Migration Letters

Volume: 20, No: S5(2023), pp. 181-201

ISSN: 1741-8984 (Print) ISSN: 1741-8992 (Online)
www.migrationletters.com

A Proposed Auditing Program for Auditing Cryptocurrencies Transactions – Analytical Study

Aya Taha Hussein Ali[1], Dr. Sinan Zuhair Muhammed Jameel[2]

Abstract

Cryptocurrencies are still a bit of an unknown entity when it comes to audit and assurance. What considerations do auditors need to take on board? & How we audit cryptocurrency?

A program for auditing cryptocurrency transactions has been proposed and it's important that Ernst & Young EY, one of the major Big 4 companies in auditing, published, on 01/30/2020, an article entitled, (How to audit the next generation of digital assets). and this article ended by acknowledging the emergence of a new generation of digital assets (cryptocurrencies), promising more stability. Since these cryptocurrencies frequently appear in financial statements, the question auditors have to consider is, how are these assets audited?

The Institute of Chartered Accountants in England and Wales ICAEW published on 09/12/2022 an article regarding the audit of entities that use cryptocurrencies, calling for the provision of an audit program for cryptocurrencies and it was titled "How to audit cryptocurrencies?" and mentioned that there are still significant challenges facing these entities when it comes to auditing accounting transactions for them, such as what considerations should auditors take? Cryptocurrency is still fairly new, even though it has been around for over a decade. Especially in the absence of any publications from professional organizations, as a result, it can be very difficult to audit. There is a real risk that cryptocurrencies could be overvalued or undervalued, given this lack of comprehensive guidance. This means that the audit risk is higher, which must be considered while accepting and retaining the customer and planning the audit procedures. It also means that auditors often have no choice but to apply steadfast general principles such as "prudential" and "On going concern".

Cryptocurrencies were also mentioned in the Journal of Accountancy article, as FASB was appointed to draft a disclosure standard for cryptocurrencies on 12/16/2022, and the Financial Accounting Standards Board (FASB) made several interim board decisions regarding its project on currency disclosure. encrypted, and the Board agreed to create a draft presentation to update the relevant accounting standards. Subsequently, the Financial Accounting Standards Board determined that entities - public and private - that maintain cryptocurrency pools within the scope of the project will be required to:

FASB decided that entities — both public and private — that hold crypto-assets within the scope of the project would be required to:

- *At a minimum, present the aggregate amount of crypto-assets separately from other intangible assets that are measured using other measurement bases.*

[1] Accounting department, College of administration & economics, University of Mosul, Iraq, aya.21bap153@student.uomosul.edu.iq

[2] Accounting department, College of administration & economics, University of Mosul, Iraq, sananzuhair@uomosul.edu.iq

- *Present gains and losses on crypto-assets in net income and present those gains and losses separately from the income statement effects of other intangible assets, such as amortization or impairments.*

- *Classify crypto-assets received as noncash consideration during the ordinary course of business that are converted nearly immediately into cash as operating cash flows.*

FASB also decided that investment companies should present their financial statements with presentation requirements in FASB ASC Topic 946, Financial Services — Investment Companies, and not-for-profit entities by the presentation requirements in Topic 958, Not-for-Profit Entities. And the board affirmed that disclosures in Topic 820, Fair Value Measurement, would be required for crypto-assets within the scope of this project. Those disclosures would be required in annual and interim periods.

Keywords: *Auditing program, Cryptocurrency, Procedures, Blockchain.*

Introduction

1. Cryptocurrency

A cryptocurrency is a class of digital currency that does not possess the legal status of currency or money, but can be accepted by natural and legal persons as a means of exchange and can be transferred, stored, and traded electronically, so it’s a digital representation of value, ordinarily issued and guaranteed directly by its developers or by algorithmic rules defined by its protocols. (ICAEW,2,2019)

And defined also by the World Bank Group WBG, as digital representations with their unified value, cryptocurrencies differ from electronic currencies that represent fiat currencies. (WBG, 2017, 3)

2. A proposed auditing program for Cryptocurrency

The researchers defined the Auditing program as a set of procedures represented in the audit scheme, which determine how the audit will be carried out. And establishing an effective audit program for entities with cryptocurrency transactions requires a good understanding of how cryptocurrencies work, understanding blockchain technology, identifying the main risks associated with cryptocurrency transactions, developing policies and procedures, implementing effective controls, training staff, and monitoring and evaluating the program.

As the researchers mentioned earlier, the audit program is a set of procedures represented in the audit scheme, which determines how the audit will be carried out, who will implement it, and what must be followed to do so. It is a set of instructions, which are followed by audit staff, for the proper implementation of the audit. It is to ensure that all cryptocurrency transactions are conducted within the entity in a compliant and secure manner and its scope includes all employees, contractors, and service providers from the three parties involved in cryptocurrency transactions on behalf of the entity.

However, before we get to know the procedures that are necessary to start the audit process, the auditor has two options, as mentioned (CPA, 2018, 3), as the auditors must be provided with examples of matters that must be considered when:

- Deciding whether to accept or reject the continuation of the audit engagement, if the institution is involved in cryptocurrency transactions.

- Identify and assess the risks of material misstatement in the financial statements related to cryptocurrency transactions and balances.

Risks are assessed by identifying the type of cryptocurrency, as cryptocurrencies (cryptocurrencies acquired for use and not for trading) associated with other economic claims (for example, gold-backed cryptocurrencies or stable coin offerings) may present different risks than those that are not. They have intrinsic value like utility tokens and native cryptocurrencies such as Bitcoin and others, and cryptocurrency-backed tokens may introduce additional complexity, as smart contract functions must also be considered, which will be discussed later. The position of any particular digital asset in the risk zone depends on several factors. The article raised some questions as follows:

1. Is Blockchain Widely Used?

2. Is it open source?

3. How many developers use it?

Also, auditors must consider whether the transactions were initiated manually or executed automatically via a smart contract. If it is automatic, there are risks of unauthorized or incorrect transactions associated with software flaws, hacking, and reliance on potentially inaccurate information provided to the Blockchain by third-party data feed services (known as oracles). These challenges are further complicated by the fact that it is more difficult for an auditor to verify the existence of cryptocurrencies compared to traditional assets.

