DIGITAL JERSEY

Digital Asset Readiness: Audit, Accounting, and Reporting Considerations

A summary of Digital Jersey's 'FinTech in Practice' webinar, where HT.Digital covered the evidence, controls, accounting judgements and reporting processes firms should consider when holding, transacting in or supporting clients with digital assets and tokenised assets

Sep 2026

Executive Summary

Digital Jersey's latest FinTech in Practice webinar examined what digital asset readiness means in practice for businesses, auditors, accountants and other professional services firms. The discussion focused on the control environment that supports reliable financial reporting, the evidence required to establish ownership and control, the completeness of blockchain-derived data, valuation challenges and the accounting frameworks that may apply.

The central message was that digital assets introduce important technical differences, but many of the underlying professional disciplines remain familiar. Firms still need clear governance, effective access and change controls, reliable records, documented accounting policies, consistent valuation methods and appropriate evidence. The technology changes how transactions are authorised, recorded and verified. It does not remove management's responsibility for the financial statements or the auditor's need for sufficient and appropriate evidence.

Three areas were identified as central to most digital asset audits: ownership, control and custody; completeness and accuracy of transaction data; and valuation. Each area requires firms to understand the full operating model, including wallets, private keys, custodians, blockchains, data extraction tools, subledgers and the general ledger. A balance visible on a blockchain may confirm that assets exist at an address, but it does not by itself prove who owns or controls that address.

The panel also emphasised the importance of audit readiness before the year end. Weak information technology general controls can make system-generated information unreliable and materially increase the work required. Similarly, unclear custody arrangements, incomplete transaction mapping, reliance on a single block explorer or inconsistent pricing policies can create avoidable audit issues.

For Jersey firms, the opportunity is practical. Digital asset activity is moving into established financial services and tokenised real-world assets. Businesses do not need to abandon familiar risk management and assurance principles. They need to apply them to new infrastructure, understand the areas where blockchain changes the evidence, and involve the right specialists early.

Executive Summary

This webinar examined what digital asset readiness means in practice for businesses, auditors, accountants and other professional services firms. The discussion focused on the control environment that supports reliable financial reporting, the evidence required to establish ownership and control, the completeness of blockchain-derived data, valuation challenges and the accounting frameworks that may apply.

The central message was that digital assets introduce important technical differences, but many of the underlying professional disciplines remain familiar. Firms still need clear governance, effective access and change controls, reliable records, documented accounting policies, consistent valuation methods and appropriate evidence. The technology changes how transactions are authorised, recorded and verified. It does not remove management's responsibility for the financial statements or the auditor's need for sufficient and appropriate evidence.

Three areas were identified as central to most digital asset audits: ownership, control and custody; completeness and accuracy of transaction data; and valuation. Each area requires firms to understand the full operating model, including wallets, private keys, custodians, blockchains, data extraction tools, subledgers and the general ledger.

The panel also emphasised the importance of audit readiness before the year end. Weak information technology general controls can make system-generated information unreliable and materially increase the work required. Similarly, unclear custody arrangements, incomplete transaction mapping, reliance on a single block explorer or inconsistent pricing policies can create avoidable audit issues.

For Jersey firms, the opportunity is practical. Digital asset activity is moving into established financial services and tokenised real-world assets. Businesses do not need to abandon familiar risk management and assurance principles. They need to apply them to new infrastructure, understand the areas where blockchain changes the evidence, and involve the right specialists early.

Laeeq Shabbir - HT.Digital

Contact

Jonathan Wade - HT.Digital

Contact

ht.digital

Digital Assets Are Broader Than Cryptocurrency

The webinar began by clarifying that digital assets cover a wider range of products and rights than cryptocurrencies alone. Blockchain technology can be used to represent value, ownership, access rights and real-world assets in digital form.

The categories discussed included:

Payment or exchange tokens

Including Bitcoin and Ether

Stablecoins

Designed to maintain a reference value, commonly against a fiat currency or reserve asset

Security tokens

Representing rights linked to equity, debt, funds or other real-world assets

Utility tokens

Providing access to a product, service or platform

Non-fungible tokens

Representing unique items, rights or identifiers

Terminology and legal classification can differ between jurisdictions. Firms should therefore avoid relying on labels alone. They need to understand what the asset represents, the rights attached to it, how it is issued and transferred, and which regulatory and accounting treatment follows from those facts.

