ACRA
Accounting And Corporate Regulatory Authority

Audit Practice Guidance No. 3 of 2026

Considerations in Digital Asset Audits

Issued on 11 November 2026



INTRODUCTION

Digital asset audits present risks that differ significantly from financial statement audits of other business models or industries. The business activities of such entities may involve:

- Being service providers such as exchanges or custodians
- Holding or trading of cryptocurrencies or crypto derivatives (e.g. crypto funds)
- Issuance of stablecoins, security tokens or utility tokens
- Mining or staking of digital assets

Certain business activities may also be subject to regulation (e.g. by the Monetary Authority of Singapore under the Payment Services Act), which may result in the entities being classified as Public Interest Entities (PIEs).

The decentralised nature of blockchain technology, the use of private keys, reliance on third-party custodians, smart contract functionality and rapidly evolving business models require auditors to adapt their risk assessment and audit procedures accordingly. Recent inspection findings indicate that many deficiencies arise from an insufficient understanding of the underlying technology or information technology (IT) environment, resulting in inadequate or ineffective audit procedures being performed and a failure to obtain sufficient and appropriate audit evidence to support the audit opinion.

The most common deficiencies in digital asset audits stem from inadequate understanding of blockchain-related risks and insufficient audit evidence due to unwarranted reliance on management or third-party information. This publication seeks to highlight the potential key considerations that audit teams should consider when planning and executing digital asset audits.

CONSIDERATIONS WHEN ACCEPTING/CONTINUING AUDIT ENGAGEMENTS AND/OR PLANNING DIGITAL ASSET AUDITS:

- Has the auditor properly assessed whether the accounting entity (AE) has the required competency or capability to perform audits that involve blockchain technology and digital assets as part of the acceptance and continuance process for the AE?
- Has the auditor obtained a sufficient understanding of the operational and business risks associated with the client, including potential fraud risks?
- Does the AE have access to the required IT, blockchain, cryptography or valuation expertise?
- Has the auditor properly identified and assessed the audit risks relating to blockchain technology and digital assets?
- Are there policies and procedures in place to apply heightened professional skepticism when performing such audits (e.g. involvement of technical consultations or engagement quality reviewers)?

Fraud risks for blockchain transactions are elevated due to the nature of the operations (being decentralised and highly automated) and the pseudo-anonymity of the parties involved.

Examples of fraud risks for digital asset audits may include:



Private keys used to access the digital assets are not properly safeguarded, resulting in fraudulent access or use



Unusual transactions involving digital assets that lack a clear business rationale or fall outside the normal course of business, especially those involving related or affiliated parties



Weak internal controls with regard to the segregation of customers' digital assets and entity's own digital assets



© Accounting and Corporate Regulatory Authority

CONSIDERATIONS WHEN EXECUTING DIGITAL ASSET AUDITS

Example 1: Crypto trading platform with exchange-held assets and cold wallets

Case Facts

Company A operates a cryptocurrency trading business using its own proprietary trading platform that automatically performs trade matching and computation of commission fee income.

Arising from its business activities, Company A holds digital assets on behalf of its customers. Company A records these digital assets as inventories in accordance with FRS 2 *Inventories* and correspondingly records amounts owing to customers as liabilities on the balance sheet. Most of the assets are held with overseas exchanges that provide custody services, while a smaller portion is kept in cold wallets managed internally by the finance team.

Company A provides the auditor with screenshots from the overseas exchange dashboards and an internally prepared cold wallet listing to support the year-end digital asset balances. Reports from the proprietary trading platform are provided to the auditor to support the year-end balances for commission fee income and amounts owing to customers.



Relevant Audit Considerations

IT considerations

- Has the auditor obtained sufficient understanding of the IT environment of Company A (such as Company A's proprietary trading platform and its digital asset wallets), in order to assess the risk of material misstatement arising from the use of IT and general IT controls in relation to the IT applications in accordance with SSA 315 (Revised) *Identifying and Assessing the Risks of Material Misstatement*? Considerations include, but are not limited to:
  - Can trade evidence/information be manipulated or falsified?
  - Can unauthorised transactions be made through the Company's digital asset wallets?
  - Can customer records of digital assets be incomplete or falsified?
- Has the auditor involved the appropriate level of specialists (e.g. IT or cryptography specialists) to address said risks?

Custody arrangement of digital assets

- Has the auditor understood the custody arrangement of Company A's digital assets that are held with the exchanges – are the assets held in Company A's own name or pooled with other customer assets?
- Has the auditor understood the custody arrangement of the digital assets that are held by Company A on behalf of its customers? Does Company A have the contractual/legal rights to utilise these assets? Are these assets pooled with Company A's own assets and are there any measures in place to safeguard the customers' assets?

© Accounting and Corporate Regulatory Authority

Risks relating to Information Produced by Entity (IPE)

- Do screenshots from the exchange dashboards and management-prepared schedules provide sufficiently reliable audit evidence over the existence and ownership of the assets as at the financial year-end in accordance with SSA 500 *Audit Evidence*?
  - Should the auditor instead obtain audit evidence from independent external information sources (e.g. by directly querying wallet balances on the blockchain)?
  - Has the auditor applied professional skepticism in considering potential tampering of the audit evidence?
- Do reports from the proprietary trading platform provide sufficiently reliable audit evidence over the completeness and accuracy of commission fee income and amounts owing to customers?
- Are there other sources (such as a System and Organisation Controls report) that report on the internal controls of the overseas exchanges for Company A that might indicate higher reliability of the audit evidence?

