Hong Kong Institute of
Certified Public Accountants
香港會計師公會

HKICPA Audit Guide: Digital Assets

Introduction

Auditing digital assets presents challenges distinct from traditional audits, particularly in relation to the rights and obligations, completeness and valuation of digital assets balances and transactions. Regulators and professional bodies have consistently emphasized that these engagements carry heightened risks arising from the complexity of the underlying technology, custody arrangements, valuation methodologies, fraud susceptibility, and an evolving regulatory landscape. In particular, two upfront audit challenges warrant focused attention:

- Establishing **rights and obligations** is rarely straightforward. Control of a digital wallet or private key does not, by itself, constitute legal or beneficial ownership. A clear distinction must be made between enforceable legal rights and mere technical access.
- The **reliability of audit evidence** obtained from blockchain explorers, third-party intermediaries (e.g., exchanges, custodians, and pricing vendors), and entity-generated reports should be specifically evaluated.

These challenges are compounded by the absence of internationally accepted digital asset–specific auditing and accounting standards. As a result, auditors must design and perform sufficient appropriate audit procedures tailored to entity-specific circumstances, exercise professional judgment and skepticism, and, where appropriate, seek input from relevant experts.

Purpose and Scope

Purpose. This non-authoritative guide assists auditors in identifying and addressing common issues in audits of entities engaged in digital asset activities, including cryptocurrencies, stablecoins and security tokens. It synthesizes regulatory inspection findings across jurisdictions, guidance from regulatory and professional bodies and emerging audit practices into structured, phase-by-phase guidance — from client acceptance and continuance through to completion and reporting.

Scope. The guide focuses on considerations for audits of general purpose financial statements conducted under the Hong Kong Standards on Auditing (HKSAs). The concepts and principles may also be broadly relevant to other digital asset related assurance engagements, such as reserve attestations or specialized regulatory reporting. Where appropriate, auditors should adapt the considerations in this guide to the specific context and requirements of the engagement.

This guide reflects the digital asset regulatory, accounting and auditing landscape in Hong Kong as at the date of issuance. Given the rapidly evolving nature of this area, auditors should consider any subsequent legislative, regulatory, accounting and auditing developments and exercise professional judgment in applying this guide. This guide is intended as a high-level general reference rather than a detailed audit methodology or step-by-step manual. It is not a

substitute for firm-specific audit methodologies, tailored specialist input, or exercise of professional judgment and skepticism.

Hong Kong Landscape

Hong Kong has rapidly emerged as a hub for digital asset activities. The regulatory landscape is evolving rapidly, with significant developments including the licensing regimes for stablecoin issuers[1] and virtual asset trading platforms (VATP).[2]

Auditors should remain alert to regulatory developments relevant to digital assets throughout the engagement. In particular, an entity's licensing status, safeguarding and client-asset segregation obligations, reserve requirements, and ongoing compliance with applicable regulatory requirements may affect:

- the legality of the entity's operations and its ability to continue as a going concern, including the implications of any licence conditions, restrictions or enforcement actions;
- the auditor's identification and assessment of risks of material misstatement, including risks of fraud and non-compliance with laws and regulations (NOCLAR);
- the recognition, measurement and classification of digital assets and related liabilities (e.g., obligations owed to clients); and
- the sufficiency and appropriateness of financial statements disclosures, including those concerning regulatory uncertainty, restrictions on operations and significant judgments.

How This Guide Is Organized

This guide is organized around the four phases of an audit engagement. For each phase, it highlights common audit issues (non-exhaustive), sets out recommended responses, and cross-references relevant Hong Kong Standards on Quality Management (HKSQMs) and HKSAs. The table below summarizes the key themes addressed in each phase.

> 💡 ***Important Note on Cross-Cutting Themes***
>
> Certain audit themes are cross-cutting and recur throughout all phases of the engagement rather than arising in isolation. In particular, auditors should continuously revisit and re-evaluate:
>
> - **Rights and obligations** — distinguish mere technical access to private key from enforceable legal or beneficial ownership.

---

[1] Effective 1 August 2025, a licence from the Hong Kong Monetary Authority (HKMA) is required for any person who issues a specified stablecoin (within the meaning of the Stablecoins Ordinance) in Hong Kong in the course of business; issues a specified stablecoin that purports to maintain a stable value with reference to Hong Kong dollars in or outside Hong Kong; or actively markets its issuance of specified stablecoins to the public of Hong Kong.

[2] Effective 1 June 2023, centralized virtual asset trading platforms that carry on business in Hong Kong, or actively market their services to Hong Kong investors, are required to be licensed and regulated by the Securities and Futures Commission (SFC).

- **Completeness** — identify the full population of on-chain and off-chain activities, including wallets, exchange accounts, sub-ledgers, smart contracts, staking validators and decentralized finance (DeFi) positions.
- **Pseudonymity** — remain alert to the pseudonymous nature of blockchain transactions and its implications for NOCLAR and undisclosed related parties.
- **Reliability of evidence** — evaluate the relevance and reliability of information used as audit evidence, particularly data sourced from blockchain explorers, third-party intermediaries and complex IT environments.
- **Involvement of experts** — assess the need for, and the adequacy of work performed by, specialists.