Why Digital Asset Readiness Matters

Digital assets are moving beyond isolated proofs of concept. Traditional financial institutions, digital-native firms and professional services providers are increasingly exploring production use cases, while regulatory frameworks and industry guidance continue to develop.

Readiness is not simply a question of whether a firm understands blockchain. It is whether the firm can demonstrate that its governance, systems, records and controls are capable of supporting the activity. This matters to the business itself, its board, its auditor, its service providers and the regulator.

For Jersey's financial services sector, tokenisation is particularly relevant because existing funds, securities and other real-world assets can be represented and administered using blockchain-based infrastructure. The potential opportunity is significant, but adoption depends on firms being able to evidence ownership, reconcile data, manage custody risks and produce reliable financial reporting.

What Makes Digital Asset Audit Different

The panel highlighted several inherent risks that are more prominent in digital asset activity:

Price volatility

Which can create valuation and impairment challenges

Irreversible transactions

Which make prevention and authorisation controls especially important

Pseudonymity

Which can obscure the identity behind a wallet address

Private key failure

Including loss, theft, copying or unauthorised access

Custody failure

Particularly where assets are held by a third party or within an omnibus structure

Regulatory uncertainty

And differences between jurisdictions

Fraud risk

Involving the loss, misappropriation or manipulation of digital assets

These risks affect familiar financial statement assertions, including existence, rights and obligations, completeness, accuracy, cut-off, classification and valuation. The audit objective has not changed, but the nature and source of the evidence may be different.

Information Technology Controls Are the Foundation

Digital asset data commonly moves from a blockchain through extraction or reconciliation software, into a subledger and then into the general ledger. If the systems and interfaces in that chain are not controlled, management and the auditor may be unable to rely on the information they produce.

The panel identified two recurring weaknesses in information technology general controls:

Change management

Poor separation between development and approval, undocumented changes, insufficient testing, or weak separation between test and production environments

Access management

Weak password standards, inappropriate user access, poor joiner and leaver processes, or a lack of periodic access reviews

Effective controls should include clear approval responsibilities, documented change requests and testing, controlled deployment, appropriate user provisioning and de-provisioning, and regular reviews of access to critical systems and wallets.

The practical consequence is important. If these controls fail, data generated by the entity's systems may not be reliable for audit purposes. This can make the audit slower, more expensive and more dependent on substantive testing or alternative evidence.

Core Management Controls

The webinar outlined six control areas that firms should consider when transacting in or holding digital assets.

1

Transaction Authorisation

Transactions should be approved by appropriately authorised people before execution. The policy should define signing thresholds, segregation of duties, approval evidence and the treatment of urgent or exceptional transactions. Multi-signature and multi-party computation arrangements can embed elements of dual control, but the underlying governance still needs to be understood and tested.

2

Blockchain Monitoring

Relevant wallet and smart contract activity should be monitored. Unusual, unauthorised or unexpected transactions should be identified, investigated and resolved promptly.

3

Data Extraction

Management should use reliable tools and documented processes to extract balances and transactions from the relevant blockchain. The firm should know which networks, addresses, smart contracts and data sources are in scope.

4

Reconciliation

On-chain balances and transactions should be reconciled to internal books and records. Controls should cover the completeness and accuracy of source data, mapping to the chart of accounts, breaks, stale items and evidence of review.

5

Cut Off

Digital asset markets operate continuously. Firms need a clear policy for the reporting cut-off, including the relevant time zone and period-end block, and should apply it consistently. Transactions are not limited to ordinary business hours, so conventional end-of-day assumptions may not be sufficient.