The researchers refer to the following basic procedures, which are considered general and include all steps of the proposed audit program, which will be presented later in the research:

1. Technical Expertise: A cryptocurrency transaction auditing program requires specialized technical expertise that is not normally required for a normal entity. It includes a comprehensive understanding of various cryptocurrencies such as Bitcoin, Ethereum, and others, along with the underlying technology, cryptographic algorithms, and transaction structures. Familiarity with Blockchain technology, including decentralized ledgers, and smart contracts, is essential. Auditors should also have knowledge about cryptocurrency wallets and addresses and the ability to analyze information associated with them. Proficiency in the use of transaction analysis tools, awareness of cybersecurity risks, the various risks associated with cryptocurrency transactions, and an understanding of regulatory compliance requirements, such as AML and KYC regulations, are vital. Staying up-to-date with industry standards, best practices, and ongoing developments in audit guidelines for cryptocurrency transactions is critical for auditors to operate effectively in this dynamic field.

2. Technical procedures: which usually include all kinds of agreements, approvals, files, documents, evaluations, and verification of balances that the auditor must go through and verify in detail by the auditor, in addition to a letter relating to the audit process, as well as documenting policies and procedures related to auditing cryptocurrency transactions. This includes guidance on data acquisition, verification methods, compliance with regulations, and the use of specialized tools or software. The sampling method and rationale behind the selection should be documented. Also documenting results of the test, including any exceptions or hits. This is because this type of scrutiny includes certain authorizations by the administration related to trading and dealing in encrypted currencies, and for the seriousness of such transactions, it is necessary to focus and pay attention to the many documents, agreements, and evaluations used in classifying encrypted currencies.

3. Security Procedures: Given the increased vulnerability of cryptocurrency transactions to security breaches, an audit program for cryptocurrency transactions should prioritize robust security procedures. This entails implementing strict security procedures to protect against unauthorized access and mitigate risks. These procedures may include adopting multi-factor authentication methods to ensure that only authorized individuals

can access cryptocurrency wallets or transaction systems. In addition, the use of cold storage, which keeps private keys offline and inaccessible to potential hackers, can enhance the security of cryptocurrencies. Encryption techniques must be used to protect sensitive information, such as private keys and transaction data, both at rest and in transit. Regular security assessments, penetration testing, and vulnerability scanning can help identify and address potential system vulnerabilities. By focusing on these security procedures, auditors can enhance the integrity and protection of cryptocurrency transactions.

4. Compliance Requirements: Auditing cryptocurrency transactions require careful consideration of the unique regulatory landscape that governs these transactions. Cryptocurrency transactions are subject to distinct compliance requirements compared to traditional transactions. As part of the audit program, auditors must ensure that entities involved in cryptocurrency transactions comply with relevant regulations, such as Anti-Money Laundering (AML) laws and regulations. This may include evaluating the implementation of effective Know Your Client (KYC) procedures as well as being guided by International Auditing and Assurance Standards IAAS and International Financial Reporting Standards IFRS, by verifying the identity of the parties involved in transactions and ensuring compliance with transaction monitoring and reporting obligations. Auditors may need to evaluate an entity's policies and procedures to detect and mitigate potential money laundering risks associated with cryptocurrency transactions. Staying abreast of evolving regulatory frameworks for cryptocurrencies is vital to accurately assessing compliance and providing assurance to stakeholders. By meeting these compliance requirements, auditors contribute to maintaining the integrity and legality of cryptocurrency transactions.

5. Record Keeping: Auditing cryptocurrency transactions requires accurate record keeping due to the unique characteristics of these transactions. A cryptocurrency transaction audit program should include stricter record-keeping procedures to ensure thorough documentation. This includes obtaining and maintaining detailed information such as the date, time, amount, sender address, and recipient address for each transaction. In addition, auditors may need to record other relevant details, such as transaction fees, transaction IDs, and any associated memos or notes. Maintaining a clear and structured audit trail is essential to tracking the flow of cryptocurrencies and facilitating subsequent analysis and verification. Strong record-keeping not only supports the accuracy and completeness of the audit process, but also enables auditors to address any inconsistencies, anomalies, or potentially fraudulent activities that may arise during the examination. By emphasizing accurate record-keeping, auditors contribute to ensuring the transparency, accountability, and integrity of cryptocurrency transactions.

6. Risk Management: Given the unique risks associated with cryptocurrency transactions, an audit program for cryptocurrency transactions must include robust risk management procedures. Auditors should be aware of the growing potential for hacking, fraud, and theft inherent in the cryptocurrency ecosystem. To address these risks, auditors must develop and implement comprehensive risk management frameworks. This includes conducting comprehensive risk assessments to identify potential system vulnerabilities and threats. Auditors must also assess the effectiveness of existing controls and security measures implemented by the audited entity to mitigate these risks. In addition, auditors may recommend additional security measures such as secure key management, penetration testing, intrusion detection systems, and regular security audits. Continuous monitoring and evaluation of risk mitigation efforts are vital to ensuring the effectiveness of risk management procedures. By focusing on strong risk management, auditors contribute to enhancing the security, trustworthiness, and resilience of cryptocurrency transactions.