🎯 1. Client Acceptance & Continuance	🔍 2. Planning & Risk Assessment
• Ensure the engagement team possesses sufficient and appropriate expertise in digital assets and related technology, including in relation to the specific digital asset business models involved (e.g., custody, staking, client asset safeguarding, platform operations) and determining whether the involvement of experts is necessary. • Assess management's integrity, governance and competence. • Evaluate the risks of NOCLAR, fraud, beneficial ownership, related parties and regulatory perimeter risks (e.g., operating unlicensed regulated activities). *→ Issues #1–2*	• Understand the entity's digital asset activities, including transaction flows, custody arrangements, IT systems and regulatory environment. This understanding should extend beyond wallets and on-chain transactions to include exchange accounts, custodial sub-accounts, internal ledgers, smart contracts, staking and DeFi positions, and other off-chain arrangements to ensure that all digital asset related activities and balances are completely identified. • Identify and evaluate digital asset-specific risks, including fraud risks, risks of non-compliance with laws and regulations (NOCLAR), and other significant risks. This should include consideration of risks arising from omnibus arrangements, delegated authority, governance changes and pseudonymous related-party exposure. • Evaluate the entity's accounting policies, valuation methods, and internal controls including general IT controls (GITCs). *→ Issues #3–6*

⚖️ 3. Responding to Assessed Risks	✅ 4. Completion & Reporting
• Private key access ≠ ownership. Auditors should clearly distinguish among access, control, legal ownership, beneficial ownership, custody arrangements and safeguarding obligations, and test key lifecycle controls and supplement with substantive procedures. • Corroborate on-chain balances and transactions independently; test off-chain balances and transactions; assess fair value, impairment, and revenue recognition. • Note the use of smart contracts where 'internal transactions' (transactions that occur between smart contracts) may arise and need to be identified. • Evaluate third-party and entity's internal information before using them as audit evidence. → ***Issues #7–13***	• Ensure sufficient and appropriate disclosures that enable users to understand the entity's digital asset risks and financial impacts, including its custody model and client-asset exposure, concentration and liquidity risks, transfer restrictions, regulatory uncertainties and significant valuation judgments. → ***Issues #14–15***

This guide is not intended to be exhaustive. It does not replace the auditor's responsibility to exercise professional judgment, apply the requirements of the HKSAs, or consider the specific facts and circumstances of each engagement. Auditors should remain alert to evolving risks, regulatory developments and emerging practices in this rapidly changing area, and should supplement this guide with other relevant standards, guidance and firm policies as appropriate.

This guide was prepared by the staff of the Hong Kong Institute of Certified Public Accountants (HKICPA or the Institute) and approved by the Institute's Auditing and Assurance Standards Committee (AASC) for general reference only. It does not necessarily reflect the views of the Institute, the Council or any of its committees. The Institute, AASC and the Institute's staff do not accept any responsibility or liability, and disclaim all responsibility and liability, in respect of this guide and any consequences that may arise from any person acting or refraining from action as a result of any materials in this guide.

🎯 Phase 1: Client Acceptance & Continuance

#	Common Audit Issue	Description of Issue	Recommended Audit Response
1	**Lack of Competence, Skills, or Resources**	• Accepting or continuing audits of entities with digital asset activities without sufficient expertise in digital assets, blockchain technology and cryptography.. The specialized and evolving nature of digital assets requires specific expertise. Engagement quality reviewers likewise require an appropriate level of knowledge. Without such expertise, engagement teams cannot effectively identify, assess and respond to digital asset related risks of material misstatement in financial reporting. • Not adequately considering the nature of the digital assets held or transacted, and whether sufficient appropriate audit evidence can be obtained, including: – the availability and reliability of audit tools and techniques (e.g., blockchain explorers, on-chain analytics) to address key assertions such as existence, rights and obligations, completeness and valuation; – the availability of relevant assurance reports (e.g., Service Organization Controls (SOC) reports) to provide audit evidence on the operating	• Ensure the engagement team collectively has the necessary competence in digital assets and the related technologies (e.g., blockchain, cryptography, distributed ledger technology). If needed, engage IT or technical accounting specialists. *(HKSQM 1 para. 32(b)–(d), HKSA 220 (Revised) para. 26; HKSA 620 para. 7)* • Assess whether the firm's quality management system addresses digital asset engagements, including competence, acceptance and continuance, consultation and oversight. *(HKSQM 1 paras. 10, 27)* • Determine whether an engagement quality reviewer is needed and whether suitably qualified reviewers are available. *(HKSQM 1 para. 34(f); HKSA 220 (Revised) para. 36)* • Evaluate compliance with relevant ethical and independence requirements at the firm, network firm and audit team levels, including identifying and evaluating threats to independence in relation to the entity, and addressing the threats by eliminating or reducing them to an acceptable level. *(HKSQM 1 para. 29; HKSA 220 (Revised) paras. 16–21)* *Note: The Code of Ethics for Professional Accountants (Code) does not prescribe independence requirements specific to entities engaged in digital asset activities. Auditors should apply the Code's conceptual framework, together with professional judgment, to identify, evaluate and address threats to independence when undertaking audits of such entities. The classification of a digital asset (e.g., as a security, asset, utility or payment token) involves significant judgment and may have differing implications for the firm's independence assessment. Further independence*

