CHARTERED PROFESSIONAL ACCOUNTANTS CANADA

VIEWPOINTS:

Applying Canadian Auditing Standards (CAS) in the Crypto-Asset Ecosystem

AUDITING MINING REVENUE OF ENTITIES ENGAGED IN CRYPTO-ASSET MINING

OCTOBER 2022

Crypto-Asset Auditing Discussion Group

The rapid rise and volatility of crypto-assets have led to increased global interest and scrutiny by organizations, investors, regulators, governments and others. An entity's financial statements may include material crypto-asset balances and transactions. Auditors need to be aware of the challenges when auditing these balances and transactions. The Chartered Professional Accountants of Canada (CPA Canada) and the Auditing and Assurance Standards Board (AASB) created the Crypto-Asset Auditing Discussion Group with representatives from the Canadian Public Accountability Board (CPAB), provincial practice inspection, academia, and firms in Canada to share views on the application of the CAS when auditing in the crypto-asset ecosystem.

Disclaimer: The views expressed in this series are non-authoritative and have not been formally endorsed by CPA Canada, the AASB, CPAB, or the firms and other organizations represented by the discussion group members. Members may have differing views on how the guidance suggested in this *Viewpoints* should be implemented.

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 of, or reliance on this material.

The technologies supporting crypto-assets can be complex and the content of this *Viewpoints* reflects this reality. For reasons of brevity, explanations are not provided for all technical concepts mentioned. Expertise in blockchain technology and related fields, such as cryptography, is often needed when auditing crypto-asset balances and transactions. It is therefore typical for the auditor to use the work of an auditor's expert.

There is no current section of the International Financial Reporting Standards (IFRS) handbook that specifically addresses crypto-asset mining. The industry has generally reported that there are contracts or arrangements between the miner and the pool and/or blockchain, leading to a revenue conclusion under IFRS 15. However, the facts and circumstances of each arrangement need to be carefully examined and the associated accounting considered. For the purposes of this document, we have presumed that IFRS 15 does apply, but are cautioning readers that this may not apply in all circumstances. In addition, the term "contract" used throughout this document is intended to include any type of arrangement and agreement between a miner and a mining pool.

Background

As the crypto-asset market continues to expand, it has highlighted challenges for auditors in obtaining assurance over this complex asset class. Traditional audit procedures may not provide appropriate evidence when auditing crypto-asset balances and transactions. Given the unique risks in this emerging industry, auditors may need to explore different ways of responding to these risks. However, due to the relatively short time frame that crypto-assets have been in existence, typical audit approaches or guidance – in Canada or globally – may present challenges in application. This inevitably increases the risk of inconsistency in practice amongst auditors and firms alike.

An audit of a crypto-asset mining entity (crypto-asset miner) presents unique audit considerations, some of which are addressed in this paper. One of the main challenges currently in the market is a gap between what crypto-asset miners expect when they undergo a financial statement audit and the auditors' responsibilities in order to comply with CAS. This challenge, amongst others, is resulting in a turnover of auditors for entities in this industry.

Purpose

The purpose of this paper is to:

- assist auditors or prospective auditors of crypto-asset miners (specifically proof of work miners) in understanding the unique risks and challenges in auditing mining revenue
- assist crypto-asset miners in understanding auditor responsibilities and requirements in facilitating the execution of the audit

By providing non-authoritative guidance for auditors and their (prospective) clients, our aim is to drive increased consistency in practice to support high-quality audits.

Scope

This paper focuses specifically on considerations regarding auditing crypto-asset mining revenue. This can be applied to companies running their own mining operations or to miners participating in a pool. In developing this guidance and to illustrate certain matters of interest, the paper considers a public company applying IFRS; however, the guidance may also be considered by entities applying other accounting standards to the extent that the accounting requirements are similar to IFRS.

