# CONSIDERATIONS FOR AUDITING CRYPTOCURRENCIES

19 September 2024

This publication highlights common risks in the audit of cryptocurrencies and provides examples of procedures that can be performed to address these risks. It is not intended to be a guide, and it does not provide a comprehensive list of risks or audit procedures.

## CONTENTS

## INTRODUCTION

The term 'crypto assets' encompasses a wide range of virtual assets which reside on a blockchain and are cryptographically secured and controlled. The type of blockchain on which a cryptocurrency resides will affect the audit risks and procedures to be performed when auditing it. For example, with a permissionless blockchain network getting data may be more straightforward as data is publicly available and easier to access. However, as there is no verification of participants, transactions and wallet balances may be pseudo-anonymous, limiting transparency. Conversely, for cryptocurrencies on private and permissioned blockchains anonymity is typically less of a challenge. A high-level overview of blockchain technology is provided in Appendix 1.

Crypto assets can be broken down into various categories including asset backed tokens (ABTs), non-fungible tokens (NFTs), security tokens, utility tokens, cryptocurrencies (including stablecoins), and central bank digital currencies (CBDCs).

While these categories are distinct, there are similarities and differences in the nature of the assets, which may impact audit risks and procedures. For example, many digital assets have similar risks relating to proof of ownership and control and valuation. However, audit procedures to obtain evidence to address these risks may be different.

In addition, individuals and organisations can interact with digital assets in various ways including holding, providing custodian services, payments, trading, staking, and mining. The nature of the interaction will determine the associated audit risks and procedures.

The focus of this publication is the audit of cryptocurrencies, and entities that:

- hold (either directly, or indirectly through a custodian), and/or trade cryptocurrencies;
- provide cryptocurrency exchange services; or
- are exposed to cryptocurrencies indirectly – for example by holding cryptocurrency related exchange-traded funds (ETFs).

It does not specifically address the audit of stablecoins, although there are elements that may be relevant because stablecoins are cryptocurrencies.

All other digital assets, including CBDCs, NFTs, security tokens and utility tokens are not discussed. Neither is the audit of entities involved in mining or staking cryptocurrencies. While some elements of the audit of entities providing custodian services are touched upon, such as safeguarding considerations, coverage is not comprehensive and areas such as segregation of assets and ability to meet client obligations are not covered.

This is not an authoritative guide to the audit of cryptocurrencies. It does not contain a comprehensive list of the risks, or the audit procedures to be performed. Its purpose is to introduce the concepts behind cryptocurrencies, highlight important ethical considerations and common risks associated with auditing them, and share examples of procedures that can be performed to address them.

All auditing activities take place in the context of relevant auditing and ethical standards. The International Standards on Auditing - ISAs (UK and Ireland) referred to in this publication are those issued by the UK's Financial Reporting Council (FRC), based on the auditing standards published by the International Auditing and Assurance Standards Board (IAASB). The ethical standards referred to are the FRC's Ethical Standard and the International Ethics Standards Board of Accountants' Code of Ethics for Professional Accountants (the IESBA Code).

## ETHICAL CONSIDERATIONS

Ethical considerations are a key part of any audit. ISA (UK) 200 *Overall Objectives of the Independent Auditor and the Conduct of an Audit in Accordance with International Standards on Auditing (UK)*, makes it clear that an ISA-compliant audit requires compliance with 'relevant ethical requirements' (Para. 14) which include the Financial Reporting Council (FRC)'s Ethical Standard and the IESBA Code.

The IESBA Code establishes the principles of integrity, objectivity, professional competence, due care, confidentiality and professional behaviour (111.1 A1) which are fundamental to auditors conducting an audit of any financial statements.

Professional competence is particularly important when contemplating an audit of an entity involved in the fast-evolving world of cryptocurrencies. This is because such assets can be complicated to both account for and audit and require knowledge of concepts such as blockchains.

If the audit firm is engaged by the entity to perform any non-audit cryptocurrency-related work, such as valuation work, in addition to the financial statement audit, a self-review threat arises if auditors intend to use that work when forming a judgment relevant to the audit engagement (defined in IESBA Code (120.6 A3) and the FRC Ethical Standard (1.33)).