#	Common Audit Issue	Description of Issue	Recommended Audit Response
		effectiveness of complementary user entity controls; and – the involvement of other third-party service providers, particularly custodians and others to whom the entity may outsource aspects of its digital asset activity, and the availability of sufficient appropriate audit evidence over the services they provide. • Inadequate understanding and evaluation of the laws and regulations applicable to the entity's digital asset activities, including whether such activities require licensing and whether the entity is appropriately regulated (e.g., licensed under the SFC's VATP regime, the HKMA's stablecoin issuer regime, or other overseas regimes and requirements). The regulatory landscape for digital assets is evolving and has a direct impact on the entity's permitted activities, compliance obligations, safeguarding requirements and the recognition, measurement, presentation and disclosure in the financial statements.	*considerations may also arise in relation to custodians, exchanges and other service organizations involved in the entity's digital asset activities. Firms are encouraged to establish internal policies and procedures to promote consistency across such engagements and to ensure that any threats to compliance with ethical and independence requirements are reduced to an acceptable level.* • Evaluate whether the preconditions for the audit are present, including whether sufficient appropriate audit evidence is expected to be available, particularly in respect of the key assertions relevant to digital assets, and whether audit tools and techniques and relevant assurance reports are available and appropriate for the purposes of the audit. *(HKSA 210 para. 6; HKSA 220 (Revised) para. 22)* • Obtain an understanding of the legal and regulatory framework applicable to the entity and its digital asset activities, and the entity's compliance with that framework (e.g., licensing requirements and ongoing obligations), and assess the implications for the audit, focusing on laws and regulations that may give rise to risks of material misstatement in the financial statements. This includes understanding whether the entity experienced any breaches, implemented corresponding remediation plans, underwent regulatory inspections, was subject to restrictions or imposed conditions, or had any enforcement interactions during the relevant period. *(HKSQM 1 para. 30; HKSA 220 (Revised) para. 22)*
2	**Management integrity and competence**	• Insufficient evaluation of management's integrity, competence and intent in relation to digital asset activities, including their ability to identify risks (e.g., rapid	• Assess management's integrity, competence and governance over digital asset activities, taking into account the entity's specific circumstances, including the nature of its digital asset activities, governance and oversight arrangements, technological complexity,

#	Common Audit Issue	Description of Issue	Recommended Audit Response
		technology change, transaction anonymity and vulnerability to theft or illegal activities), implement controls and prepare related financial reporting, and operate within a regulated environment. Entities transitioning from an unregulated to a regulated environment may exhibit gaps in governance and internal controls which may have implications for the entity's financial statements and audit engagement. • Insufficient consideration of governance structure, related parties, beneficial ownership, founders, affiliates, market makers, outsourced operators, omnibus arrangements and other parties that may influence or control the entity's digital asset activities.	safeguarding arrangements, pseudonymous transaction nature and the applicable regulatory environment. *(HKSQM 1 para. 30(a); HKSA 220 (Revised) para. 22).* • If management lacks the necessary skills or competence (including over internal control and financial reporting) to identify and respond to digital asset risks, assess whether the audit is feasible. *(HKSQM 1 para. 30(a); HKSA 200 para. 4; HKSA 210 para. 6)* • Understand the entity's governance structure and parties influencing or controlling its digital asset activities; its business purpose and model and funding sources for digital asset activities; its use of unregulated platforms or counterparties; and maintain professional skepticism about any actual or suspected NOCLAR relevant to the financial statements and the auditor's responsibilities. *(HKSQM 1 para. 30(a); HKSA 220 (Revised) paras. 22–23, HKSA 250 paras. 13–15)*

🔍 Phase 2: Planning & Risk Assessment

#	Common Audit Issue	Description of Issue	Recommended Audit Response
3	**Insufficient understanding of the entity's digital asset activities**	• Insufficient understanding of the entity's digital asset activities, including their business objectives, strategies, custody arrangements, key management controls and applicable regulatory requirements.	• Understand the entity's specific role in the digital asset ecosystem (e.g., token issuance (issuer), proprietary trading, custodial services for clients, brokerage services, mining, staking, technology solutions or platform provision) as each role presents distinct risks,

#	Common Audit Issue	Description of Issue	Recommended Audit Response
		This results in inadequate identification and assessment of risks of material misstatement including fraud risks, and the resulting audit procedures are not sufficiently responsive to those risks. • Not sufficiently establishing the completeness of the entity's digital asset activities to identify all areas where balances, liabilities or commitments that may exist. This includes not only wallets and public addresses, but also exchange accounts and custodial sub-accounts; internal sub-ledgers and omnibus arrangements; smart contracts; staking validators; DeFi positions; and other off-chain records where balances or obligations may exist. • Lack of recognition between the entity using the blockchain as a system of record versus using the blockchain as a mirror/shadow record. In the case of the latter, auditors who review both the primary records and blockchain shadow records could be double-counting entries.	transaction flows and control considerations. *(HKSA 315 (Revised 2019) para. 19)* • Understand the entity's purpose and use of digital assets, such as: – types held; – acquisition and disposal methods; – transaction nature, frequency and value; – custody arrangements (self-custodied vs. third party; hot vs. cold wallets; single- vs. multi-signature); – reliance on blockchain technology and valuation processes; and – use as a primary system of record or merely a shadow/mirror record. *(HKSA 315 (Revised 2019) para. 19)* • Determine the specific classification of digital assets by distinguishing among native crypto assets, tokenized real-world assets (RWAs), wrapped or synthetic tokens, and other relevant types. *(HKSA 315 (Revised 2019) para. 19)* • For tokenized RWAs and wrapped or synthetic tokens, understand and evaluate the linkage to the underlying asset, including the issuer's identity, the legal form of the claim and key supporting evidence (e.g., offering documents, agreements, registries, CUSIPs or equivalents), and use this to inform the assessment of risks, rights and obligations, and the appropriateness of the entity's accounting treatment. *(HKSA 315 (Revised 2019) paras. 19–20, 28; HKSA 540 (Revised), para. 13)* • Understand the applicable legal and regulatory requirements and their implications on the financial statements, including those arising