After presenting the previous procedures above, the researchers presented the following audit program:

No.	Audit Program	Auditor's name and signature	Worksheet number
1	**Procedures for managing cryptocurrency wallets:** • Secure storage: All cryptocurrency wallets must be stored securely using industry-standard security measures such as cold storage, hardware wallets, and multi-factor authentication MFA. • Access control: Access to cryptocurrency wallets must be limited to authorized personnel only. Access should be granted based on a need-to-know basis and according to job responsibilities. • Record keeping: All transactions involving cryptocurrency wallets must be recorded in a logbook, including the date, time, amount, sender, and recipient. • Regular reconciliation: Cryptocurrency wallets must be reconciled regularly to ensure that all transactions are accurately recorded and accounted for.		
2	**Procedures for processing cryptocurrency transactions:** • Authorization: All cryptocurrency transactions must be authorized by authorized personnel before they can be processed. The authorized personnel should verify the transaction for accuracy, authenticity, and compliance with company policies and external regulations. • Verification: All cryptocurrency transactions must be reviewed and verified for accuracy before they can be processed. Verification includes confirming the transaction details, ensuring that the sender has sufficient funds, and validating the recipient's wallet address. • Recording: All cryptocurrency transactions must be recorded in the company's accounting system. The record should include the transaction date, time, amount, sender, recipient, and any associated fees. • Reconciliation: Cryptocurrency transactions must be reconciled regularly to ensure that all transactions are accurately recorded and accounted for.		
3	**Procedures for managing cryptocurrency risks:** • Risk assessment: All potential risks associated with cryptocurrency transactions must be identified and assessed. This includes risks such as hacking, fraud, theft, and money laundering. • Controls implementation: Controls must be put in place to mitigate the identified risks. Examples of controls include multi-factor authentication, encryption, and regular security assessments. • Monitoring: The effectiveness of the controls must be monitored and evaluated on an ongoing basis. This includes regular security assessments, transaction monitoring, and employee training.		
4	**Procedures for ensuring compliance:** • Policy and procedure development: Policies and procedures must be developed to ensure compliance with internal policies and external laws and regulations. • Training and awareness: All employees involved in cryptocurrency transactions must be trained on the company's policies and procedures as well as relevant laws and regulations. • Compliance monitoring: All cryptocurrency transactions must be reviewed and verified to ensure compliance with internal policies and external laws and regulations. This includes regular audits and reviews of transaction logs.		

When the auditor prepares to start the audit process, the following detailed procedures must be taken into consideration:

No.	Detailed procedures followed by the auditor regarding each step	Auditor's name and signature	Worksheet number	Time taken to complete	Total Time
The general procedures followed by the auditor					
1. The Initial Work Management Procedures Stage:					
1	Understand the nature of the activity and type of entity dealing with cryptocurrencies and crypto by collecting information about the entity's business operations by management.				
2	Ensure that the administration has the necessary approvals (decision documents) to deal with cryptocurrencies.				
3	Verify the details of the administration's approvals, has a decision been made to buy or mine cryptocurrencies with the decision document for that?				
4	Exercising accuracy and utilizing various auditing procedures to detect potential management violations and irregularities, and addressing them.				
5	Performing intensive data analysis, conducting investigations, and relying on external sources to obtain corroborative evidence to verify the accuracy and completeness of reported encryption transactions.				
6	Evaluating the adequacy and effectiveness of internal controls and assessing the integrity and reliability of management declarations regarding cryptocurrencies.				
7	Establishing confidential agreements with the entity, its management, and relevant employees to ensure the protection of sensitive information related to the audit.				
8	Ensuring the handling of personal and sensitive information related to encryption transactions is in compliance with applicable data privacy laws and regulations.				
9	Evaluating data protection measures within the entity, including data encryption, access controls, and data retention policies.				
10	Verifying compliance with customer consent and privacy preferences when collecting and processing personal data.				
11	Evaluating the security protocols used for the transmission of encrypted data during the auditing process. This includes assessing encryption mechanisms, secure file transfer protocols, and secure communication channels used by the entity and its service providers.				

12	The auditor's understanding of regulatory requirements related to purchasing cryptocurrencies or cryptocurrency mining, including compliance with Anti-Money Laundering (AML) and Know Your Customer (KYC) regulations.				
13	Conducting training programs for the audit team before and during the auditing process.				
14	Requesting the documents and records that support the acquisition of cryptocurrencies, such as purchase agreements, transaction records, and wallet addresses.				
15	Ensuring that the entity's internal system allows for trading cryptocurrencies in case of cryptocurrency purchases.				
16	Verifying the authorization documents that empower the management to purchase cryptocurrencies.				
17	Verifying the authorization documents to ensure they include the relevant individuals' permissions to engage in cryptocurrency transactions.				
18	Verifying the presence of documents specifying the minimum and maximum purchase limits set by the management.				
19	Verifying the entity's ability to continue its operations in accordance with International Auditing Standard 570.				
20	Verifying that the financial manager is adequately funded with the required amounts to engage in cryptocurrency transactions.				
2. Processing Procedures Stage:					
21	Reviewing the processes of purchasing or mining cryptocurrencies, with particular emphasis on controls related to obtaining cryptocurrencies and maintenance.				
22	Auditing all cryptocurrency transactions and verifying their accuracy before processing them.				
23	Ensuring whether the cryptocurrencies are purchased for trading purposes or for holding them for more than a year.				
24	Verifying their proper recording in the financial, in case of a purchase for trading purposes statements.				
25	Verifying their proper recording in the financial statements, in case of purchase for holding them for more than a year.				
26	The reassessment is conducted by the International Accounting Standard (IAS) 38. In case of reassessment, the verification ensures that the evaluation process is objective, in case of a purchase for holding them for more than				