The identification of ethical risks and necessary steps to reduce or eliminate them are commonly achieved through a firm's quality management processes and are the responsibility of the firm's ethics partner.

The fundamental principles and threats are kept in mind at all stages of the audit.

## RISK ASSESSMENT

The cryptocurrency ecosystem is a dynamic environment that presents specific risks and audit challenges. Those challenges include gathering sufficient, relevant data and understanding the complex IT and business environments of entities in the ecosystem. Auditors take care to understand the potential dangers and demanding situations when devising an appropriate methodology to identify and assess the risks of material misstatements.

In performing the risk assessment, auditors consider ISA (UK) 315 *Identifying and Assessing the Risks of Material Misstatement* (Para. 19 – 27), which requires auditors to obtain a sufficient understanding of the entity and its environment, together with its risk assessment procedures and wider processes and controls.

In assessing audit risks, auditors follow a process that begins with considerations before accepting an audit engagement and ends with the finalisation of the audit.

### Understanding the entity

To obtain an understanding of the entity and its environment, auditors gather records that relate to the entity's strategy, operations, internal controls, and its role in the cryptocurrency ecosystem.

Enquiries auditors may make of management and other relevant parties to better understand the nature of the entity and its environment include but are not limited to the following questions.

- What is the entity's motive related to holding and transacting in cryptocurrencies?
- What type(s) of asset(s) does the entity hold, how did it acquire them and what controls does it have in place to safeguard them? How does the entity maintain custody of the assets? Does it use a third-party custodian?
- If the entity does use a third-party, what sort of checks does it run to assess the third-party's systems and controls? (ISA (UK) 402 Audit Considerations Relating to an Entity Using a Service Organization (Para. 9))
- What type(s) of wallet(s) does the entity use to hold the cryptocurrencies?
- What controls does management have in place for wallet management – ie, access and key generation process?
- What is the nature, frequency, volume, and value of the entity's cryptocurrency transactions?
- How does the entity reflect on- and off-chain transactions in its books and records?

### Entity's risk assessment

Enquiries auditors may make of management and other relevant parties to help better understand the entity's risk assessment process include but are not limited to the following.

- Management's policies, procedures, and other information relevant to cryptocurrencies (ie, the processes for onboarding new assets and engaging with exchanges).
- Management's policy for identifying objectives and risks related to cryptocurrencies, as well as the approach to assessing and mitigating those risks.
- Management's policies and procedures for ensuring that appropriate due diligence and anti-money laundering checks are performed on relevant counterparties in the cryptocurrency space. As part of risk assessment procedures, auditors obtain an understanding of the legal and regulatory framework applicable to the entity and its industry, including how the entity is complying with that framework (ISA (UK) 250 (Para 13)).
- Processes for identifying new risks in a timely manner, including those related to changes in applicable laws and regulations that affect compliance.

- Processes for identifying new risks related to changes in blockchain technology that affect the safeguarding of the cryptocurrencies.

It is necessary for management to be able to identify the unique risks posed by cryptocurrencies and to implement appropriate processes and controls to mitigate them. However, that may be impeded by the attractiveness of the cryptocurrency market, due to its apparent ease of entry to those who may lack the required competence.

Another consideration when assessing the robustness of management's risk assessment process is that, even when management possesses an appropriate level of technical capability in cryptocurrency technologies, that competence may not necessarily indicate that they are equally capable in relation to financial reporting.

### Wider processes and controls

Auditors obtain an understanding of the entity's wider processes and controls, relevant to its engagement with cryptocurrencies.

#### Transacting in cryptocurrencies

The principles, methods, and controls linked to transacting in cryptocurrencies are often most relevant to rights and obligations, occurrence, and completeness assertions. Categories of assertions are defined by ISA (UK) 315 (Para. A190). It is critical for the entity to set up appropriate methodologies and controls focused on key aspects of cryptocurrency transactions, such as authorisation of transactions by appropriate individuals and counterparty identification procedures. A non-exhaustive catalogue of such control activities can be found in Appendix 3 of ISA (UK) 315 (Para. 20).