Frequently asked questions (FAQ)

The following questions are covered in a FAQ format:

1. Why can auditing a crypto-asset miner be difficult?
2. When looking for an audit, what can a crypto-asset miner expect from the auditor as they undertake their client acceptance procedures?
3. Since the transactions are recorded on the blockchain, can the auditor simply place reliance on the blockchain itself?
4. Can the auditor rely on transactions that are confirmed with the mining pool?

5. What are some of the types of controls, including general information technology controls (GITCs), that the auditor may be interested in understanding and testing?
6. What controls are necessary over the physical mining assets?
7. What are some of the additional considerations when the crypto-asset miner hosts machines for third parties?

Appendix – Illustrative examples

Two examples showing substantive analytical procedures are provided in the Appendix. These examples show varying levels of complexity to illustrate inputs that may be required to develop an expectation at an appropriate level of precision.

Note that the questions covered in this paper are not exhaustive and the examples are for illustrative purposes only. Appropriateness of audit procedures depends on the individual facts and circumstances of the entity and audit risks. The approach should be tailored accordingly.

Frequently asked questions

1. Why can auditing a crypto-asset miner be difficult?

The pseudo-anonymity of the blockchain may bring unique challenges to both the audit and the development of a robust control environment by management. This can create challenges, for example, in the entity's ability to demonstrate the completion of their performance obligations (as required by the accounting revenue recognition standards) and demonstration of ownership of the digital assets.

Revenue from Contracts with Customers[1] has a five-step model that is used to determine when revenue can be recognized. These criteria are applied by the reporting issuer when determining when to recognize mining revenue and are considered by the auditor when performing audit procedures over revenue. In particular, it may not be sufficient for management to simply use crypto-assets received as the trigger when recognizing revenue. Management must demonstrate, and the auditor needs to verify, that the performance obligation (as defined in IFRS 15) has been satisfied, meaning that the mining entity has performed a service and has been compensated accordingly. Without this, it can be difficult for the entity to demonstrate that they have earned all revenue being reported or that they have received all revenue to which they are entitled.

In addition, in a financial statement audit the auditor is required to identify and assess the risks of material misstatement due to fraud[2]. The business model of crypto-asset mining raises unique opportunities to commit fraud. Here are some examples:

- The miner "spoofs" generating revenue that would be earned for hash power delivered to the mining pool using a separate arrangement (e.g., a borrowing arrangement, arrangement with a related party) with another party to deposit crypto-assets or transaction fees into its mining

1 IFRS 15, *Revenue from Contracts with Customers*, paragraph 9.

2 CAS 240, *The Auditor's Responsibilities Related to Fraud in an Audit of Financial Statements*, paragraphs 17 and 24.

rewards wallets. If the auditor is not informed of this arrangement the miner could attempt to present the borrowed assets received as revenue in its financial statements.

- An individual at the entity, without the authorization of management, gains access to the mining hardware and redirects a fraction of the hash power to a non-company affiliated wallet. This would result in reduced revenue for the entity and misappropriation of the entity's assets (through stealing hash rate, rewards or electricity).
- A mining pool does not deliver the proportionate share of mining rewards owed to a participant in the mining pool, undercompensating the miner in the process and reducing revenue for the entity.

These examples are not meant to be an exhaustive list but provide insight into the unique fraud opportunities that may be available in the crypto-asset mining industry. The auditor may not be able to obtain audit evidence to address these risks based on substantive procedures alone and may need to rely on the entity having appropriate internal controls to mitigate these risks[3].

2. When looking for an audit, what can a crypto-asset miner expect from the auditor as they undertake their client acceptance procedures?

Due to the auditing challenges noted in the industry, the auditor may need to perform additional procedures to satisfy the firm requirements for client acceptance. These procedures may include in-depth procedures to understand the operations of the entity, including control walkthroughs and obtaining and analyzing contracts. The purpose of these procedures is to assess the current control environment and structure to identify if the entity has put in place the appropriate processes, systems, and controls to report its mining operating results. This information can help the auditor determine if it is likely they will be able to obtain sufficient appropriate audit evidence over the financial statements as a whole. If these procedures are not performed prior to client acceptance there is a risk that the auditor may be forced to resign at a later date if sufficient appropriate audit evidence cannot be obtained.