	a year.				
27	The auditor examines the regulatory requirements related to purchasing cryptocurrencies or cryptocurrency mining, including compliance with Anti-Money Laundering (AML) and Know Your Client (KYC) regulations.				
28	Verifying that the entity's internal system allows for cryptocurrency mining, in case of mining activities.				
29	Verifying that the entity provides the necessary hardware and equipment for cryptocurrency mining.				
30	Evaluating the entity's criteria for repair and maintenance of mining equipment by the guidance provided by IAAS (International Auditing and Assurance Standards).				
31	Verifying the security of the accounting system when it accepts transactions involving cryptocurrencies.				
32	Verifying the entity's infrastructure to ensure it allows for dealing with cryptocurrencies.				
33	Verifying the presence of a strong and effective internal control system that enables dealing with cryptocurrencies.				
3. Risk assessment and risk mitigation stage:					
34	Evaluating the inherent risks of transactions involving cryptocurrencies as outlined in the International Auditing Standard 315.				
35	Verifying the availability of the human resources (entity's employees) who are capable of dealing with cryptocurrencies.				
36	Ensuring the presence of specialized experts in technology and cryptocurrencies throughout the audit process by International Auditing Standard 620.				
37	Ensuring the protection of the system from potential breaches and intrusions.				
38	Verifying the availability of all the required records to confirm the transactions.				
39	Reviewing wallet security practices, including multi-factor authentication, cold storage, and key management procedures, to mitigate the risks of unauthorized access or loss of cryptocurrencies.				
40	Securing all cryptocurrency wallets properly using security measures compliant with industry standards.				
41	Verifying that access to cryptocurrency wallets is restricted to authorized individuals only.				
42	Ensuring that all transactions involving				

	cryptocurrency wallets are recorded in a dedicated ledger.				
43	Verifying that the dedicated ledger contains the date, time, amount, sender, and recipient for each transaction.				
44	Ensuring that all cryptocurrency transactions are approved by an authorized employee before being processed.				
45	Verifying any discrepancies or deviations identified during the settlement and testing process, considering their impact on the financial statements.				
46	Determining the applied method of depreciation for the cryptocurrencies used in cryptocurrency mining.				
47	When determining the depreciation method, consideration should be given to using either the declining balance method or the revaluation method based on its technological nature.				
48	Identifying and assessing all potential risks associated with cryptocurrency transactions.				
49	Identifying weaknesses and evaluating the effectiveness of security controls to protect cryptocurrencies and mining equipment.				
50	Assessing and reviewing cybersecurity measures to ensure the provision of appropriate financial statements.				
4. Compliance with international guidelines and standards stage:					
51	Reviewing IAAS guidelines to ensure that the audit engagement aligns with relevant auditing standards and ethical considerations for auditing cryptocurrency transactions.				
52	Evaluating the design and effectiveness of controls to mitigate risks associated with the recording, evaluation, and maintenance of mining equipment and cryptocurrencies, by Standard 315.				
53	Testing the operational effectiveness of controls through a sampling of testing and verification procedures, considering their impact on the acquisition of cryptocurrencies, depreciation, and maintenance standards.				
54	Verifying the existence and ownership of acquired cryptocurrencies, while ensuring compliance with the requirements of international financial reporting standards for recognition and measurement.				
55	Evaluating the appropriate classification and disclosure of cryptocurrencies and mining equipment, along with the				

	related requirements and any income or expenses associated with them.				
56	Conducting reconciliations between the entity's records and external sources to ensure the accuracy and completeness of cryptocurrency balances.				
57	Matching balances and transactions of cryptocurrencies with the financial statements and general ledger accounts, along with supporting documents, to ensure compliance with the requirements of international financial reporting standards for presentation and disclosure.				
58	Conducting a representative sample test of transactions, including acquisition, depreciation, maintenance, and revenue recognition, to ensure accuracy, validity, and compliance with the guidance of international financial reporting standards.				
59	Recording all cryptocurrency transactions in the company's accounting system.				
60	Reviewing the entity's financial statements to ensure recognition and measurement by principles and standards.				
61	Reviewing the entity's financial statements to ensure proper presentation and disclosure of cryptocurrencies and related mining activities by principles and standards.				
62	Documenting all audit procedures conducted, including scope, methodology, and findings, and ensuring compliance with IAAS requirements for documentation and report preparation.				
63	Conduct penetration testing on the software, if designed to be secure against hacking, to ensure its integrity and resistance to unauthorized access.				
64	Preparing the audit report for management, stakeholders, and regulatory authorities as required, following IAAS guidelines for communication and report preparation.				
65	Preparing a comprehensive audit report that highlights the audit findings, including any specific issues related to holdings, depreciation, maintenance, and financial statement presentation, following international guidelines.				

When auditing financial statements, cryptographic transactions are usually presented based on applicable accounting standards, such as International Financial Reporting Standards (IFRSs). The exact financial statement presentation will depend on the nature of crypto transactions and the purpose for which they are held. The researchers point out the following some common methods through which encryption transactions can be presented and highlighted in the financial statements:

1. Financial Position Statement:

A. Cryptocurrencies held as assets: Cryptocurrencies held for investment purposes or as current assets are usually reported as a separate item under “non-current assets” or “Current assets”, respectively on the right side of the financial position statement.

B. Liabilities related to cryptocurrencies: If an entity has any liabilities related to crypto transactions (for example, loans outstanding in cryptocurrencies), these are disclosed under “non-current liabilities” or “Current liabilities” respectively on the left side of the financial position statement.

2. Income Statement:

A. Cryptocurrency-related revenue: If an entity earns revenue from crypto-related activities (for example, mining bonuses, trading winnings), it will be reported as revenue under the appropriate income statement categories, such as “sales revenue” or “other income”.

B. Cryptocurrency-related expenses: Expenses incurred in connection with cryptocurrency transactions, such as transaction fees, mining costs, or security expenses, will be recognized as an expense on the income statement under the appropriate expense categories.

3. Cash Flows Statement:

Cryptocurrency-related cash flows: Cash flows arising from cryptocurrency transactions, such as purchases, sales, or cryptocurrency transfers, will be disclosed in the cash flows statement. These are usually classified as operating, investing, or financing activities, depending on the nature of the transaction.

4. Notes to the financial statements:

A. Disclosure of Crypto Holdings: An entity may provide additional information in the notes to the financial statements, disclosing details about the types of cryptocurrencies held, their book value, valuation methods, and any significant limitations or risks associated with their ownership.