Due to the characteristics of cryptocurrencies, auditors keep in mind the manner in which management and those charged with governance have tailored the entity's controls 'considering the nature and complexity of the entity' (ISA (UK) 315 (Para. 21)). The controls consider potential extra risks and issues regarding relevant cryptocurrencies. These may encompass areas such as the entity's methodology for assessing risks presented by the purchase and transaction of cryptocurrencies, and the monitoring of controls as new assets with new properties are added to the entity's portfolio.

Reporting virtual asset transactions entails the following procedures:

- monitoring cryptocurrency transactions on the blockchain;
- assessing the reliability of blockchain records, and strategies for extracting blockchain information;
- determining the appropriate classification and size of virtual-asset transactions; and
- determining a suitable cut-off for cryptocurrency transactions.

The decentralised nature of the blockchain means that cryptocurrency transactions are not necessarily restricted to normal business hours and can vary in the speed at which they are processed. Careful consideration of potential cut-off issues is warranted. As part of auditors' risk assessment processes, performed in accordance with ISA (UK) 315, auditors assess how management records transactions and balances of cryptocurrencies in its books and records, in the interests of completeness, accuracy, and classification. That would involve obtaining an understanding of 'how information flows through the entity's information system' (ISA (UK) 315 (Para. 25)), including the methods used to extract relevant information from the blockchain, and any risks involved in the process.

Management enquiries to aid auditors' knowledge may consist of the following:

- How does the entity assess the reliability, integrity, and availability of information obtained from the blockchain?
- How does management confirm accuracy in the preparation of cryptocurrency reconciliations?

- What controls are in place to support completeness and accuracy of data used in the reconciliations?
- How does management record cryptocurrency transactions and balances in its books and records?
- How does management verify the reliability of information acquired from a third party when cryptocurrency transactions are not processed on a blockchain?
- What volume of public addresses does the entity control for each cryptocurrency, and how are cryptocurrency balances dispersed among the public addresses?
- How does management validate that each cryptocurrency transaction is authorised by an appropriate individual?
- How might management realise if a security breach has occurred that would compromise the entity's keys?
- What tools are used to extract transactions and balances from each relevant blockchain?
- How does management consider the reliability of each relevant blockchain and the entity's chosen data-extraction tools?
- To what extent do the blockchain's parameters make it difficult to determine a point-in-time balance (ie, privacy coins)?
- How does management identify related-party transactions on the blockchain? Auditors' responsibilities when gaining an understanding of related-party relationships and transactions of an entity are clarified by ISA (UK) 550 Related Parties (Para. 12 – 14).

### Safeguarding

Demonstration of ownership and control of private keys is an important element for confirming ownership and control of cryptocurrencies. Developing procedures and controls that mitigate the danger of inappropriate access to those keys presents challenges.

Methods of safeguarding private keys can include:

- use of multi-signature addresses which require more than one signature or private key to authorise and process cryptocurrency transactions;
- encryption of private keys;
- security procedures surrounding key generation; and
- physical security of the facilities and infrastructure for storing the private keys.

Relevant information for auditors to consider include information about the initial key-generation process, backups, access to perform transactions, and segregation of duties.

There are also unique fraud and related-party issues that auditors consider when performing risk assessment procedures, for entities in the cryptocurrency space (in line with ISA (UK) 315). Fraudulent financial reporting, misappropriation of cryptocurrencies and undisclosed related-party transactions may be facilitated due to the particularities of private keys and the pseudonymous nature of blockchain records, which can obscure the identities of counterparties and impede efforts to demonstrate that a transaction has taken place at arm's length.

Since the 'primary responsibility for the prevention and detection of fraud rests with (…) those charged with governance (…) and management' (ISA (UK) 240 *The Auditor's Responsibilities Relating to Fraud in an Audit of Financial Statements* (Para. 4)), as a first step, auditors obtain an understanding of management's own assessment of the entity's susceptibility to fraud, as well as the controls and processes in place to prevent and detect it.