For controls, the auditor may inquire about controls in areas such as: revenue recognition, completeness of revenue including considerations over the reliability of the underlying data, mining assets, anti-money laundering (AML) and know your customer (KYC), related parties, etc. They may also inquire about service providers who are involved with the entity's crypto-assets, such as custodians or crypto-asset trading platforms. The auditor may also consider initial tests of controls to assess their design and operating effectiveness prior to acceptance. The use of information technology (IT), blockchain or other specialists may be required in assessing controls due to the complexity of the systems.

The auditor may ask for a sample of contracts, such as those with a mining pool. The structure of these arrangements can be very complex and have significant impacts on the auditing and accounting, both of which need to be understood by the auditor.

3 CAS 330, *The Auditor's Responses to Assessed Risks*, paragraph 8(b).

In addition, the auditor may ask questions about sources of financing and the management and governance structure of the entity, including management's level of financial reporting and crypto-asset experience. If entity management is lacking in either, this can be a hurdle to an auditor's client acceptance process.

In many instances, these procedures take additional time as compared to the client acceptance procedures in other, and potentially less complex, industries. Entities should be prepared for this when they are looking to engage an audit firm. The auditor may also need to perform such in-depth procedures annually to satisfy the firm requirements for client continuance or retention.

It is highly recommended that appropriate and verifiable control activities and governance structures be implemented by management prior to beginning a discussion with a potential auditor as they contribute to a robust control environment, especially for reporting issuers who also have certification responsibilities on the operating effectiveness of controls.

3. Since the transactions are recorded on the blockchain, can the auditor simply place reliance on the blockchain itself?

While tracing to the blockchain may demonstrate that the crypto-asset exists, it does not demonstrate the completion of the performance obligation[4], and therefore does not provide sufficient audit evidence to support the recognition of revenue.

The blockchain also cannot demonstrate the completeness of revenue, as it will not disclose how much revenue the entity was actually entitled to. In other words, the blockchain will only show a transfer of a crypto-asset to the entity.

Finally, it is still up to the entity to demonstrate that the crypto-asset on the blockchain actually belongs to the entity since the blockchain itself cannot demonstrate ownership. Access alone to a crypto-asset wallet does not demonstrate ownership. Further guidance on ownership is available in CPA Canada's publication titled ***Obtaining Audit Evidence to support the Ownership Assertion***.

Audit evidence obtained from the blockchain will need to be combined with other audit procedures to provide audit evidence over the completeness and occurrence of revenue.
Examples of other audit procedures could include:

- control procedures related to the entity's internal monitoring systems to measure hash power
- control procedures over the entity's mining hardware controls
- confirmation with the mining pool (if a pool is used)
- analytics performed by management as part of their control environment which may be used as the basis for the auditor's analytical procedures

4 IFRS 15, paragraph 31.

- other substantive procedures, such as measuring the amount of revenue expected to be generated based on other verifiable variables. An example of an analytic of this nature is provided in the Appendix of this paper, which can be combined with other methods and audit evidence to address the revenue recognition requirements without relying solely on the amounts received as evidence

It should be noted that reliance on a substantive analytical procedure requires a significant amount of work from the auditor. The level of precision required from the analytic is high and the work required to evaluate the relevance and reliability of all material inputs is significant due to the risk profile of crypto-assets.

Finally, if the auditor is using tools to evaluate the blockchain the auditor is also required to evaluate the reliability of the tools[5]. Learn about the factors an auditor may consider regarding the reliability of a blockchain itself (from which the information is obtained) and the appropriateness of technological resources, such as block explorers (used to display the information recorded on a blockchain) in CPA Canada's publication on the *Relevance and Reliability of Information from a Blockchain*.