#	Common Audit Issue	Description of Issue	Recommended Audit Response
			from cross-jurisdictional activities, and how the entity is complying with them. *(HKSA 315 (Revised 2019) para. 19(a)(ii); HKSA 250 para. 13–15)* • Understand and evaluate the end-to-end digital asset transaction flows—including initiation, prefunding, execution, trading, settlement, recording and reporting—and the related information systems, business processes and internal controls. *(HKSA 315 (Revised 2019) paras. 25–26)* • Identify all addresses, wallets, platforms and service providers; understand IT and other controls over wallet, including key generation, storage, recovery, incident response, approvals and transaction signing, and the use of smart contracts. *(HKSA 315 (Revised 2019) paras. 25–26)* • Where smart contracts are used, obtain an understanding of their design and operation and identify the existence of internal transactions; consider any related smart contract review or audit and their results where relevant *(HKSA 315 (Revised 2019) paras. 25–26)* • Use the understanding obtained to identify and assess risks of material misstatement; determine whether any are significant risks; and determine whether specialist skills are needed. *(HKSA 315 (Revised 2019) paras. 28–32; HKSA 620 para. 7)*
4	**Inadequate risk assessment, including fraud and significant risks**	• Failure to identify digital asset specific risks or evaluate management's own risk assessment process, including key risk drivers such as omnibus or nominee arrangements, delegated authority, emergency wallet access, protocol or governance changes, and non-arm's-	• Hold engagement team discussions on fraud risks specific to digital assets. This includes considering how the pseudonymous nature of on-chain transactions may act as a fraud risk factor, such as potentially providing opportunities for unauthorized transfers or concealing related party transactions. *(HKSA 240 para. 16; HKSA 315 (Revised 2019) para. 17)*

#	Common Audit Issue	Description of Issue	Recommended Audit Response
		length transactions obscured by pseudonymous addresses. • Not adequately assessing and responding to fraud risks associated with digital asset activities. • Failure to detect that an apparently independent counterparty wallet used to conceal related-party transactions.	• Consider whether there is limited or a lack of governance and oversight regarding digital asset activities and the impact that this may have on the overall risk assessment. *(HKSA 315 (Revised 2019) paras. 19(a)(i), 21)* • Understand management's policies and procedures relating to digital assets, including those for: – identifying related parties and related-party transactions; – performing due diligence on digital assets the entity intends to transact with; – onboarding new customers and counterparties in the digital asset ecosystem; and – ongoing monitoring for illegal or suspicious activity. *(HKSA 315 (Revised 2019) para. 19(a), 21; HKSA 250 para. 13; HKSA 550 para. 14)* • Review all correspondence and notes of meetings between the entity and relevant regulators, such as the SFC and the HKMA, to understand any regulatory risks or irregularities. *(HKSA 250 paras. 13–15; HKSA 315 (Revised 2019) para. 19(a)(ii))* • Ensure the risk assessment addresses digital asset specific factors and determine whether any identified risks are fraud or significant risks, such as: – management override of key generation, access, storage and transaction authorization; – pseudonymous transactions making it hard to identify the party in actual control of the wallets, including cases where a wallet appears to belong to an independent third party but is, in

#	Common Audit Issue	Description of Issue	Recommended Audit Response
			substance, controlled by a related party and used to conceal related party transactions; – complex, unusual, unsupported or off-chain transactions without clear business purpose; – transactions with non-commercial rationale and/or outside the normal course of business, including those to conceal misappropriation; – susceptibility to manipulation, theft or illicit finance arising from digital asset characteristics (e.g. irrevocability, private key compromise, decentralized platforms) – patterns of rapid in-and-out or offsetting trades, or repeated trading with wallets under common control, indicating possible wash trading or round-tripping with related parties; and – risks arising from the digital asset related technology and ecosystem, such as: ▪ technology and protocol, including the security and stability of the underlying code, smart-contract and protocols; ▪ decentralization and governance, including consideration of who effectively controls or influences the protocol or network; ▪ liquidity and market manipulation that may affect valuation, fair value measurement and disclosure; ▪ custody and key management such as loss, theft or destruction of private keys; unauthorized access; multi-signature governance; ▪ regulatory and compliance, licensing status, ongoing licence conditions, cross-border requirements; and

#	Common Audit Issue	Description of Issue	Recommended Audit Response
			illicit-finance risks, e.g., money laundering, sanctions evasion, exposure to addresses flagged on public watchlists.*(HKSA 315 (Revised 2019) paras. 28–32; HKSA 240 paras. 24–28)* • Understand and evaluate how the entity reflects on- and off-chain transactions in its records, including how management verifies the reliability of information for transactions not processed on a public blockchain, and determine what audit evidence is available to support their existence. *(HKSA 315 (Revised 2019) para. 25)*
5	**Insufficient assessment of the entity's accounting policies and treatment**	• Not appropriately assessing the entity's accounting for digital assets, including the classification, measurement basis and applicable accounting policies for each type or class of digital asset held or transacted. For example, management may treat all digital assets alike, despite that payment tokens, stablecoins, wrapped tokens, self-issued tokens, security tokens and tokenized claims can have materially different accounting implications depending on their legal form, contractual rights, redemption features, restrictions, issuer relationship and the entity's business model. In the absence of a digital-asset-specific accounting standard, the accounting treatment involves significant management judgment, giving rise to complexity and uncertainty for both management and the auditor.	• Determine the nature and characteristics of each type or class of digital asset and related transaction, and evaluate the appropriateness of the accounting policies adopted by management in light of the digital assets held, the entity's business model, contractual arrangements etc. • Evaluate management's policies for identifying and recognizing digital assets arising from non-standard acquisition events (e.g., airdrop and dusting) and assess whether all such transactions and balances are recognized appropriately. • Evaluate how the entity generates revenue from digital assets (e.g., trading fees, mining rewards, staking yields, transaction facilitation) and the related recognition policies. • Where the entity holds multiple types of digital assets or engages in different business activities (e.g., proprietary vs. custodial), assess whether management has appropriately distinguished the accounting treatment for each. • Evaluate the entity's valuation policies and processes, including:

#	Common Audit Issue	Description of Issue	Recommended Audit Response
		• Not sufficiently understanding the entity's staking, lending, DeFi and mining pool arrangements, resulting in key features being overlooked and misstatements in classification, measurement, disclosure and going concern. • Not appropriately assessing the entity's self-issued tokens (utility, governance or security-like) and security tokens on the balance sheet to determine whether they represent equity, financial liabilities, revenue, utility rights or other obligations.	– how management identifies and determines the principal market for each digital asset, including whether the market is active and orderly and the pricing sources used; – the valuation and impairment approach adopted; and – the measurement date and time applied, and consistency of application across periods. • Understand each material staking, lending and DeFi arrangement, including its key terms and economics, and determine the resulting assets, liabilities or derivatives and their appropriate classification and measurement. • Where the entity participates in mining pool arrangements, understand the relevant contractual terms and reward-sharing mechanism; evaluate management's accounting policy for recognizing mining rewards; and assess whether amounts receivable from, or held by, the pool operator are appropriately recognized and recoverable. • Evaluate whether self-issued tokens are appropriately classified (equity, liability, revenue or other obligations) and assess whether token-based compensation, airdrops and incentives are fully recorded and correctly classified. • For security tokens on the balance sheet, evaluate classification and measurement based on the token's own rights and obligations, including its instrument nature (e.g., equity, debt or derivative), the tokenization structure and how ownership and claims are legally enforceable. • Stay current with evolving financial reporting developments, engaging technical accounting specialists and advisory teams as needed.

#	Common Audit Issue	Description of Issue	Recommended Audit Response
			(HKSA 315 (Revised 2019) paras. 19(b), 20; HKSA 540 (Revised) para. 13)
6	**Inadequate understanding and assessment of the entity's internal controls, including controls over Anti-Money Laundering (AML) and Know Your Customer (KYC) processes, GITCs & cybersecurity**	• Not evaluating whether the entity's controls over digital asset activities are designed and operating effectively, including controls over wallet creation and decommissioning; seed phrase recovery and backup; privileged or emergency access; changes to smart contract parameters; and segregation of client assets from proprietary positions where relevant. For example, management's review of variances is aggregated and on a net basis rather than individually and on an absolute basis, which may mask asset-level misstatements. • Insufficient understanding and evaluation of the entity's controls over AML and KYC processes, IT environment and GITCs relevant to digital asset activities. *Note: Even where the auditor does not plan to test the operating effectiveness of controls, an understanding of the IT environment, and IT applications and GITCs that address the IT risks identified is required.*	• Understand and evaluate the design and operating effectiveness of the entity's controls over digital asset activities. Test the operating effectiveness of these controls where the auditor plans to rely on them or where substantive procedures alone cannot provide sufficient appropriate audit evidence. • Understand and evaluate the entity's internal controls over AML and KYC processes, particularly in relation to customer onboarding, revenue and other relevant transaction cycles where AML/KYC failures may give rise to risks of material misstatement. • Understand the entity's IT environment for digital assets, including IT applications (e.g., blockchain nodes, wallet systems, trading platforms, custodial systems, sub-ledger/reporting systems), transaction flows and degree of automation. • Understand cyber risk management controls for digital asset safeguarding (e.g., network security, anti-phishing, intrusion detection, incident response). • Identify risks arising from the use of IT (e.g., unauthorized access to private keys, changes to wallet configurations or smart contracts) and the GITCs that address them. • For IT-related risks, evaluate the design and implementation of GITCs that address those risks. Where reliance on controls is planned, test the operating effectiveness of the relevant GITCs. • For platform providers regulated by the SFC, understand and evaluate the entity's security controls over platform infrastructure,

#	Common Audit Issue	Description of Issue	Recommended Audit Response
			including whether the entity has established a Security Operations Centre or equivalent function as required by the SFC. • Where financial reporting processes or controls are performed by a service organization, – understand the entity's use of the services, including the nature and significance of the services, the nature and materiality of the transactions processed or transactions affected, etc.; and – identify and evaluate the design and implementation of relevant user-entity controls. Where sufficient understanding cannot be obtained from the entity, obtain it through a service auditor's SOC report or other appropriate procedures. • When using a SOC report, evaluate the service auditor's competence and independence, the standards applied, the relevance of the scope and period covered, the sufficiency of evidence provided, and whether relevant complementary user entity controls have been designed and implemented. *(HKSA 315 (Revised 2019) paras. 25–26; HKSA 330 para. 8; HKSA 402 paras. 9–14)*

⚖️ Phase 3: Responding to Assessed Risks

#	Common Audit Issue	Description of Issue	Recommended Audit Response
7	**Insufficient evidence over existence, completeness and**	• Not verifying the completeness and accuracy of the wallet and address listing.	• Verify the completeness of the wallet and address listing, for example, by:

#	Common Audit Issue	Description of Issue	Recommended Audit Response
	accuracy of digital asset transactions and balances	• Relying on records from the blockchain or internal systems as evidence of existence without evaluating the relevance and reliability of that information. • Not identifying or testing off-chain transactions and balances that are not verifiable through blockchain explorers, such as activities within exchange internal ledgers, omnibus positions, certain staking or lending arrangements, or undocumented side agreements, where on-chain procedures alone are insufficient to address the completeness of off-chain activities. • Not adequately assessing balances held at unregulated exchanges or platforms where the legal enforceability of claims, segregation of client assets and quality of financial information are uncertain.	– using blockchain analytics tools to corroborate management's records and identify undisclosed wallets, addresses or transactions; – identifying transactions that may not be surfaced by standard explorers and designing procedures to capture them. This evaluation should be informed by a sufficient understanding of the entity's business, transaction flows and use of smart contracts, recognizing that internal transactions may not be visible through standard explorers and that cross-explorer comparison alone may not overcome such limitations; – inspecting legal contracts, service agreements and side letters to identify undisclosed off-chain transactions, lending terms, collateral requirements, or staking arrangements that do not trigger on-chain movements; and – for digital assets held on centralized platforms, obtain and reconcile the entity's internal records to account statements, activity logs, and internal sub-ledgers provided by the platform or exchange. • For digital assets held at exchanges or on third-party platforms, independently and directly confirm balances with the exchange institutions or custodians as at the reporting date. • Agree additions and disposals of digital assets to relevant supporting documentation (e.g., trade orders and confirmations) and assess whether the entity has properly recorded and recognized the transactions. • For entities holding digital assets on behalf of clients as well as on their own account, evaluate controls over the segregation and

#	Common Audit Issue	Description of Issue	Recommended Audit Response
			reconciliation of client balances from the entity's proprietary balances. • Where the entity engages in mining activities using equipment hosted at third-party facilities, consider performing a site visit of the hosting facility, including observation of physical and environmental controls over the mining equipment. • Obtain management representations confirming that all digital asset transactions, wallets, addresses and holdings have been disclosed. • For balances at unregulated exchanges, obtain additional evidence over recoverability and consider whether limitations in available evidence represent a limitation of scope. • Note that, in audits of entities with complex digital asset activities, substantive procedures alone are generally unlikely to provide sufficient appropriate audit evidence. A combination of testing the operating effectiveness of relevant controls including GITCs and substantive procedures is typically required to address the assessed risks of material misstatement. *(HKSA 330 para. 8; HKSA 500 paras. 6–7, 9; HKSA 505 para. 16; HKSA 580 para. 10)*
8	**Insufficient evidence over rights and obligations**	• Insufficient distinction between legal ownership, beneficial ownership, technical control of a wallet/private key, custody arrangements and safeguarding obligations, for example, treating signing ability or wallet access as evidence of ownership. • Not obtaining sufficient appropriate audit evidence to verify the ownership of digital	• Design and perform a combination of procedures—such as on-chain verification, evaluation of controls over private-key management and other substantive procedures—to address the rights and obligations assertion, distinguishing legal ownership, beneficial ownership, technical control, custody arrangements and safeguarding obligations. Signing ability or possession of a private key is not, in itself, evidence of ownership.

#	Common Audit Issue	Description of Issue	Recommended Audit Response
		assets, including those associated with a public address. • Relying on blockchain records or private key access as sole evidence of ownership, without recognizing that private keys may be accessible by multiple parties, and that technical control or signing ability alone does not establish legal ownership. • Relying on custodian confirmations without evaluating custodian controls or service organization reports. • Treating multi-signature or hardware wallet set-ups at face value (for example, "3-of-5" wallets) and overlooking indicators that unauthorized parties can still move assets unilaterally, so genuine multi-party control is not achieved.	• Test the entity's effectiveness of controls that mitigate the risk of theft, loss, destruction, unauthorized acquisition, use or disposition of assets. • Test controls over the lifecycle of private keys regarding whether they are generated, distributed, stored, used, rotated and backed up in a secure and confidential manner. • Verify the entity's control over private keys through procedures such as: – physically observing the entity's key generation ceremony and wallet creation process; – observing the entity cryptographically signing a test transaction or message using the private keys of its wallets at the reporting date; – observing a controlled transfer of digital assets between the entity's wallets to evaluate whether the entity has sole control over those wallets; and – confirming control with other supportive evidence. If needed, supplement with post-year-end testing. • For initial engagements, if the entity was already in operation prior to the audit, evaluate whether to request the entity to re-generate wallets and keys for audit evidence over opening balances and prior-period key ownership. • For third-party custodied assets, review custodial agreements (including terms on segregation of client assets, safeguarding obligations, sub-custody and liability), obtain independent confirmations of balances and ownership from the custodian, and assess whether a SOC report is available and sufficient for the

#	Common Audit Issue	Description of Issue	Recommended Audit Response
			auditor's purposes, including coverage of relevant control objectives, scope and period, exceptions noted, and complementary user entity controls. • Where a SOC report is not available or insufficient, determine what additional procedures are necessary, which may include: – test the custodian's controls directly where permitted; – test the entity's oversight controls used to monitor the custodian; – reconcile custodian statements with the entity's internal records and on-chain data; and – verifying on-chain balances and transactions at custodial wallet addresses confirmed by the custodian using reliable blockchain explorers or analytics tools. • Consider the timing of ownership verification procedures relative to the reporting date and whether roll-forward or roll-back procedures are needed. *(HKSA 330 paras. 6–10; HKSA 402 paras. 15–18; HKSA 500 para. 6; HKSA 505 para. 16; HKSA 510 para. 6(c);)*
9	**Inadequate assessment of valuation and fair value measurement**	• Not evaluating the relevance or reliability of third-party pricing information used in management's valuation of digital assets. • Inadequate assessment of the principal market identified by management for each digital asset, including how liquidity, transfer restrictions, market depth and pricing anomalies may vary significantly by token, venue and time. This is	• Obtain independent prices and compare them with those used by the entity. Evaluate the relevance and reliability of the pricing information used as audit evidence, having regard to the highly volatile nature of digital asset prices and the potential for sudden and extreme fluctuations. *(HKSA 500 paras. 6–7)* • For digital assets measured at fair value, evaluate: – the appropriateness of the fair value hierarchy and classification;