Entities in the cryptocurrency space may have a heightened risk of fraud in cases where multiple parties may be able to access the same cryptocurrencies with the use of their own private keys. Management may also fraudulently record the loss or theft of private keys and subsequently

misappropriate the assets for their own benefit. The engagement discussion around the entity's susceptibility to fraud covers these specific considerations (ISA (UK) 240 (Para. 16)).

The engagement team also discusses to what extent management is incentivised or pressured to engage in fraudulent financial reporting via the execution of fictitious transactions with no business substance, aided by the pseudo-anonymity of cryptocurrency records.

Auditors obtain an understanding of the entity's relationships and transactions with any related parties that may affect the risk of material misstatement. Such considerations also form part of the engagement team's discussion (ISA (UK) 550 (Para. 12)). In addition, auditors obtain an understanding of management's controls and processes to 'identify, account for and disclose related party relationships and transactions in accordance with the applicable financial reporting framework' (ISA (UK) 550 (Para. 14)).

This is of particular importance given that the blockchain may obfuscate the identity of counterparties in a cryptocurrency transaction. Cryptocurrency transactions that are significant and fall outside the normal course of business may indicate the presence of undisclosed related parties. Auditors make enquiries of management about the nature of such transactions – and if the business rationale behind those transactions is not apparent, auditors also consider the potential that the financial statements may be misstated due to fraud.

The possibility of self-dealing and 'round tripping' – whereby the entity fraudulently reports higher numbers of sales and purchases of cryptocurrencies by selling and buying back the same or similar assets at the same price – are further, potential risks.

Any discussions, whether with the team or management, are appropriately documented in line with the provisions of ISA (UK) 230 *Audit Documentation*.

### Cryptocurrencies held on behalf of clients

Companies that keep cryptocurrencies on behalf of others, as well as their own, need to have in place processes and controls to:

- track client balances separate from their own balances in cases where they are commingled in the reconciliation process;
- onboard new clients;
- authorize and monitor cryptocurrency transactions; and
- affirm that sufficient cryptocurrencies are held to satisfy client obligations.

### Cryptocurrencies held via third parties

An entity may use a third party to maintain custody of its cryptocurrencies, or of any cryptocurrencies it holds on others' behalf. In such circumstances, the entity is responsible for ensuring that the third party has designed appropriate controls related to cryptocurrency safeguarding and any other relevant processes that exist at the third party. As ISA (UK) 402 (Para A11-1) indicates, 'use of a service organization does not diminish the ultimate responsibility of those charged with governance (…) for conducting its business in a manner which meets their legal responsibilities, including those of safeguarding (…) assets.' The existence of a Service Organisation Controls (SOC) report, as defined by this ISA (Para. 8), may provide some evidence regarding the effectiveness of the controls in place to deal with the relevant risks.

Auditors enquire of management and those charged with governance, whether any cryptocurrencies belonging to the entity are held on other platforms outside the entity's control. Auditors also obtain an understanding of how the entity utilises any third-party service organisations in its operations, including the nature of the services provided, their significance to the entity, and the nature of the relationship between the entity and the third party. That includes relevant contractual terms for the activities that the third party has undertaken (ISA (UK) 402 (Para. 9)).

In obtaining an understanding of controls implemented by the entity over third parties, auditors may consider the following questions:

- Who is the person initiating and authorizing transactions with the third party?
- What processes does the entity have in place over such initiation?
- How are transactions with the third party recorded and reconciled in the entity's accounting records?
- How does the entity validate that the third party maintains control of the cryptocurrencies in its custody, particularly when cryptocurrencies are commingled?
- How does the entity monitor the effectiveness of the third party's internal controls?
- How does the third-party conduct risk assessments of clients, including AML checks?

Further guidance specific to considerations around the nature of transactions processed by third parties as well as the degree of interaction between third parties and the entity is set out in ISA (UK) 402 (Para. A6 – A8).