4. Can the auditor rely on transactions that are confirmed with the mining pool?

If the auditor plans to rely on third-party confirmations, the auditor needs to consider whether information is relevant and reliable[6]. In the case of crypto-asset mining pools, at the time of publication, most pools in Canada do not have control reports, such as a system and organization controls (SOC) 1 report. When a SOC 1 Type 2 report is available, the auditor may use the report to evaluate whether the information reported by the mining pool operator is subject to controls that are designed, implemented, and operating effectively[7]. When the auditor is unable to use a SOC 1 Type 2 report, the auditor would need to find other ways to verify the reliability of the information provided by the pool (such as external verification of inputs, consistency with management records, etc.).[8] This often leads back to the entity's own systems for tracking hash power and demonstrating the completion of the revenue performance obligation. Further guidance on third-party service providers is available in CPA Canada's publication titled *Third-Party Service Provider Considerations*.

It is important that the auditor sufficiently understands the relationship between the entity being audited and the pool to assess the audit evidence required to audit the revenue from the pool. In some instances, the auditor may be able to audit around the pool, but the auditor will need to understand the mechanisms used by the pool to measure and distribute rewards amongst the mining pool participants.

The auditor also needs to perform procedures to ensure that crypto-asset revenue is actually coming from the pool and not from other sources, as this could be an indicator of fraud as further described in question #1.

5 CAS 500, *Audit Evidence*, paragraph 9.

6 CAS 500, paragraph 7.

7 CAS 402, *Audit Considerations Relating to an Entity using a Service Organization*, paragraph 17.

8 CAS 402, paragraph 12(b)-(d).

5. What are some of the types of controls, including general information technology controls (GITCs), that the auditor may be interested in understanding and testing?

The entity needs to be able to demonstrate they have fulfilled the performance obligation related to the crypto-asset mining revenue. The entity cannot rely solely on the blockchain or remittances from the pool to record revenue. Understanding management controls over mining revenue is essential for the auditor and the controls can be highly sophisticated. In addition to controls over revenue, the auditor would expect a combination of:

- physical controls over mining hardware
- mining monitoring systems
- AML/KYC controls when engaging in buying or selling crypto-assets or entering into mining revenue contracts
- GITCs

If crypto-assets are held by the entity after mining activities occur, controls over wallets including appropriate segregation of duties, private key generation, lifecycle management and other controls over existence, and rights and obligations would be expected.

In the area of GITCs, certain standard GITCs have a greater level of importance because of the risk associated with misappropriation of crypto-assets. The following is a non-exhaustive list of the types of controls that a mining operation may be expected to establish. Each mining operation is unique and may structure their controls in different ways to achieve the same control objectives.

- **Logical access controls** over how user accounts are granted, periodically reviewed, and revoked. This would include considerations over the usernames and passwords to access the mining hardware, where the pool membership and reward wallets are set, or collective management software if that is used instead. The initial granting of access should be approved by a member of management, and the evidence of that approval should be retained. Periodic review of access involves obtaining a user list from each machine, as well as any software used to manage all of the machines collectively and having a member of management review who has access and the level of access granted. Revocation of access should involve retaining evidence that the user access for employees departing or changing roles was revoked, generally within 24 hours or less of the event.
- **Change controls** over the programming code used in operations.
  - Where a client maintains custom code, the programmers should not have access to the production version of the code. Instead, code should be migrated from the development environment to a code repository. A testing group should retrieve the code from the repository and compile it into a testing/business user acceptance environment where its functionality is tested. Once it passes the user acceptance testing, then it should be promoted into production by a system administrator who is different from the programmer.
  - Where the client is using purchased software, similar user acceptance testing should be completed prior to promoting the software into production.

  - A file integrity monitoring system should be used to detect changes in software or configurations on servers and mining machines to detect unauthorized changes, including changes to the mining pool configuration and rewards wallet.