B. Accounting policies: An entity will disclose its accounting policies for cryptocurrencies, including the applicable recognition, measurement, and derecognition principles.

It is important to note that specific presentation and disclosure requirements may vary based on the entity's circumstances, accounting standards, and industry practices. It is advised to refer to relevant accounting standards, such as IFRS 9 Financial Instruments, and seek guidance from accounting professionals to ensure accurate and consistent presentation of cryptographic transactions in financial statements.

3. Statistical Analysis

To find out the opinions of the researched sample about the suggested program (The general procedures followed by the auditor), a questionnaire was designed representing four stages and 65 procedures and distributed to a random sample that included 230 accountants, of which 210 were retrieved, and 198 of them were valid for analysis. The analysis was done using the statistical program (SPSS-27) and EasyFit-5.5.

3.1. Statistical description of general information:

The general information of the research is summarized in Table 1.

Table 1. The statistical description of general information

General Information	Frequency	Percent
1. Qualification:		
Ph.D.	87	43.9%
Master	57	28.8%
Higher Diploma	6	3%
Bachelor	33	16.7%
Chartered Accountant / or equivalent	15	7.6%
Other	0	0%
2. Field of work:		
Academic	105	53%
Professional	93	47%
3. Job title or scientific title:		
Professor	16	8.1%
Assistant Professor	42	21.2%
Lecturer	32	16.2%
Assistant Lecturer	30	15.2%
Certified Public Accountant	9	4.5%
Auditor	6	3%
Account Manager	9	4.5%
Assistant Auditor	6	3%
Other	48	24.2%
4. Years of experience in professional or academic work:		
5 years or less	21	10.6%
(6-10) years	54	27.3%
(11-15) years	33	16.7%
(16-20) years	39	19.7%
20 years and over	51	25.8%
Total	198	100%

Table (1) shows that the study sample included four general information, qualifications distributed among 43.9% of Ph.D., 28.8% of Master, 3% of Higher Diploma, 16.7% of Bachelor, and 7.6% of Chartered Accountant / or equivalent. Field of work, 53% of Academic, and 47% of Professional. Job title or scientific title, 8.1% of Professor, 21.2% of Assistant Professor, 16.2% of Lecturer, 15.2% of Assistant Lecturer, 4.5% of Certified Public Accountant, 3% of Auditor, 4.5% of Account Manager, 3% of Assistant Auditor, and 24.2% of Other. Years of experience in professional or academic work, 10.6% of (5 years or less), 27.3% of (6-10) years, 16.7% of (11-15) years, 19.7% of (16-20) years, and 25.8% of (20 years and over).

3.2. Description and diagnosis of program stages:

In this analysis, the mean, standard deviation, and degree of agreement with the program stages will be calculated, which included (65) items segmented into three stages. the arithmetic means for every item from the questionnaire evaluated by the Likert scale (Totally not agree = 1, Not agree = 2, Not sure = 3, Agreed = 4, and totally agree =5), it is summarized as follows:

First Stage: The Initial Work Management Procedures Stage includes 20 steps; it is summarized in the following table:

Table 2. Descriptive Statistics for the first stage

No. Item	Item	Mean	Std. Deviation	Percent
q1	Understand the nature of the activity and type of entity dealing with cryptocurrencies and crypto by collecting information about the entity's business operations by management.	4.3939	.60149	87.88
q2	Ensure that the administration has the necessary approvals (decision documents) to deal with cryptocurrencies.	4.4242	.65440	88.48
q3	Verify the details of the administration's approvals, has a decision been made to buy or mine cryptocurrencies with the decision document for that?	4.3636	.66767	87.27
q4	Exercising accuracy and utilizing various auditing procedures to detect potential management violations and irregularities, and addressing them.	4.4242	.72084	88.48
q5	Performing intensive data analysis, conducting investigations, and relying on external sources to obtain corroborative evidence to verify the accuracy and completeness of reported encryption transactions.	4.2879	.79526	85.76
q6	Evaluating the adequacy and effectiveness of internal controls and assessing the integrity and reliability of management declarations regarding cryptocurrencies.	4.2879	.67060	85.76
q7	Establishing confidential agreements with the entity, its management, and relevant employees to ensure the protection of sensitive information related to the audit.	4.0152	.86369	80.30
q8	Ensuring the handling of personal and sensitive information related to encryption transactions complies with applicable data privacy laws and regulations.	4.2121	.66490	84.24
q9	Evaluating data protection measures within the entity, including data encryption, access controls, and data retention policies.	4.2121	.77095	84.24
q10	Verifying compliance with customer consent and privacy preferences when collecting and processing personal data.	4.1970	.78475	83.94
q11	Evaluating the security protocols used for the transmission of encrypted data during the auditing process. This includes assessing encryption mechanisms, secure file transfer protocols, and secure communication channels used by the entity and its service providers.	4.3030	.69741	86.06

q12	The auditor's understanding of regulatory requirements related to purchasing cryptocurrencies or cryptocurrency mining, including compliance with Anti-Money Laundering (AML) and Know Your Customer (KYC) regulations.	4.2273	.85131	84.55
q13	Conducting training programs for the audit team before and during the auditing process.	4.3485	.68691	86.97
q14	Requesting the documents and records that support the acquisition of cryptocurrencies, such as purchase agreements, transaction records, and wallet addresses.	4.2879	.71457	85.76
q15	Ensuring that the entity's internal system allows for trading cryptocurrencies in case of cryptocurrency purchases.	4.2727	.68809	85.45
q16	Verifying the authorization documents that empower the management to purchase cryptocurrencies.	4.3485	.61683	86.97
q17	Verifying the authorization documents to ensure they include the relevant individuals' permissions to engage in cryptocurrency transactions.	4.2727	.61814	85.45
q18	Verifying the presence of documents specifying the minimum and maximum purchase limits set by the management.	4.1364	.71715	82.73
q19	Verifying the entity's ability to continue its operations by International Auditing Standard 570.	4.1212	.66490	82.42
q20	Verifying that the financial manager is adequately funded with the required amounts to engage in cryptocurrency transactions.	4.2121	.77095	84.24
Average		**4.2674**	**.71100**	**85.35**

Table 2. shows that the research sample agreed with the steps of the first stage, with a mean agreement greater than (4), and an agreement percentage of more than 80%, while the standard deviation values were limited indicating the convergence of the researched sample opinions and their lack of dispersion about the steps of the first stage (The Initial Work Management Procedures) for the suggested program.