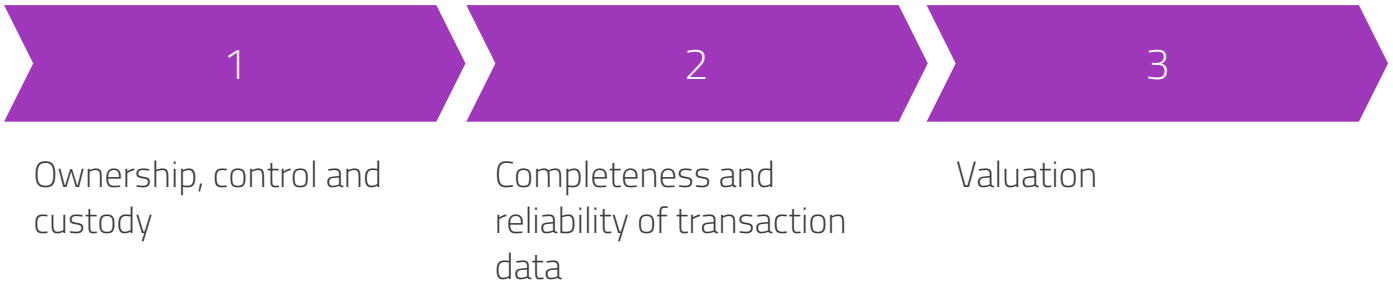
6

Classification and Measurement

Controls should support the correct classification and measurement of each asset and transaction. This requires an understanding of the asset's contractual rights, purpose, market activity and applicable reporting framework.

The Three Areas That Drive the Audit

The panel grouped the main audit considerations into three connected areas:



Weakness in one area often affects the others. For example, a firm may have a complete on-chain transaction history but still be unable to prove that it controls the wallet. It may prove ownership and completeness but still lack a defensible period-end price for an illiquid token.

Ownership, Control and Custody

The key question is whether the entity owns and controls the digital assets recorded in its financial statements. A public blockchain can show that an address exists and contains a balance, but it does not ordinarily identify the legal owner or demonstrate exclusive control.

Private keys are central because the party able to use the key can move the assets. If a key or key shard has been copied, disclosed, lost, compromised or transferred, the entity may not have sole control even if the balance remains visible on-chain.

Self Custody

Under self-custody, the entity manages its own wallets and private keys. The audit may therefore need to consider the entity's controls over:

- Wallet and key generation
- Secure storage and backup
- Access to keys or key shards
- Transaction initiation and approval
- Recovery procedures
- Changes in authorised personnel
- Reconciliation between wallets and accounting records

Evidence of control may include a cryptographic message signed by the wallet or a controlled transfer of a small, auditor-specified amount. These procedures can demonstrate an ability to use the key, but they should be considered alongside governance and key-management evidence.

Third Party Custody

Where a regulated or professional custodian holds the assets, the risk of key loss or theft moves into the custodian's control environment. Relevant evidence may include:

- The custody agreement and terms governing client ownership and transaction authority
- A direct balance confirmation or account statement
- Reconciliation to the entity's books and records
- An appropriate service organisation assurance report, such as a SOC 1 Type 2 report, where available and relevant

A confirmation alone may not address every risk. The auditor needs to understand the custody model, the controls covered by the assurance report and the records supporting the client's entitlement.

Segregated and Commingled Wallets

A segregated wallet address can provide a clearer link between a client's holdings and an on-chain balance. In a commingled or omnibus wallet, the blockchain shows the total balance but not each customer's allocation.

For commingled arrangements, assurance relies more heavily on the custodian's allocation records, reconciliation processes, client statements, confirmations and control reports. The evidence is stronger where a provider can also link the client's internal allocation to a distinct on-chain address or auditable sub-account structure.

Multi Signature and Multi Party Computation

Multi-signature arrangements require a defined threshold of signatures before a transaction can be authorised. Multi-party computation splits the signing process across separate key shares so that no single person holds the complete key.

Both can support dual control. However, multi-party computation may appear as a normal single signature on-chain. The design cannot therefore be verified from blockchain data alone and may require controls testing or provider assurance.

Completeness and End to End Reconciliation

Completeness risk arises because transactions may occur across multiple wallets, blockchains, exchanges, protocols, custodians and off-chain systems. Data can be omitted, duplicated, misclassified or recorded in the wrong period as it moves from the blockchain into the financial statements.

The firm should map the complete transaction lifecycle. This may include:

- Originating and destination wallets
- Smart contracts and protocol addresses
- Exchanges, custodians and decentralised venues
- Fees, staking rewards, collateral and redemptions
- Fiat on-ramps and off-ramps
- Data extraction tools and subledgers
- The accounting rules used to post into the general ledger

The panel described a practical case in which a client's protocol trading fees were switched on without an established accounting structure. The team used test transactions and an end-to-end flow-of-funds analysis to identify relevant smart contracts, treasury addresses, collateral mechanics, redemption routes and operational disbursements.