#	Common Audit Issue	Description of Issue	Recommended Audit Response
		particularly critical for volatile or thinly traded assets and for measurements determined at a specific reporting date and time. • Not adequately assessing fair value and its hierarchy classification, especially for less liquid or restricted digital assets.	– the valuation methodology, assumptions and data used; and – whether the fair value measurement is determined in accordance with the applicable financial reporting framework. *(HKSA 540 (Revised) paras. 22–26, 31)* • For digital assets measured at cost less impairment, evaluate the impairment assessment approach and the impairment indicators applied. *(HKSA 540 (Revised) paras. 22–26)* • For entities holding mining equipment, evaluate management's identification and assessment of impairment indicators, such as a significant decline in the price of the relevant cryptocurrency which may imply impairment of the equipment's recoverable amount including value-in-use. *(HKSA 540 (Revised) paras. 22–26)* • Given the 24/7/365 nature of digital asset trading, evaluate the entity's cut-off convention including the specific measurement date and time (e.g., UTC 00:00 on the reporting date) and its consistent application in valuation and measurement. *(HKSA 540 (Revised) paras. 23, 25)* • Where expert assistance is needed (e.g., principal market determination, valuation of illiquid or level 3 digital assets), evaluate the expert's qualifications, competence and objectivity, the relevance and reasonableness of their conclusions, and the key assumptions and valuation methods applied, including the completeness and accuracy of any source data. *(HKSA 620 paras. 7, 9, 12)*
10	**Insufficient procedures related to occurrence and**	• Not adequately responding to the risks of material misstatement related to revenue generated from diverse digital asset activities, including trading, mining,	• Check digital asset trade transactions to the underlying trade orders, relevant settlement evidence and confirmations obtained by the auditor.

#	Common Audit Issue	Description of Issue	Recommended Audit Response
	recognition of revenue	staking rewards, validator income, custody or safeguarding fees, platform fees, token issuance-related arrangements and white-label service models. • Not performing procedures to assess the appropriateness of revenue recognition related to the transfer of digital assets.	• Perform cut-off testing, considering blockchain confirmation times and pending transactions at reporting date. • For entities providing technology solutions or white-label services, check service fees recognized to relevant evidence including agreements, transaction records and invoices. • Assess whether a transfer of digital assets (including a transfer to a related party) qualifies as a contract with a customer under the applicable financial reporting framework and, if so, whether the relevant revenue recognition criteria have been met. *(HKSA 330 para. 6; HKSA 500 paras. 6, 7, 9)*
11	**Relying on unverified information as audit evidence**	• Relying on information from third-party tools (e.g., blockchain explorers and exchange platforms) or the entity's internally generated reports as audit evidence without testing the completeness and accuracy of that information. • Performing substantive procedures that are dependent on the entity's internally generated data and reports, or on the effectiveness of controls such as over custody or private key safeguarding, without testing those information or controls. • Not testing the completeness of populations used for substantive testing.	• Evaluate the relevance, reliability and completeness of information obtained from blockchain explorers, exchange platforms, internal systems and other third-party sources before using it as audit evidence. Example procedures may include: – assessing the reliability of the explorer or analytics tool used, including whether it is a firm-approved tool that has undergone appropriate testing, or a public explorer whose output is corroborated against at least two other independent explorers; – multi-source validation where third-party tools (blockchain explorers) are being used, while taking into consideration factors such as node independence and common data sourcing/ownership among blockchain explorers; – verifying on-chain balances and transactions and reconciling them with internal records, custodian statements and other sources, with consideration of the explorer's coverage and limitations; and

#	Common Audit Issue	Description of Issue	Recommended Audit Response
			– where only one explorer exists for a given blockchain, consider whether the results are sufficiently reliable or perform additional procedures. • Obtain audit evidence regarding the completeness of populations or listings used to select items for testing (e.g., cold storage movements, system changes, inter-wallet transfers) by testing the operating effectiveness of controls over the production and maintenance of the data, noting that testing internal controls or GITCs is often necessary to effectively address information completeness in digital asset systems. • Where substantive procedures are dependent on the entity's internally generated data and reports, or on the operating effectiveness of controls (e.g., controls over private key safeguarding), test those information or controls for completeness and accuracy before using them to perform substantive procedures. *(HKSA 500 paras. 7–9, HKSA 330 para. 8(a))*
12	**Failure to assess whether client assets held under trust, custody or bankruptcy-remote structures and related obligations should be recognized on the balance sheet**	• Not obtaining sufficient evidence over the completeness and measurement of customer and other liabilities when the entity holds assets on behalf of customers. • Where client assets are held for others (e.g., under trust, custody or bankruptcy-remote structures), not clearly assessing whether the assets and related obligations meet the criteria for recognition on the entity's balance sheet or should instead be presented	• Design procedures specifically over the completeness and measurement of customer and other liabilities, including procedures to identify unrecorded or off-chain obligations such as borrowings, margin and settlement obligations, redemption commitments, pledged assets. • For entities holding client assets, evaluate the legal form and substance of the arrangement (for example, whether the entity acts as principal, agent, custodian or trustee) and, under the applicable reporting framework, assess whether the entity controls the related assets and obligations and meets the recognition criteria in that framework, in order to determine whether to recognize them on