- **Manage operations controls** including monitoring mining machine, power consumption, or downtime and a follow-up process to return down miners into production. This will reduce the risk that mining equipment is inappropriately reported as being down when their hash power is being diverted for personal gain by employees.

6. What controls are generally necessary over the physical mining assets?

Auditors may require evidence through control procedures over the existence of material assets used in the mining operations. Controls may include those related to:

- restriction of physical access to the hardware
- regular counting and physical inspection of hardware
- the purchase and disposal of hardware
- monitoring of hardware up and downtime
- Power Purchase Agreement obligations, etc.

7. What are some of the additional considerations when the crypto-asset miner hosts machines for third parties?

Given the significant infrastructure requirements to host a crypto-asset mining operation, it is not uncommon for miners to host their own mining equipment alongside third-party equipment or to rent out the use of equipment to third parties. If the entity under audit hosts machines for other entities it can create additional complexities. For instance, how does the company properly track the relative contribution of each machine to ensure that the crypto-asset is properly allocated and distributed? These arrangements highlight again the need for the auditor to fully understand all mining arrangements in order to identify and assess risks and develop an appropriate audit approach.

Different types of hosting arrangements can raise various financial reporting questions (and audit considerations) related to allocation of revenue, expenses, and ownership of assets, among others.

Appendix – Illustrative examples

Bitcoin mining revenue analytics

The following are examples of substantive analytical procedures that an auditor may prepare to predict the expected revenue from Bitcoin mining operations. Appropriateness of audit procedures depends on the individual facts and circumstances related to the entity and the audit risks identified in the engagement. The audit approach and procedures are tailored accordingly to these facts and circumstances.

The Bitcoin network is calibrated so that a new block is discovered approximately every 10 minutes. If more mining capacity comes online and the time between discoveries shortens to less than 10 minutes, then the network automatically increases the level of difficulty so that more work is required to mine a block, returning the average time to every 10 minutes. Conversely, if mining capacity goes offline and the average time between discoveries increases beyond 10 minutes, then the level of difficulty is decreased again, returning the average time to 10 minutes. Because of this auto-calibration mechanism, an average of 144 new blocks are added to the Bitcoin network every day, as reflected in equation D in the first example below.

The reward earned for discovering a new block is calculated using a pre-determined schedule embedded in the Bitcoin blockchain. This reward is cut in half every 210,000 blocks, or approximately every 4 years. In 2009, the reward was 50 Bitcoins, then 25 in 2013, then 12.5 in 2016, and now 6.25 as of 2020, as reflected in the illustrative examples.

Due to the nature of mining, rewards from solo mining, where an organization mines themselves and does not share their computing capacity or winnings with others, are inherently uneven. There will be periods where no rewards are earned at all, and then a block is successfully mined, and the earnings are briefly much higher than the long run average. Because of this, the earnings from small solo mining operations are inherently very difficult to predict and do not lend themselves well to this analytic. It is common for miners to be members of pools, whereby thousands of mining computers owned by different entities share their computational power and share in their earnings. This allows for much more evenly spread earnings and lends itself well to this analytic. The pool operator typically charges a fee, such as 1%, to cover their costs of running the pool. This pool fee must be subtracted from the expected earnings of the miner.

An auditor should validate all significant inputs into this model, including machine hash rate, client hash rate, network hash rate, pool fee, Bitcoin price, actual electricity usage per machine, total electricity usage per utility bill, and final earnings received from the mining pool. In addition, actual electricity consumption should be used to verify representations from management about machine uptime. The difference between the expected revenue should then be compared against the actual results and differences should be analyzed to determine their source and the reasonableness in the context of the materiality of the client.

Example 1

The first example calculates the expected revenue in a year of a single mining computer with specifications of a hash rate of 110 terahashes per second (TH/s) and a power consumption of 3,250 watts. The hash rate is a measure of the computational power of the mining computer, with a higher number indicating a higher rate of mining. Different mining computers have different hash rates, so this must be adjusted for the hardware used in a specific mining operation. This example assumes that the single computer has 100% uptime.