Private key ownership

- Has the auditor performed sufficient appropriate audit procedures to understand who controls the private keys of the cold wallets, in ascertaining the ownership of the digital assets held in these wallets?

© Accounting and Corporate Regulatory Authority

Example 2: Staking business using smart contracts

Case Facts

Company B earns revenue by staking digital asset Token X through a decentralised protocol. Staking rewards are calculated automatically by smart contracts and reported through a third-party blockchain explorer for Token X.

Management records staking income based on monthly reports exported from Token X's blockchain explorer, together with its own spreadsheet calculations.



Relevant Audit Considerations

Understanding staking arrangements

- Has the auditor obtained sufficient understanding of the blockchain infrastructure of the staked Token X and the related automated transaction processing in accordance with SSA 315 (Revised) *Identifying and Assessing the Risks of Material Misstatement*, in addressing the key risks around revenue recognition?
  - How does the staking protocol work?
  - Is Company B acting as a validator or delegator in the staking arrangement?
  - How and when are rewards generated? How do these rewards meet the performance obligations of Company B in accordance with FRS 115 *Revenue from Contracts with Customers*?

Risks relating to Information Produced by Entity (IPE)

- Has the auditor assessed the risks associated with system-generated or blockchain-derived information as reliable audit evidence, in accordance with SSA 500 *Audit Evidence*?
  - What is the accuracy and completeness of information extracted by the blockchain explorer for Token X from the blockchain?
  - Are there other sources (such as a System and Organisation Controls report) that report on the internal controls of the blockchain explorer for Token X that might indicate higher reliability of the audit evidence?

The auditor should not assume that outputs from a blockchain explorer or dashboards are complete and accurate solely because they are derived from or linked to public blockchain data.

© Accounting and Corporate Regulatory Authority

Example 3: Token issuer holding own tokens

Case Facts

Company C issues its own utility token (Token Y) to raise funds for a blockchain-based platform. Token Y is classified as an intangible asset with indefinite useful life, based on the revaluation model in accordance with FRS 38 *Intangible Assets*.

At initial recognition, minted Token Ys allocated to Company C as part of Token Y's initial coin offering are recorded at zero cost.

Subsequently, based on the latest quoted price of Token Y from a lightly traded exchange on the transaction date:

- Company C recognises proceeds from sales of Token Y as revenue; and
- Company C also uses corresponding amounts of Token Y to pay vendors for expenses, whereby expenses are recognised with equivalent realised gains from transferring Token Y to vendors.

Management records token sales revenue and realised gains from disposing Token Y based on monthly reports exported from Token Y's blockchain explorer, together with its own spreadsheet calculations.



Relevant Audit Considerations

Token economics

- Has the auditor obtained sufficient understanding of the token economics of Token Y?
  - Based on the initial coin offering protocols for Token Y, when does Company C have rights and obligations to the Token Y that it receives, in order for such Token Ys to be recognised as assets?

Measurement considerations

- Is it appropriate for Token Y to be initially measured at nil value? Are there directly attributable costs related to creating Token Y that should be considered?
- Is it appropriate for Token Y to continue to be valued at nil value, even after they are unlocked for use/trading by Company C? Has the fair value of Token Y changed as a result of it being unlocked for use/trading by Company C?
- For tokens with limited trading activity, does the quoted price of such tokens represent fair value in accordance with FRS 113 *Fair Value Measurement*? Are any adjustments required to be made to the quoted price?

Risks relating to Information Produced by Entity (IPE)

- Given that Company C issues Token Y, are there potential risks when using Token Y's blockchain explorer to ascertain the occurrence, accuracy and completeness of Company C's token sales revenue relating to Token Y?
  - Who created and developed Token Y's blockchain explorer?
  - Who owns, controls and maintains Token Y's blockchain explorer?
  - As the issuer of Token Y, can Company C impact the output obtained from Token Y's blockchain explorer (e.g. having the ability to make changes to the blockchain's source code or holding on to a majority stake of Token Ys such that Company C might be able to alter blockchain records)?

Such considerations are also applicable to audit clients that are related to or affiliated with a token issuer.

© Accounting and Corporate Regulatory Authority

CONCLUSION

In a time of rapid technology development, blockchain technology provides the opportunity for groundbreaking business models and innovative product/service offerings that are radically different from traditional brick-and-mortar businesses or financial institutions.

ACRA and other stakeholders (e.g. other regulators such as the Monetary Authority of Singapore (MAS), investors and customers) expect auditors to obtain a robust understanding of the underlying business and technological risks and to adopt a more technology-informed, risk-focused and evidence-driven approach. As digital asset ecosystems become increasingly sophisticated, such an approach is essential to delivering high-quality audits and maintaining trust in the business ecosystem.





About Accounting and Corporate Regulatory Authority

The Accounting and Corporate Regulatory Authority (ACRA) is the regulator of business registration, financial reporting, public accountants, and corporate service providers. We are responsible for developing the accountancy sector and setting the accounting standards for companies, charities, co-operative societies, and societies in Singapore. ACRA fosters a vibrant and trusted business environment that enables innovation and growth and contributes towards making Singapore the best place for business.

For more information, please visit www.acra.gov.sg

Copyright © 2026 All rights reserved. Accounting and Corporate Regulatory Authority
This document is exclusive property of the Accounting and Corporate Regulatory Authority. Any revision, use, duplication or commercial distribution of this work is permitted only with the consent of the Accounting and Corporate Regulatory Authority.

ACRA
ACCOUNTING AND CORPORATE REGULATORY AUTHORITY