Second Stage: The processing procedures stage includes 13 steps; it is summarized in the following table:

Table 3. Descriptive Statistics for the second stage

No. Item	Item	Mean	Std. Deviation	Percent
q1	Reviewing the processes of purchasing or mining cryptocurrencies, with particular emphasis on controls related to obtaining cryptocurrencies and maintenance.	4.3485	.61683	86.97
q2	Auditing all cryptocurrency transactions and verifying their accuracy before processing them.	4.1515	.65862	83.03

q3	Ensuring whether the cryptocurrencies are purchased for trading purposes or for holding them for more than a year.	4.1970	.70285	83.94
q4	Verifying their proper recording in the financial, in case of a purchase for trading purposes statements.	4.3788	.67060	87.58
q5	Verifying their proper recording in the financial statements, in case of purchase for holding them for more than a year.	4.2727	.61814	85.45
q6	The reassessment is conducted by the International Accounting Standard (IAS) 38. In case of reassessment, the verification ensures that the evaluation process is objective, in case of a purchase for holding them for more than a year.	4.0455	.68557	80.91
q7	The auditor examines the regulatory requirements related to purchasing cryptocurrencies or cryptocurrency mining, including compliance with Anti-Money Laundering (AML) and Know Your Client (KYC) regulations.	4.3182	.55625	86.36
q8	Verifying that the entity's internal system allows for cryptocurrency mining, in case of mining activities.	4.3030	.62850	86.06
q9	Verifying that the entity provides the necessary hardware and equipment for cryptocurrency mining.	4.2727	.68809	85.45
q10	Evaluating the entity's criteria for repair and maintenance of mining equipment by the guidance provided by IAAS (International Auditing and Assurance Standards).	4.1364	.62648	82.73
q11	Verifying the security of the accounting system when it accepts transactions involving cryptocurrencies.	4.2424	.60608	84.85
q12	Verifying the entity's infrastructure to ensure it allows for dealing with cryptocurrencies.	4.3182	.55625	86.36
q13	Verifying the presence of a strong and effective internal control system that enables dealing with cryptocurrencies.	4.3333	.70531	86.67
Average		**4.2552**	**.64000**	**85.10**

Table 3. shows that the research sample agreed with the steps of the second stage, with a mean agreement greater than (4), and an agreement percentage of more than 80%, while the standard deviation values were limited indicating the convergence of the researched sample opinions and their lack of dispersion about the steps of the second stage (Processing Procedures Stage) for the suggested program.

Third Stage: The risk assessment and risk mitigation stage include 17 steps; it is summarized in the following table:

Table 4. Descriptive Statistics for the third stage

No. Item	Item	Mean	Std. Deviation	Percent
q1	Evaluating the inherent risks of transactions involving cryptocurrencies as outlined in the International Auditing Standard 315.	4.3182	.65669	86.36
q2	Verifying the availability of the human resources (entity's employees) who are capable of dealing with cryptocurrencies.	4.3030	.62850	86.06
q3	Ensuring the presence of specialized experts in technology and cryptocurrencies throughout the audit process in accordance with International Auditing Standard 620.	4.2727	.73101	85.45
q4	Ensuring the protection of the system from potential breaches and intrusions.	4.3939	.57562	87.88
q5	Verifying the availability of all the required records to confirm the transactions.	4.3788	.71457	87.58
q6	Reviewing wallet security practices, including multi-factor authentication, cold storage, and key management procedures, to mitigate the risks of unauthorized access or loss of cryptocurrencies.	4.1818	.71763	83.64
q7	Securing all cryptocurrency wallets properly using security measures compliant with industry standards.	4.2424	.63070	84.85
q8	Verifying that access to cryptocurrency wallets is restricted to authorized individuals only.	4.3333	.61289	86.67
q9	Ensuring that all transactions involving cryptocurrency wallets are recorded in a dedicated ledger.	4.2727	.73101	85.45
q10	Verifying that the dedicated ledger contains the date, time, amount, sender, and recipient for each transaction.	4.4697	.55791	89.39
q11	Ensuring that all cryptocurrency transactions are approved by an authorized employee before being processed.	4.3939	.54852	87.88
q12	Verifying any discrepancies or deviations identified during the settlement and testing process, considering their impact on the financial statements.	4.2727	.66559	85.45
q13	Determining the applied method of depreciation for the cryptocurrencies used in cryptocurrency mining.	4.1515	.89401	83.03
q14	When determining the depreciation method, consideration should be given to using either the declining balance method or the revaluation method based on its technological nature.	4.1364	.88793	82.73
q15	Identifying and assessing all potential risks associated with cryptocurrency transactions.	4.2727	.75156	85.45
q16	Identifying weaknesses and evaluating the effectiveness of security controls to protect cryptocurrencies and mining equipment.	4.3788	.69293	87.58

q17	Assessing and reviewing cybersecurity measures to ensure the provision of appropriate financial statements.	4.4394	.65599	88.79
Average		**4.3066**	**.6855**	**86.13**

Table 4. shows that the research sample agreed with the steps of the third stage, with a mean agreement greater than (4), and an agreement percentage of more than 80%, while the standard deviation values were limited indicating the convergence of the researched sample opinions and their lack of dispersion about the steps of the second stage (risk assessment and risk mitigation) for the suggested program.