Some of the larger custodians in the market currently issue International Standard on Assurance Engagements (ISAE) 3402 or US-style Type 1 SOC reports relating to controls at service organisations. However, many custodians are not issuing these for the foreseeable future. As such, auditors consider alternative procedures to gain sufficient, appropriate audit evidence for those balances. Type 2 SOC reports, covering applicable trust-principle criteria with a focus on technology and cybersecurity, are currently more popular with custodians. While the purpose of such reports is not to satisfy a financial reporting objective, there may be sufficient overlap in scope that enables an auditor to obtain some audit evidence relating to certain controls in those reports. If no published report exists, auditors consider exercising 'right to audit' clauses that may be included in the contract between the audit entity and the service organisation to perform controls testing directly at the service organisation as explained in ISA (UK) 402 (Para A30).

If the above channels are exhausted, auditors are required to consider the effect on the audit report, if sufficient, appropriate audit evidence cannot be obtained to address the assessed risks of material misstatement regarding a third party. That includes a 'limitation of scope,' as per the provisions of ISA (UK) 705 *Modifications to the Opinion in the Independent Auditor's Report* (Para. 19).

## SPECIFIC RISKS

This section builds on the risks covered in the risk assessment section above and explores in more detail some common risks related to cryptocurrencies and provides example procedures that auditors can perform to address them. However, it is not a comprehensive list of risks or audit procedures.

### Onboarding

Relevant risks are considered when onboarding new entities that hold cryptocurrencies, as well as for existing audited entities that have become holders of cryptocurrency. Risk considerations might also apply to entities – whether existing clients or new – that are dealing with cryptocurrencies without 'touching' them, for example, through net settling in cash.

Firms exercise caution and consider the specific risks and challenges before attempting to conduct audits of entities in this space. ISQM (UK) 1 *Quality Management for Firms that Perform Audits* or *Reviews of Financial Statements*, or *Other Assurance or Related Services Engagements* (ISQM (UK) 1) emphasises a 'risk-based approach', which considers 'the nature and circumstances' of the firm, and of 'the circumstances of the engagements performed by the firm'. (Para. 10).

Previous and existing risk assessment, risk management and onboarding procedures may not be adequate to cover the take-on risks associated with cryptocurrencies. As such, a review and update of those processes may be necessary, and may include, for example, the extension of existing questionnaires to include questions relevant to cryptocurrencies, or the inclusion of specialist review.

#### Auditor competencies and skillsets

Due to the mechanics of blockchain technology, auditors ensure that engagement teams have sufficient 'competence and capabilities' (ISQM (UK) 1 (Para. 32) and ISA (UK) 220 (Para. 26)) to understand how entities are using the technology, and to identify the risks of material misstatement and the internal controls that address these risks. Furthermore, audit evidence may be in electronic format and therefore 'obtaining audit evidence about the accuracy and completeness of the information' is important (ISA (UK) 500 (Para. 9)).

Three components considered when making the acceptance decision are a firm's current industry experience, its understanding of cryptocurrencies, and its understanding of how they are being used by the entity in the environment in which it operates.

In accordance with ethical standards, ISA (UK) 220 Quality Management for an Audit of Financial Statements (Para. 26) and ISQM (UK) 1 (Para. 32), the firm's ability to perform the engagement depends on auditors possessing 'the appropriate competence and capabilities', which includes knowledge of all three components. To make an informed acceptance decision, auditors evaluate each component.

Firms consider whether existing staff qualifications and certifications remain appropriate for undertaking this type of engagement, or whether additional training, qualification or certification may be necessary. They also consider whether engagement teams are given 'sufficient time' to perform quality engagements involving cryptocurrencies (ISA (UK) 220 (Para. 26) and ISQM (UK) 1 (Para. 32)).

Firms may update, or add, additional oversight to current systems of quality management. For example, more consideration and attention may be given to determine whether the auditor has sufficient employees with the necessary competence and capabilities, 'relevant to the engagements the firm performs', including those relevant to the cryptocurrency ecosystem (ISQM (UK) 1 (Para. 32)). If firms intend to pursue audit work for entities participating in the ecosystem, and recruitment and training programs do not currently contemplate issues particular to that ecosystem, more thought and attention may need to be given to adding such programs to help audit staff 'develop and maintain the appropriate competence' (ISQM (UK) 1 (Para. 32)).