#	Common Audit Issue	Description of Issue	Recommended Audit Response
		off-balance-sheet with appropriate disclosures.	balance sheet or to present them off balance sheet with appropriate disclosures. *(HKSA 300 para. 6; HKSA 500 para. 6)*
13	**Failure to adequately assess going concern and stressed liquidity**	• Management's going concern assessment is accepted without sufficient challenge, even where the entity faces significant volatility, asset concentration risk, reliance on a few key counterparties. • The auditor focuses on point-in-time balance sheet values without considering stressed realisability, including assets that are restricted, locked, pledged, self-issued, illiquid or operationally inaccessible.	• Critically assess management's going concern analysis, including key assumptions and the realisability of digital asset liquidity under stress, taking into account concentration, market depth, lock-ups, staking or collateral restrictions and dependence on key exchanges. • Perform sensitivity analysis on severe but plausible downside scenarios. • Given the volatility of the digital asset industry, evaluate subsequent events occurring between the reporting date and the date of the auditor's report (and, where relevant, up to the date the financial statements are issued) that may affect the going concern assessment, particularly for entities with significant exposure to digital assets, and determine whether such event is appropriately reflected in the financial statements in accordance with the applicable financial reporting framework. Relevant subsequent events may include exchange insolvencies, wallet compromises, changes in licence status and enforcement actions. *(HKSA 560 paras. 6–9; HKSA 570 (Revised) para. 12)*

✅ Phase 4: Completion & Reporting

#	Common Audit Issue	Description of Issue	Recommended Audit Response
14	**Inadequate assessment of disclosures relating to digital assets activities**	• Not evaluating whether disclosures related to digital asset activities are complete, accurate and in conformity with the applicable financial reporting framework. • Not evaluating whether accounting policies on digital assets are a key source of significant management judgment and estimation uncertainty. • Not evaluating whether disclosures and information relating to the entity's digital asset activities, including significant accounting policies, judgments, key sources of estimation uncertainty and related risks are adequate to enable financial statements users to understand their financial effects.	• Evaluate whether digital asset disclosures are relevant, reliable, comparable and understandable, and sufficient to enable intended users to understand the associated risks, uncertainties and their effect on the financial statements, including where relevant, the custody model and any client-asset exposure; concentration risks and liquidity limitations; legal and regulatory uncertainties surrounding the digital assets; significant valuation judgments made by management. *(HKSA 700 (Revised) para. 13)* • Evaluate the balance sheet presentation of digital assets held on behalf of others (on- vs. off-balance sheet) and assess how this accounting treatment impacts the risk of material misstatement. *(HKSA 700 (Revised) para. 13)* • Read other information in the annual report on any material inconsistencies with the financial statements or the auditor's knowledge, including digital asset information. *(HKSA 720 (Revised) paras. 14–15)*
15	**Consideration of auditor opinion**	• Not considering whether the unique risks and uncertainties of digital asset activities warrant additional communication in the auditor's report. • The complexity of digital asset arrangements and uncertainties may create difficulties for the auditor to obtain sufficient appropriate audit evidence.	• Where sufficient appropriate audit evidence cannot be obtained, consider the implications for the auditor's report, including whether a qualified opinion or disclaimer of opinion is appropriate. *(HKSA 330 para 27; HKSA 705 (Revised) para. 6(b))*

Resources

HKICPA Reference Library

📌 **The Institute has developed the following resources to support auditors in relation to digital assets:**

- **Practice Note (PN) 831, *Reporting on Reserve Assets of Licensed Stablecoin Issuers under the Stablecoins Ordinance*** — guidance on stablecoin reserve attestation engagements under the HKMA stablecoin issuer licensing regime. Although outside the scope of this guide, PN 831 may offer useful practical reference for practitioners.
- **Accounting guidance on cryptocurrencies and stablecoins** — guidance on which HKFRS Accounting Standards apply to cryptocurrencies and stablecoins, including classification and measurement under HKAS 2, HKAS 38 and HKAS 32.
- **E-learning course: Accounting and auditing considerations for digital assets** — covering common accounting issues including classification, measurement, presentation and disclosure, and auditing considerations such as confirmation challenges and valuation.

Other Guidance and Resources

Source	Overview	Link
🔍 **CPAB**	Inspection insights from oversight of Canadian Public Accountability Board (CPAB) on the crypto-asset sector audits. Highlights common deficiencies and regulatory expectations on audit quality in digital asset-related engagements.	*cpab-ccrc.ca/insights/crypto-assets*
📘 **ICAEW**	Considerations for auditing cryptocurrencies, including key concepts, ethical considerations and common risks associated with auditing cryptocurrencies.	*icaew.com/technical/technology/blockchain-and-cryptoassets/blockchain-helpsheets/considerations-for-auditing-cryptocurrencies*
🌐 **IAASB**	Guidance and resources to support practitioners in navigating the use and impact of technology in auditing.	*iaasb.org/focus-areas/technology*
🛡️ **PCAOB**	Public Company Accounting Oversight Board's (PCAOB) inspection observations related to public company audits involving crypto assets.	*pcaobus.org/documents/crypto-assets-spotlight.pdf* *pcaobus.org/documents/target-team-2023-inspections-spotlight.pdf*

Publication Date: July 2026