Fourth Stage: The risk assessment and risk mitigation stage include 15 steps; it is summarized in the following table:

Table 5. Descriptive Statistics for the fourth stage

No. Item	Item	Mean	Std. Deviation	Percent
q1	Reviewing IAAS guidelines to ensure that the audit engagement aligns with relevant auditing standards and ethical considerations for auditing cryptocurrency transactions.	4.3636	.59532	87.27
q2	Evaluating the design and effectiveness of controls to mitigate risks associated with the recording, evaluation, and maintenance of mining equipment and cryptocurrencies, in accordance with Standard 315.	4.3182	.63308	86.36
q3	Testing the operational effectiveness of controls through sampling of testing and verification procedures, considering their impact on the acquisition of cryptocurrencies, depreciation, and maintenance standards.	4.2121	.70922	84.24
q4	Verifying the existence and ownership of acquired cryptocurrencies, while ensuring compliance with the requirements of international financial reporting standards for recognition and measurement.	4.2576	.66019	85.15
q5	Evaluating the appropriate classification and disclosure of cryptocurrencies and mining equipment, along with the related requirements and any income or expenses associated with them.	4.1212	.77095	82.42
q6	Conducting reconciliations between the entity's records and external sources to ensure accuracy and completeness of cryptocurrency balances.	4.3182	.72292	86.36
q7	Matching balances and transactions of cryptocurrencies with the financial statements and general ledger accounts, along with supporting documents, to ensure compliance with the requirements of international financial reporting standards for presentation and disclosure.	4.4091	.55125	88.18

q8	Conducting a representative sample test of transactions, including acquisition, depreciation, maintenance, and revenue recognition, to ensure accuracy, validity, and compliance with the guidance of international financial reporting standards.	4.2576	.78651	85.15
q9	Recording all cryptocurrency transactions in the company's accounting system.	4.3333	.70531	86.67
q10	Reviewing the entity's financial statements to ensure recognition and measurement in accordance with principles and standards.	4.3182	.63308	86.36
q11	Reviewing the entity's financial statements to ensure proper presentation and disclosure of cryptocurrencies and related mining activities in accordance with principles and standards.	4.2879	.64749	85.76
q12	Documenting all audit procedures conducted, including scope, methodology, and findings, and ensuring compliance with IAAS requirements for documentation and report preparation.	4.3485	.61683	86.97
q13	Conduct penetration testing on the software, if designed to be secure against hacking, to ensure its integrity and resistance to unauthorized access.	4.2879	.64749	85.76
q14	Preparing the audit report for management, stakeholders, and regulatory authorities as required, following IAAS guidelines for communication and report preparation.	4.3636	.59532	87.27
q15	Preparing a comprehensive audit report that highlights the audit findings, including any specific issues related to holdings, depreciation, maintenance, and financial statement presentation, following international guidelines.	4.3636	.59532	87.27
Average		**4.3040**	**.65800**	**86.08**

Table 5. shows that the research sample agreed with the steps of the third stage, with a mean agreement greater than (4), and an agreement percentage of more than 80%, while the standard deviation values were limited indicating the convergence of the researched sample opinions and their lack of dispersion about the steps of the second stage (Compliance with international guidelines and standards stage) for the suggested program. The average and percentage agreement for the four stages and the program as a whole are summarized in Table 6.

Table 6. Descriptive Statistics for the stages program

Stage		**Mean**	**Std. Deviation**	**Percent**
1	The Initial Work Management Procedures Stage	4.2674	.71100	85.35
2	Processing Procedures Stage	4.2552	.64000	85.10
3	Risk assessment and risk mitigation stage	4.3066	.6855	86.13
4	Compliance with international guidelines and standards stage	4.3040	.65800	86.08
Average	The general procedures followed by the auditor	4.2833	.67360	85.67

The average agreement with the suggested program (The general procedures followed by the auditor) was (4.2833), which is greater than the Likert average (3), at a percentage of 85.67%. The average agreement with the first stage (The Initial Work Management Procedures Stage) was (4.2674), which is greater than the Likert average (3), at a percentage of 85.35%. The average agreement with the second stage (Processing Procedures Stage) was (4.2552), which is greater than the Likert average (3), at a percentage of 85.10%. The average agreement with the third stage (Risk assessment and risk mitigation stage) was (4.3066), which is greater than the Likert average (3), at a percentage of 86.13%. The average agreement with the fourth stage (Compliance with international guidelines and standards stage) was (4.3040), which is greater than the Likert average (3), at a percentage of 86.08%.

3.3. Test reliability coefficient and Validity of the questionnaire (consistency):

Reliability, simply put, a reliable measuring instrument is one which gives you the same measurements when you repeatedly measure the same unchanged objects or events. Also note that I can never know what the reliability of an instrument (a test) is, because I cannot know what the true scores are. I can, however, estimate reliability. Cronbach’s alpha is a measure of internal consistency, that is, how closely related a set of items are as a group. It is considered to be a measure of scale reliability. A “high” value for alpha does not imply that the measure is unidimensional. If, in addition to measuring internal consistency, you wish to provide evidence that the scale in question is unidimensional, additional analyses can be performed. Exploratory factor analysis is one method of checking dimensionality. Technically speaking, Cronbach’s alpha is not a statistical test – it is a coefficient of reliability (or consistency). On this basis, it will be used Cronbach's alpha coefficient.

On the other hand, Content Validity assumes that we can detail the entire population of behavior (or other things) that operationalization is supposed to capture. Now consider our operationalization to be a sample taken from that population. Our operationalization will have content validity to the extent that the sample is representative of the population. To measure content validity, we can do our best to describe the population of interest and then ask experts (people who should know about the construct of interest) to judge how well representative our sample is of that population. To measure the consistency with sincerity (which represents the root of the reliability coefficient) questionnaire and summarized in Table (7).