The following are procedures that firms may carry out as part of the acceptance process for engagements involving cryptocurrencies.

- Specify the types of entity or engagements the firm can accept in the cryptocurrency ecosystem, with reference to ISQM (UK) 1's risk-based approach to engagement acceptance.
- Establish firm-wide focus areas or engagement-acceptance standards for entities in the ecosystem for cryptocurrencies.
- Implement training initiatives to familiarise personnel with the risks and issues that may arise during the engagement.
- Develop a general understanding of the risks present in the cryptocurrency ecosystem among firm employees, to raise levels of awareness of those risks and the resources available for ongoing engagements.
- Provide relevant firm personnel with consultation tools, training, continuing professional development, work experience or coaching (ISQM (UK) 1 (Para. A88) and ISA (UK) 220 (Para. A68)).
- Reassess on an annual basis the continuance of an engagement, depending on evolving information and circumstances.
- Identify a person, or people – either from within or outside the firm – with the required knowledge to participate in engagement-acceptance decisions.

Firms also determine whether they intend to use and have access to reliable tools for the audit. For any tools to be used, firms perform relevant procedures relating to their reliability (see the section on risks around accuracy of data).

### Management's competence and responsibility

As blockchain technology and cryptocurrencies can be very complicated, firms take steps to ensure that senior staff at the entity have the right skills and abilities. There is a risk that the entity's management team may not know how to maintain adequate controls, including record-keeping.

The complexity of the underlying technology and the unique risks and related audit challenges in gathering 'sufficient, appropriate audit evidence' (as defined in (ISA (UK) 500 Audit Evidence (Para. 5)) means that auditors determine whether the entity's management can prepare and take responsibility for the 'preparation of the financial statements in accordance with the applicable financial reporting framework including where relevant their fair presentation' and 'for such internal control as management determines is necessary to enable the preparation of financial statements that are free from material misstatement'.

The acknowledgement of those responsibilities by management is a precondition for an audit (ISAs (UK) in ISA (UK) 200 (Para. 4) and ISA (UK) 210 (Para. 6)). Even if management and those charged with governance are honest and have good intentions, an audit may not be possible if they do not have the necessary skills, or the entity has not kept good records or had the right processes and controls in place. Internal controls – including controls over information technology – have a direct effect on the auditability of the underlying financial activity. As such, auditors may expand traditional acceptance procedures to understand those challenges.

An audit may also not be possible if the entity has sought to rely on the auditors' judgement. That scenario could make it hard for auditors to give an independent opinion on the financial statements or provide other forms of assurance, since 'the concept of an independent audit requires that auditors' roles do not involve taking responsibility for the preparation of the financial statements or for the entity's related internal control' (ISA (UK) 210 *Agreeing the Terms of Audit Engagements* (Para. A11)).

### Management's integrity

Auditors demonstrate that they have considered the 'integrity and ethical values' of management and have "obtained information about the nature and circumstances of the engagement and the integrity and ethical values of the client" in deciding whether to accept or continue a client relationship or specific engagement (ISQM (UK) 1 (Para. 30) and ISA (UK) 220 (Para. A50)).

Examples (as listed in ISQM (UK) 1 (Para. A68)) of such considerations include, but are not limited to:

- management's reputation and background;
- the nature of the entity's operations;
- indications of money laundering or other criminal activities; and
- any other indications as to limitation of scope.

Given the ways in which cryptocurrencies, aided by the pseudo-anonymity of some blockchain records, can be used to facilitate criminal activity – including financing terrorism and money laundering – it is of particular importance that auditors be alert to the possibility of actual or suspected non-compliance with laws and regulations in line with ISA (UK) 250 Section A *Consideration of Laws and Regulations in an Audit of Financial Statements*. This includes Anti Money Laundering (AML) and Know Your Client (KYC) regulations. Systems for compliance with these regulations may be relatively immature in, for example, exchanges where cryptocurrencies are traded for fiat (ie, traditional) currencies such as GBP.

As always, auditors maintain professional scepticism throughout the audit 'recognising the possibility of a material misstatement due to facts or behaviour indicating irregularities, (...) notwithstanding their past experience of the honesty and integrity of the entity's management (...).' (ISA (UK) 200 (Para. 15).

