sample Characteristics of 52 Subjects

Subject Background and Experience	Number of Responses	Percentage of Responses
1. Currently employed in public accounting	29	56%
2. Hold CPA, CISA, CIA or CMA	36	69%
3. Work/worked in accounting or auditing	51	98%
4. More than two years work experience	42	81%
5. Company planning or working on cryptocurrency	9	17%
6. Personal cryptocurrency experience	9	17%
7. Cryptocurrency engagements	4	8%
8. Cryptocurrency audit training and/or discussions	16	31%

The CPAC risks are the basis for nine of the ten survey scenarios. For example, we ask the participants:

> **The entity chooses to use a cryptocurrency exchange that does not have effective controls over the transactions it enters into on behalf of the entity or over the balances of cryptocurrency maintained in the entity's accounts.** To the best of your judgment, please assess the likelihood of this scenario occurring (scale of 1 = very high, to 5 = very low, and 6 = unable to determine) and the impact it would have on the financial statements (identical scale) if the scenario occurred.

We also collect demographic and experience data of the participants.[2]

Responses from 52 accounting professionals serve as the basis for the study's results. Demographic data of the participants are reported in Table 1.[3] Of the participants, 56 percent are currently employed in public accounting, 81 percent have more than two years of work experience, and 69 percent hold professional accounting certifications. Important to the purpose of our study,

[2] We collected data for our analyses by emailing an electronic survey to a list of alumni and personal contacts in professional accounting positions and encouraging the potential participants to forward the survey to others to produce a snowball sample. The three sections of the survey were background (demographics and experience), inherent risk and audit fee questions, and the risk scenarios and questions. The background questions were intended to gain a better picture of the professional background of the research subjects including years of experience, certifications, direct auditing and accounting experience, and experience with cryptocurrencies. The inherent risk and fee section consisted of two questions about the participants' perception of cryptocurrency transactions on audit risk and audit fees. The third section presented ten cryptocurrency risk scenarios which we asked participants to rate on two dimensions: likelihood and impact. Qualitative responses recorded in the background section were coded by the researchers with the integers 1 to 5 for very low to very high, and 0 for unable to determine. Failure to respond was coded 0. There were four unanswered questions out of 1,040 numeric responses (0.38 percent). Nulls/blanks and observations marked "unable to determine" are dropped from the analysis of each scenario (not included in the risk means and rankings) but are retained for the regressions. Retaining observations containing "unable to determine" and null responses retains records with many otherwise valid responses while introducing some noise into the regression. Overall, because of the relatively small number of observations, the need to preserve records holds greater weight than the issue of noise in the data. Having this noise in the data tends to increase variance and biases against findings with statistical significance.

[3] The average survey duration was 12 minutes, 34 seconds. The longest duration was three hours, 20 minutes, and 28 seconds. Two surveys were completed in less than three minutes. These observations were removed from the analyses as this was considered insufficient to carefully respond to the survey questions.

TABLE 2

Risk Factors and Rankings

Risk	Likelihood Mean (1)	Impact Mean (2)	Inherent Risk Total [Likelihood (1) + Impact (2)]	Inherent Risk Ranking	n(1)/n(2)
Ineffective exchange controls over transactions and balances	3.31	4.00	7.31	1	51/51
Difficulty determining cryptocurrency value	3.45	3.74	7.19	2	51/50
Unauthorized private key access	2.98	4.15	7.13	3	49/47
Unsecure private key[a]	3.06	3.96	7.02	4	49/47
Unaccounted crypto wallet	3.04	3.81	6.85	5	51/47
Unidentified related-party transaction	3.29	3.29	6.58	6	49/51
Misrepresentation of ownership	2.71	3.86	6.57	7	51/49
Lost private key	2.75	3.71	6.46	8	48/45
Cryptocurrency sent to wrong address	2.82	3.54	6.36	9	51/50
Significant delay in end-of-period processing	2.80	3.12	5.92	10	49/49

[a] Indicates risk added by authors.