The wider lesson is that firms should not begin with the accounting entries alone. They should first establish what happens operationally, which systems and addresses are involved, and how each event is captured.

Reliability of Blockchain Data Sources

Free public block explorers are useful, but they are not automatically reliable audit evidence. They may not be independently tested, may lack historical point-in-time functionality, can lag protocol changes and may cease operating during an engagement.

A more defensible approach may include:

- Using an independently tested data tool or subledger
- Corroborating balances and transactions across at least two genuinely independent sources
- Confirming that apparently separate data sources are truly independent
- Querying the historical balance at the reporting date or relevant block
- Running a node where the scale, risk and cost justify it

Running an internal node may provide more direct access to blockchain data, but it can be expensive and operationally demanding. The panel's view was that firms should apply a proportionate cost and benefit assessment rather than assume every auditor or business must build this capability internally.

Valuation Considerations

The principal valuation judgement under IFRS 13 is the market used to determine fair value. A firm should not automatically use the exchange on which it usually trades. It should assess the principal market, or in the absence of one, the most advantageous market that the entity can access.

Consistent Measurement Time

Because digital asset markets do not close, firms need a documented and consistently applied valuation time. Midnight UTC is one possible convention, but another time may be appropriate if it is clearly defined and used consistently. A small deviation may not always change the reported value materially, but it can indicate that the underlying control is not operating as designed.

Price Source Reliability

Volume and pricing data can be unreliable or manipulated. Firms should assess the quality and independence of pricing sources and corroborate material valuations where possible.

Liquid and Illiquid Assets

Widely traded assets may have observable prices on active markets. Tokenised real-world assets, private market interests, thinly traded tokens and non-fungible tokens may require Level 2 or Level 3 inputs and a bespoke valuation approach. A valuation specialist should be considered where the exposure or judgement is material.

Tokenisation Does Not Create Liquidity

Representing a private or illiquid asset as a token does not automatically create market demand. Valuation still needs to consider trading venue, transfer restrictions, market participants, transaction volume and the depth of the secondary market.

The value of a tokenised interest may be informed by the underlying asset, but the token's own rights, liquidity and market conditions also matter. Digital availability and fractionalisation do not by themselves justify a higher value.

Accounting and Reporting Considerations

There is no single global accounting answer for all digital assets. The appropriate treatment depends on the reporting framework, the characteristics of the asset and why the entity holds it.

IFRS

The session highlighted the following possible treatments:

- IAS 38 Intangible Assets may apply to many cryptocurrency holdings. The cost or revaluation model may be relevant, subject to the standard's requirements and the existence of an active market.
- IAS 2 Inventories may apply where cryptoassets are held for sale in the ordinary course of business. Broker-traders may be able to use fair value less costs to sell through profit or loss.
- IFRS 9 Financial Instruments may apply where the token gives a contractual right to cash or another financial asset. This is less common for mainstream cryptocurrencies but may be relevant to some stablecoins or asset-backed tokens.

The speakers also noted the asymmetric effect that can arise under the IAS 38 revaluation model, with some decreases recognised in profit or loss and increases generally recognised through other comprehensive income and the revaluation surplus, subject to the standard's detailed requirements.

UK GAAP

Under FRS 102, the session referred to Section 18 for intangible assets, including cost less amortisation and impairment, with revaluation dependent on the existence of an active market. Impairment considerations under Section 27 may also be relevant.

US GAAP

The panel referred to the dedicated fair value model introduced by ASU 2023-08 for in-scope cryptoassets. The scope is specific and may exclude some wrapped tokens and non-fungible tokens. This may be relevant where a Jersey entity reports into a US parent or group.

Disclosures

Financial statement disclosures should explain the accounting policy, significant judgements, valuation methodology, material concentrations, custody arrangements and relevant risks. Firms should also consider related-party disclosures where transactions involve connected parties.

Accounting guidance continues to evolve, particularly for assets such as stablecoins and tokenised instruments. Complex or material positions should be assessed with appropriate specialists.