### Valuation Risks

Cryptocurrencies may be transacted directly between market participants. However, in practice, they are often purchased through cryptocurrency exchanges. Those exchanges enable customers to trade cryptocurrencies with counterparties in exchange for fiat currencies, or other cryptocurrencies. A key difference between a cryptocurrency exchange and a stock exchange is that a cryptocurrency exchange is often designed as a direct-to-customer platform, which typically operates without the need for intermediaries. As such, a cryptocurrency exchange can function as a broker, custodian and trading venue, all at the same time.

Cryptocurrencies are typically traded on more than one exchange, which can lead to inconsistent pricing throughout those diverse marketplaces. That may provide service companies such as those that provide custodian services with the opportunity for self-dealing (benefiting from transactions conducted on behalf of another party). Controls need to be in place to ensure that the valuation of cryptocurrencies is consistently and appropriately applied in accordance with the entity's accounting policies.

Auditors obtain an understanding of management's process for pricing cryptocurrencies to evaluate whether accounting and disclosure requirements are 'appropriate and consistent with the applicable financial reporting framework' (ISA (UK) 315 (Para. 20)). That understanding may be obtained by inspecting management's valuation policies and documentation and making enquiries of management, or those charged with governance, that address various considerations – including, but not limited to, how the entity:

- identifies the principal marketplace for each cryptocurrency;
- considers the reliability of pricing records received;
- evaluates any potential variances among prices; and

- identifies and assesses indicators of impairment in accordance with its accounting policies (where the entity applies an accounting policy that calls for assessment of asset impairment, for instance if accounted for as intangible assets).

Auditors also enquire whether any modifications were made to the entity's valuation methodology and the 'reasons for any changes thereto' (ISA (UK) 315 (Para. 19)).

The following valuation sections focus on where entities report under International Financial Reporting Standards (IFRS) and cryptocurrencies are classified such that they are measured at fair value through profit and loss. Such valuation is permissible where the assets are:

- intangible assets measured under the revaluation method in IAS 38;
- inventory under IAS 2 where the broker-dealer exemption is applied; or
- held as financial instruments and measured at fair value under IFRS 13.

Fair value is an accounting estimate, and the entirety of ISA (UK) 540 Auditing Estimates and Related Disclosures is relevant to the audit of fair values.

Other measurement approaches are permissible under certain circumstances (ie, other than fair value). However, many cryptocurrency holdings are likely to fall under one of the fair value circumstances above. As such, alternative measurement bases are outside the scope of this publication.

### Determination of the asset's principal market

Fair-value measurement typically assumes any sale of the cryptocurrency in its principal market, if one exists, or the most advantageous market, if a principal market does not exist. Determining the principal market can be challenging for the reasons set out below.

| Common challenge | Considerations |
|---|---|
| **Principal market with lower level of activity**<br><br>An entity may 'normally transact' in, and therefore have readily available pricing information for, a market such as a cryptocurrency exchange that has a lower trading volume and level of activity for the relevant asset than other markets which the entity can access. | As exchange volume and activity data for more common cryptocurrencies such as Bitcoin and Ether is generally readily available, auditors cannot assume, without undertaking further evaluation, that any exchange on which the entity primarily transacts is the entity's principal market. It may be that an entity's primary transactional market for an asset is not the asset's principal market. |
| **Multiple markets**<br><br>An entity may 'normally transact' in multiple markets for the same cryptocurrency, with no single exchange representing the market in which the entity 'normally transacts'. | An entity may not have a market to which to apply the presumption of a principal market if it regularly transacts in multiple markets for the same cryptocurrency.<br><br>If there is no readily available information about other markets accessible to the entity, and the entity therefore concludes that its primary transactional market is its principal market, it may be appropriate to consider:<br>• which of the markets in which the entity normally transacts has a greater volume and level of trading activity for the cryptocurrency in question; and<br>• if all the markets in which the entity typically transacts are of a similar size (or the relative size of those markets is not known), which market the entity would be likely to access for a hypothetical |