Table (7): Reliability Statistics

Stages	Cronbach's Alpha	Validity	N of Items
First	0.936	0.967	20
Second	0.884	0.940	13
Third	0.917	0.958	17
Fourth	0.935	0.967	15
All stages	0.970	0.985	65

Table (7) shows that the reliability statistics, for Cronbach alpha values are (0.936, 0.884, 0.917, 0.935, and 0.970) and the validity values are (0.967, 0.940, 0.958, 0.967, and 0.985), and they are all greater than 0.60 and 0.80 respectively and it reflects the high reliability of the measuring instrument. Moreover, it indicates a high level of internal consistency with respect to the specified sample.

3.4. Test data distribution:

Here will test questionnaire data and whether the means have a normal distribution or not through the use of a Kolmogorov-Smirnov (K. S.) and Anderson-Darling (A. D.) test (by using the Easy Fit program) which determines the tool and the appropriate test to test the study hypotheses, test the following hypotheses (Ali et al 2023):

H_0 : The means of the questionnaire data have a normal distribution.

H_1 : The means of the questionnaire data have non-normal distribution.

The test results are summarized under the significance level (0.05) in the following table:

Table (8): Test of Normality

Stages	K.S.			A. D.		Result
	Statistic	p Value	Critical Value	Statistic	Critical Value	
All stages	0.0705	0.266	0.0965	0.8669	2.5018	Normal

Table (8) shows the suggested program by using (K.S.) test, the means of the suggested program have normal distribution since the p-value is equal to (0.266) and greater than the significance level (0.05), and the test statistic (0.0705) is less than (0.0965). By using the (A. D.) test, the means of the suggested program have normal distribution since the test statistic (0.8669) is less than (2.5018).

3.5. Study hypotheses test:

The study hypothesis is tested on the extent of the sample's agreement about the suggested program and its four stages, and the possibility of generalizing questionnaire results to the population as a whole. On this basis, the following hypotheses were tested:

The main hypothesis: There is agreement about the suggested program (The general procedures followed by the auditor)

First sub-hypothesis: There is agreement about the first stage (The Initial Work Management Procedures Stage)

Second sub-hypothesis: There is agreement about the second stage (Processing Procedures Stage)

Third sub-hypothesis: There is agreement about the third stage (Risk assessment and risk mitigation stage)

Fourth sub-hypothesis: There is agreement about the fourth stage (Compliance with international guidelines and standards stage)

Testing whether there is an agreement with the suggested program and its four stages, was done by calculating the means to the questionnaire items which were answered by the (198) respondents according to the Likert scale depending on the extent of their agreement with the hypothesis of the study and specifically test the average equal to the (3) for the respondents (because the average of Likert equal to 3) against the average is greater than the number (3). Because the data have a normal distribution (Ali 2022), a one-sample t-test was used under the level of significance (0.05). The results are summarized in Table (9):

Table (9): One-Sample Test for the Study Hypotheses

Average test value = 3							
Hypothesis	Mean	Mean Difference	Std. Error Mean	t-calculated	t-tabulated	p-value	Result
Mian	4.2837	1.2837	0.02841	45.180	1.96	0.000	Sig.
First	4.2674	1.2674	0.03408	37.188	1.96	0.000	Sig.
Second	4.2552	1.2552	0.02950	42.550	1.96	0.000	Sig.
Third	4.3066	1.3066	0.03226	40.499	1.96	0.000	Sig.
Forth	4.3040	1.3040	0.03400	38.352	1.96	0.000	Sig.

Table (9) shows that the agreement mean with the hypotheses are (4.2837, 4.2674, 4.2552, 4.3066, and 4.3040 respectively), which is greater than the hypothetical Likert mean (3) by (1.2837, 1.2674, 1.2552, 1.3066, and 1.3040 respectively). While the t-calculated values were (45.180, 37.188, 42.550, 40.499, and 38.352) which is greater than the t-tabulated value (1.96), and the p-values are equal to (0.000) which is less than the significance level (0.05), therefore, the null hypothesis is rejected and accept the alternative hypothesis (Ali and Jwana 2022) which states that “There is agreement about the suggested program and its four stages” According to the opinions of the researched sample, which has been tested and the possibility of generalizing its results to the population as a whole.

References

A. Official documents:

1. Ali, Taha Hussein and Jwana Rostam Qadir. "Using Wavelet Shrinkage in the Cox Proportional Hazards Regression model (simulation study)", Iraqi Journal of Statistical Sciences, 19, 1, 2022, 17-29.
2. Ali, Taha Hussein. "Modification of the adaptive Nadaraya-Watson kernel method for nonparametric regression (simulation study)." Communications in Statistics-Simulation and Computation 51.2 (2022): 391-403.
3. Ali, Taha Hussein, Nasradeen Haj Salih Albarwari, and Diyar Lazgeen Ramadhan. "Using the hybrid proposed method for Quantile Regression and Multivariate Wavelet in estimating the linear model parameters." Iraqi Journal of Statistical Sciences 20.1 (2023): 9-24.
4. ICAEW, “CRYPTO-ASSETS: ANTI-MONEY LAUNDERING GUIDANCE FOR ACCOUNTANTS”, London (2019).

B. Books

1. CPA, 2018, “Audit Considerations Related to Cryptocurrency Assets and Transactions”.
2. WBG, 2017, “Distributed Ledger Technology (DLT) and Blockchain”.

C. Websites & Internet

1. ey.com

https://www.ey.com/en_us/blockchain-platforms/explorer-visualizer

2. ey.com

https://www.ey.com/en_iq/assurance/how-to-audit-the-next-generation-of-digital-assets

3. Icaew.com

https://www.icaew.com/insights/viewpoints-on-the-news/2022/sept-2022/how-do-we-audit-cryptocurrency

4. Journalofaccountancy.com

https://www.journalofaccountancy.com/news/2022/dec/fasb-set-draft, crypto asset-disclosure-standard.html