17 percent have personal experience with cryptocurrency—they personally own or control a company that owns cryptocurrency, 17 percent have worked for a company that has or is considering having cryptocurrency transactions, 8 percent have worked on client engagements where the client held or mined cryptocurrency engagements, and 31 percent have had cryptocurrency audit training and/or discussions within their company or firm about cryptocurrencies. Beyond formal instruction, it is probable that accounting professionals have exposure to firm updates and media reports concerning the risks of cryptocurrency.

III. RESULTS

Table 2 tabulates the participants' evaluations of the likelihood and impact of cryptocurrency risks which are ranked in order of inherent risk (sum of likelihood and impact). The likelihood and impact measures have a theoretical maximum value of 5 and a minimum of 1 (zeros and nulls are not included in this analysis), therefore inherent risk has a theoretical maximum of 10 and a minimum of 2.

The cryptocurrency risk that participants perceive as having the highest likelihood of occurrence is difficulty determining cryptocurrency value. Cryptocurrency value is much more difficult to establish than the value of an exchange-traded security or currency. Although popular cryptocurrencies are frequently traded, different exchanges have different currency values, and there is no standardized coin price. Any snapshot of the price can only provide guidance for determining cryptocurrency value (Deloitte 2021). Most published coin prices are averages based on recent trades at prominent exchanges (Reiff 2019). Lack of trades make valuation subjective and difficult. Vincent and Wilkins (2020) identify several risk factors of inaccurate valuations (low trading volume and difficulty converting cryptocurrencies to cash, etc.) and make suggestions for mitigating risks, such as determining management's method of valuation.

The accounting professional-participants perceive unauthorized private key access as having the highest impact on the financial statements. Cryptocurrencies are stored in a software wallet

accessed for spending using a private key. Access to a private key value constitutes the ability to use currency in the software wallet. If the private key is compromised, losses can be staggering for an entity storing a significant amount of cryptocurrency in its wallet. The AICPA (2020) suggests that auditors inquire about the segregation of duties related to authorizing cryptocurrency transactions as well as determining who has access to the keys and how many users are required to process a transaction. Physical location and security of that location are also of high concern.

Combining the participants' reports of likelihood and impact, ineffective exchange controls over transactions is the highest ranked cryptocurrency inherent risk. Ineffective exchange-level controls can lead to unsecure private keys and unauthorized transfers of balances. This was the case for Coincheck that lost an estimated $520 million when private keys were maintained online in a "hot wallet" (Bloomberg 2018). The hot wallet was accessed and hundreds of millions in cryptocurrency were stolen from exchange accounts. Ineffective exchange-level controls pose high risk and may not be controllable from the perspective of the coin owner; however, the more established exchanges may have the resources to develop stronger controls. The AICPA (2020) recommends understanding the process of interacting with exchanges and confirming cryptocurrency balances to help mitigate this risk.

To determine the impact of an accountant's experience with cryptocurrency on their risk assessments, we regressed measures of inherent risk and audit fees (as a proxy for audit risk) on each of the experience and demographic characteristics reported in Table 2. The regression model and explanation of variables are described in Table 3.

We find that personal cryptocurrency experience and working with a company planning or working on cryptocurrency are significant predictors of inherent risk. Having cryptocurrency experience reduces the perception of inherent risk. There are several potential explanations for this finding. Prior literature shows that experience influences the selection and weighting of information cues (Bonner 1990). An experienced auditor's knowledge structure enables the auditor to identify the information cues that should be selected and appropriately weighted to form the auditor's judgment (Bonner 1990; Libby 1995). Fazio and Zanna (1978) hypothesize that inexperienced decision makers have a lower confidence level than experienced decision makers. Another possible explanation is that as individuals become more familiar with the technologies enabling cryptocurrency, their confidence in the technologies and controls increases. The cryptocurrency environment itself may attract individuals who tend to underestimate risk, while individuals outside it may overestimate risk.