Example 2

The second example shows the uptime percentages by month for 20 mining computers. Machines 1-4 are sold towards the end of the year and therefore finish with 0% uptime, while machines 15-20 are purchased throughout the year and therefore start with 0% uptime. Other uptime percentages reflect technical issues, power outages, maintenance, and voluntary idling of the machines by the mining operator. The total machine equivalents are then calculated at the bottom, as well as the expected annual revenue for the pool and the expected electricity usage.

EXAMPLE 1: EXPECTED OUTPUT FOR 1 MACHINE WITH 100% UPTIME

Month (2021)	Client Hash Rate (TH/s) A	Network Hash Rate (TH/s) B[9]	Days in Month C	Blocks per Month D = C x 144	Reward per Block (BTC) E	Pool Fee F	Expected Revenue (BTC) G = (A/B) x D x E x (1-F)	Bitcoin Price (CAD) H[10, 11]	Expected Revenue (CAD) I = G x H	Hours J = C X 24	Watts Usage K	Electricity Usage (kWh) L = J x K / 1000
Jan	110	149,196,972	31	4,464	6.25	1%	0.02036	44,064	897	744	3,250	2,418
Feb	110	155,100,116	28	4,032	6.25	1%	0.01769	58,315	1,032	672	3,250	2,184
Mar	110	159,601,625	31	4,464	6.25	1%	0.01904	68,467	1,304	744	3,250	2,418
Apr	110	157,234,579	30	4,320	6.25	1%	0.01870	71,385	1,335	720	3,250	2,340
May	110	161,245,123	31	4,464	6.25	1%	0.01884	57,123	1,076	744	3,250	2,418
Jun	110	120,098,019	30	4,320	6.25	1%	0.02448	43,867	1,074	720	3,250	2,340
Jul	110	100,355,391	31	4,464	6.25	1%	0.03028	42,881	1,298	744	3,250	2,418
Aug	110	120,709,404	31	4,464	6.25	1%	0.02517	57,390	1,445	744	3,250	2,418
Sep	110	136,607,014	30	4,320	6.25	1%	0.02152	58,345	1,256	720	3,250	2,340
Oct	110	149,109,956	31	4,464	6.25	1%	0.02038	71,330	1,454	744	3,250	2,418
Nov	110	160,886,125	30	4,320	6.25	1%	0.01828	76,494	1,398	720	3,250	2,340
Dec	110	173,191,889	31	4,464	6.25	1%	0.01754	63,546	1,115	744	3,250	2,418
Total							**0.25228**	**713,207**	**14,684**			**28,470**