Questions Addressed in the Webinar

How Can a Firm Prove Wallet Ownership and Control

The evidence depends on the custody model. For third-party custody, firms may use contractual terms, confirmations, statements and relevant assurance reports. For self-custody, evidence may include controls over key generation and storage, a signed message or an auditor-directed transfer.

No single item of evidence necessarily resolves the full question. Firms should distinguish the ability to transact from the legal ownership of the assets and the exclusivity of control.

What Evidence Is Needed for a Commingled Wallet

Where an on-chain wallet contains assets for many customers, the client's balance cannot usually be identified from the blockchain alone. Supporting evidence may include customer allocation records, reconciliations, statements, confirmations and a relevant SOC 1 Type 2 report. Providers that can link internal allocations to auditable on-chain sub-accounts may offer stronger evidence.

Is One Free Block Explorer Enough

Generally, one free source is difficult to defend for material audit evidence. Firms should consider an independently tested tool or compare results from multiple independent sources.

Should Firms Run Their Own Node

Running a node can provide direct data, but the build, maintenance and query capability can be costly. It may be appropriate for larger firms or higher-risk engagements, but it is not necessarily proportionate for every business.

How Should Staking Rewards Be Considered

The starting point is to understand the entity's rights to the rewards and when those rights arise, even if the rewards cannot yet be claimed. The analysis should then consider contractual lock-ups, protocol mechanics, technological restrictions and the applicable accounting framework.

How Should a Tokenised Real World Asset Be Valued

The underlying asset remains important, but the analysis should also consider the legal rights represented by the token, accrued returns, transfer restrictions, listing venue, market participation and liquidity. Tokenisation does not remove the valuation challenges of the underlying private asset and may introduce additional market-specific adjustments.

Practical Next Steps for Businesses

Define the activity and asset

Document what each token represents, how it is used and which legal and economic rights attach to it.

Map the operating model

Identify every wallet, custodian, exchange, protocol, smart contract, data tool, subledger and accounting system.

Confirm the custody model

Establish who controls the keys, how transactions are approved, how access changes are managed and how assets can be recovered.

Assess information technology controls

Review access management, change management, segregation of duties and the reliability of interfaces.

Build end-to-end reconciliations

Reconcile on-chain activity through to the general ledger and investigate all breaks.

Set a cut-off policy

Define the reporting time, time zone and period-end block consistently.

Establish defensible data sources

Assess the reliability and independence of explorers, data vendors and subledgers.

Document the valuation approach

Identify the principal market, pricing sources, liquidity assumptions and the need for specialist input.

Determine the accounting treatment

Assess each asset against the applicable reporting framework and document significant judgements.

Prepare the disclosures

Explain policies, judgements, valuation methods, concentration, custody and connected-party considerations.

Engage auditors and specialists early

Resolve evidence gaps before the reporting deadline rather than during final audit testing.

Start proportionately

Pilot a defined activity, learn from the control and reporting requirements, then scale with governance.

Jersey Opportunity

Digital asset readiness builds on Jersey's established strengths in governance, administration, audit and professional services. The core disciplines remain the same, but firms must understand how they apply when ownership is represented by keys, transactions operate continuously and data comes from a blockchain.

Firms that build capability now will be better placed to support digital-native businesses, tokenised funds and real-world asset structures. This requires internal knowledge, adapted onboarding and controls, credible technology and custody partners, and specialist input where risks or accounting judgements are material.

Digital assets are not risk-free, but the risks can be identified, governed and evidenced through proportionate, disciplined risk management.

Top 10 Takeaways

01

Digital asset readiness depends on robust evidence, controls and reliable reporting.

02

On-chain balances alone do not prove legal ownership or exclusive control.

03

Audit priorities are ownership and custody, data completeness and valuation, with evidence tailored to the custody model.

04

Reliable reporting requires assessed data sources, consistent cut-off times, defensible pricing and strong reconciliations.

05

Established audit and accounting principles still apply, supported by professional scepticism and specialist advice where needed.

Disclaimer

This summary is provided for general information only and reflects themes discussed during the webinar. It does not constitute accounting, audit, legal, regulatory, tax, financial or investment advice. Firms should obtain appropriate professional advice based on their circumstances, reporting framework and proposed digital asset activities.

Nathan de la Haye - nathan.delahaye@digital.je

www.digital.je

www.fintech.je