IV. CONCLUSIONS

The growing acceptance of and use of cryptocurrencies increases the need for accounting and auditing professionals to understand the inherent risks of cryptocurrency. Our ranking of cryptocurrency inherent risk both informs managers in establishing and monitoring internal controls over cryptocurrency transactions and informs auditors in planning an effective audit for clients with cryptocurrency transactions. While our finding that higher levels of cryptocurrency experience bias toward lower inherent risk evaluations is mostly of theoretical significance, it can help set expectations on audit engagements.

This research has certain limitations. First, all the survey's scenarios asked about increasing or heightened risk of cryptocurrency. Participants were not given decreasing or lower risk options which could have influenced their risk evaluations. Since the study was primarily focused on cryptocurrency risks relative to one another, we do not believe this limitation nullifies its conclusions. Second, our focus was on the inherent risks of cryptocurrency rather than overall

TABLE 3

Inherent Risk and Audit Fee Regressions Equation

$$INHERENT\ RISK(or\ AUDIT\ FEE) = \beta_0 + \beta_1(CEPA) + \beta_2(CERT) + \beta_3(WAA) + \beta_4(WE2) + \beta_5(PCE) + \beta_6(CPWC) + \beta_7(WCE) + \beta_8(CATD) + \in_i$$

Variable	Definition
INHERENT RISK[a]	A dummy variable equal to 1 (raise) or 0 (lower or no change) based on the subject's response to the question, "how will cryptocurrency transactions and/or accounts affect general audit risk (inherent risk) all other things being equal?"
AUDIT FEE[a]	A dummy variable equal to 1 (raise) or 0 (lower or no change) based on the subject's response to the question, "how will material cryptocurrency transactions and/or accounts affect audit fees all other things being equal?"
CEPA	A dummy variable equal to 1 if a subject is currently employed in public accounting, and 0 otherwise.
CERT	A dummy variable equal to 1 if a subject currently holds a certification (CPA, CISA, CIA, or CMA), and 0 otherwise.
WAA	A dummy variable equal to 1 if a subject has worked in accounting or auditing, and 0 otherwise.
WE2	A dummy variable equal to 1 if a subject has more than two years work experience, and 0 otherwise.
PCE	A dummy variable equal to 1 if a subject has personal cryptocurrency experience (mining or holding cryptocurrency personally or through a closely held company), and 0 otherwise.
CPWC	A dummy variable equal to 1 if the company/employer is processing or planning to process cryptocurrency transactions, and 0 otherwise.
WCE	A dummy variable equal to 1 if the subject has worked on engagements where clients were involved with cryptocurrency (held as investment, mined, processed transactions), and 0 otherwise.
CATD	A dummy variable equal to 1 if the subject has had cryptocurrency audit experience or training (involved in audit testing, audit training specifically related to cryptocurrency), and 0 otherwise.

[a] *AUDIT FEE* is substituted for *INHERENT RISK* in the second regression.
One subject responded "unable to determine" on both the inherent risk and audit fee questions. This response was coded as 0 for both regressions.

audit risk, which could be a subject of future research. Third, the inherent risk measures are based on the judgments of accounting professionals. Support for accuracy of these judgments may evolve over time as additional research is conducted.

REFERENCES

American Institute of Certified Public Accountants (AICPA). 2020. *Accounting for and Auditing of Digital Assets*. Durham, NC: AICPA. Available at: https://us.aicpa.org/content/dam/aicpa/interestareas/informationtechnology/downloadabledocuments/2104-39790-da-pda-update-web.pdf

Bloomberg. 2018. How to steal $500 million in cryptocurrency. *Fortune* (January 31). Available at: https://fortune.com/2018/01/31/coincheck-hack-how/

Bonner, S. E. 1990. Experience effects in auditing: The role of task-specific knowledge. *The Accounting Review* 65 (1): 72–92.