9 Source for monthly average bitcoin network hash rates (TH/s): www.blockchain.com/charts/hash-rate

10 Source for monthly average USD market-prices across major bitcoin exchanges: www.blockchain.com/charts/market-price

11 Source for monthly average exchange rates for conversion from USD to CAD: www.bankofcanada.ca/rates/exchange/

EXAMPLE 2: EXPECTED OUTPUT FOR 20 MACHINES WITH VARIABLE UPTIME

Month (2021)	Eqn.	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec	Total
Revenue for 100% uptime per machine (CAD)	**A**	897	1,032	1,304	1,335	1,076	1,074	1,298	1,445	1,256	1,454	1,398	1,115	14,684
Electricity usage for 100% uptime per machine (kWh)	**B**	2,418	2,184	2,418	2,340	2,418	2,340	2,418	2,418	2,340	2,418	2,340	2,418	28,470
Machine 1		96%	95%	95%	96%	99%	93%	98%	100%	17%	0%	0%	0%	
Machine 2		97%	99%	99%	95%	97%	95%	96%	96%	96%	9%	0%	0%	
Machine 3		93%	95%	95%	98%	99%	95%	99%	100%	93%	2%	0%	0%	
Machine 4		93%	96%	95%	94%	97%	98%	96%	94%	98%	95%	14%	0%	
Machine 5		97%	98%	94%	96%	94%	99%	95%	100%	97%	96%	12%	17%	
Machine 6		97%	99%	95%	97%	99%	97%	94%	98%	99%	95%	95%	94%	
Machine 7		96%	97%	95%	93%	97%	97%	97%	95%	99%	97%	99%	95%	
Machine 8		94%	93%	97%	97%	98%	96%	98%	97%	100%	94%	93%	97%	
Machine 9		94%	99%	99%	96%	99%	100%	96%	95%	94%	94%	97%	98%	
Machine 10		99%	99%	93%	99%	100%	96%	94%	99%	94%	99%	100%	97%	
Machine 11		93%	97%	97%	93%	95%	94%	98%	97%	95%	100%	94%	97%	
Machine 12		95%	97%	93%	94%	97%	98%	99%	96%	98%	96%	94%	99%	
Machine 13		98%	95%	100%	94%	99%	96%	98%	96%	96%	93%	96%	93%	
Machine 14		95%	94%	97%	100%	99%	95%	100%	98%	99%	96%	99%	98%	
Machine 15		0%	4%	94%	95%	94%	94%	96%	98%	97%	96%	96%	96%	
Machine 16		0%	0%	7%	97%	99%	98%	93%	93%	98%	99%	97%	94%	
Machine 17		0%	0%	0%	16%	97%	96%	100%	94%	99%	98%	95%	95%	
Machine 18		0%	0%	0%	0%	17%	95%	94%	98%	96%	100%	97%	97%	
Machine 19		0%	0%	0%	0%	0%	17%	98%	100%	99%	98%	97%	93%	
Machine 20		0%	0%	0%	0%	0%	0%	8%	96%	95%	96%	97%	93%	
Total Machine Equivalents	**C**	**1337%**	**1357%**	**1445%**	**1550%**	**1676%**	**1749%**	**1847%**	**1940%**	**1859%**	**1653%**	**1472%**	**1453%**	
Expected Revenue (CAD)	**D = A x C**	11,993	14,004	18,843	20,693	18,034	18,784	23,974	28,033	23,349	24,035	20,579	16,201	238,522
Expected Electricity Usage (kWh)	**E = B x C**	32,329	29,637	34,940	36,270	40,526	40,927	44,660	46,909	43,501	39,970	34,445	35,134	459,248

Acknowledgments

CPA Canada wishes to express its gratitude to the CPA Canada and Auditing and Assurance Standards Board's Crypto-Asset Auditing Discussion Group for its assistance in the authoring and review of this publication. The Discussion Group is composed of representatives from the Canadian Public Accountability Board, provincial practice inspection, academia, and volunteers from the following Canadian firms: BDO, Deloitte, Davidson & Company, EY, KPMG, MNP, PwC, and Raymond Chabot Grant Thornton.

CPA Canada gratefully acknowledges PwC for leading the authoring of this publication and EY for providing the illustrative examples on behalf of the Discussion Group.

Additional resources

Visit CPA Canada's blockchain and crypto-assets resource page for the following, and other relevant resources for CPAs:

1. Audit considerations related to cryptocurrency assets and transactions (2018)
2. Viewpoints (Auditing crypto-assets): Are tests of controls needed regarding the ownership assertion? (2020)
3. Viewpoints (Auditing crypto-assets): Relevance and reliability of information from a blockchain (2020)
4. Viewpoints (Auditing crypto-assets): Third-party service provider considerations (2021)

Comments

Comments on this *Viewpoints* or suggestions for future *Viewpoints* should be sent to:

Grace Gilewicz, CPA
Principal, Audit & Assurance
Research, Guidance and Support
Chartered Professional Accountants of Canada
277 Wellington Street West
Toronto ON M5V 3H2
Email: ggilewicz@cpacanada.ca