Chartered Professional Accountants Canada (CPAC). 2018. *Audit Considerations Related to Cryptocurrency Assets and Transactions*. Toronto, Canada: CPAC. Available at: https://www.cpacanada.ca/en/business-and-accounting-resources/audit-and-assurance/canadian-auditing-standards-cas/publications/cryptocurrency-audit-considerations

Clayton, J. 2017. *Statement on Cryptocurrencies and Initial Coin Offerings*. Washington, DC: SEC. Available at: https://www.sec.gov/news/public-statement/statement-clayton-2017-12-11

Deloitte. 2021. *Corporates Investing in Crypto*. London, UK: Deloitte. Available at: https://www2.deloitte.com/us/en/pages/audit/articles/corporates-investing-in-crypto.html

Erb, K. 2019. *IRS sending warning letters to more than 10,000 taxpayers about cryptocurrency reporting*. (June 26). Available at: https://www.forbes.com/sites/kellyphillipserb/2019/07/26/irs-sending-warning-letters-to-more-than-10000-taxpayers-about-cryptocurrency-reporting/#786228345d3b

Fazio, R. H., and M. P. Zanna. 1978. On the predictive validity of attitudes: The roles of direct experience and confidence. *Journal of Personality* 46 (2): 228–243. https://doi.org/10.1111/j.1467-6494.1978.tb00177.x

Hopkins, P. 2020. Companies accepting Bitcoin: Why corporate is taking crypto. *SmartBrief* (August 5). Available at: https://www.smartbrief.com/original/2020/08/companies-accepting-bitcoin-why-corporate-taking-crypto

IPX. 2021. *Prospectus Supplement, Amendment No. 2 to Form F-1*. (March 30). Washington, DC: SEC. Available at: https://www.sec.gov/Archives/edgar/data/0001725882/000121390021018494/ea138533-posam_inxlimited.htm#a_001

Libby, R., 1995. The role of knowledge and memory in audit judgment. In *Judgment and Decision-Making Research in Accounting and Auditing*, edited by R. H. Ashton and A. H. Ashton, 176–206. Cambridge, UK: Cambridge University Press. Available at: https://www.cambridge.org/core/books/abs/judgment-and-decisionmaking-research-in-accounting-and-auditing/role-of-knowledge-and-memory-in-audit-judgment/08FF018437C1BB175E1CBA6FC51E18FD

Marr, B. 2017. A short history of Bitcoin and crypto currency everyone should read. *Forbes* (December 6). Available at: https://www.forbes.com/sites/bernardmarr/2017/12/06/a-short-history-of-bitcoin-and-crypto-currency-everyone-should-read/#633c436c3f27

Popper, N. 2015. For ransom, Bitcoin replaces the bag of bills. *The New York Times* (July 25). Available at: https://www.nytimes.com/2015/07/26/business/dealbook/for-ransom-bitcoin-replaces-the-bag-of-bills.html

Reiff, N. 2019. Why is the price of Bitcoin different around the world? *Investopedia* (June 25). Available at: https://www.investopedia.com/news/why-price-bitcoin-different-around-world/#:~:text=The%20primary%20explanation%20for%20discrepancies,any%20given%20period%20of%20time

Securities and Exchange Commission (SEC). 2020. *Unregistered ICO Issuer Agrees to Disable Tokens and Pay Penalty for Distribution to Harmed Investors*. SEC Press Release. (September 15). Washington, DC: SEC. Available at: https://www.sec.gov/news/press-release/2020-211

Smith, S. S., and J. Castonguay. 2019. Accounting for cryptoassets. *Strategic Finance* 101 (5): 30–37.

Sterley, A. 2019. Cryptoassets: Accounting for an emerging asset class. *The CPA Journal* 89 (6): 6–7.

Vincent, N. E., and A. M. Wilkins. 2020. Challenges when auditing cryptocurrencies. *Current Issues in Auditing* 14 (1): A46–A58. https://doi.org/10.2308/ciia-52675