| | |
|---|---|
| | sale of its entire holding of the cryptocurrency on the measurement date.<br><br>Blockage factors are estimates of reductions in quoted prices of financial instrument that would occur if a market participant sold a large holding of instruments at once. Consideration of 'blockage factors' in fair value is prohibited by IFRS 13, as this is an entity-specific consideration.<br><br>Notwithstanding that blockage factors are not factored into the fair value, where entities hold cryptocurrencies as financial instruments, the circumstances which give rise to those factors may have a broader impact on an entity which has large holdings of a cryptocurrency in comparison to the market volume. As a result:<br>• Comparatively large holdings of individual cryptocurrencies represent a business risk and, as such, would likely meet IFRS 7 risk disclosure requirements.<br>• There may be additional related-party considerations, which can be particularly prevalent in the cryptocurrency sector. See the next section on other valuation challenges for further detail on related-party considerations. |
| **No access to principal market**<br>An entity may not be able to access a particular market for a cryptocurrency | The principal market for an asset needs to be accessible to the entity at the measurement date. As such, auditors consider all legal, practical and/or economic restrictions on the entity's ability to access a particular market. |
| **Changes to principal market**<br>The principal market for a cryptocurrency may change between measurement dates, given the evolving nature of the market. | Auditors review the entity's principal (or most advantageous) market conclusion whenever facts or circumstances change in ways that could affect that conclusion. |

### Other fair-value valuation challenges

While the determination of the principal market is a key challenge for fair-value measurement of cryptocurrencies, there are other fair-value challenges to consider.

| Common challenge | Considerations |
|---|---|
| **Accuracy of volume data**<br>Accurate volume and activity data may be difficult to obtain and/or be unreliable. Conflicting volume data often exists, and the cryptocurrency market has been impacted by fraudulent trading and volume data. | Auditors exercise judgment in determining the appropriateness of the entity's sources for, and reliability of, cryptocurrency volume and activity data. Market data from multiple sources is used when assessing the principal market for a cryptocurrency, and whether those sources substantially corroborate each other. |
| **Related-party considerations** | Auditors assess the impact of related party cryptocurrency transactions when reviewing |

| | |
|---|---|
| Where transactions of cryptocurrencies occur between related parties, determining an arm's length market price can be challenging. | management's determination of the fair value of cryptocurrencies. |

### Valuation risks of material misstatement and response

In accordance with ISA (UK) 315 (Para. 9), auditors may consider the valuation of cryptocurrencies as a significant risk area due to the potential presence of several inherent risk factors, such as:

- estimation uncertainty;
- subjectivity; and
- complexity.

Consequently, this requires careful assessment of the methods and assumptions used in valuation.

Examples of substantive procedures to respond to risks of material misstatement identified with respect to the valuation of cryptocurrencies are included in the table below. Disclosure considerations are not included.

| Key risks of material misstatement | Considerations | Procedures to Consider (non-exhaustive list) |
|---|---|---|
| Inappropriate initial, and/or subsequent, measurement bases selected by the entity for its cryptocurrency holding(s). | Auditors evaluate the measurement basis selected by the entity for all asset holdings.<br><br>Specifically, auditors understand the nature of the cryptocurrency holding and whether it is consistent with the measurement basis selected by the entity in accordance with ISA (UK) 540 (Para. 13).<br><br>Key considerations for determining an appropriate initial and subsequent measurement basis include the entity's cryptocurrency strategy and rationale for investing in the specific assets held, as well as characteristics of the individual assets. | • Inspect the entity's accounting policy for cryptocurrencies and evaluate it against the requirements of the applicable financial reporting framework.<br>• Evaluate whether the initial and subsequent measurement bases determined by the entity are appropriate, given the purpose and nature of the holding.<br>• Evaluate whether the principal market selected by the entity is appropriate in light of the considerations set out in the section above on determination of the asset's principal market.<br><br>Further guidance relating to an auditor's understanding of the requirements of the applicable financial reporting framework for accounting estimates is available in ISA (UK) 540 (Para. A24 – 25). |
| Fair value of assets with observable inputs is inappropriately determined. | According to IFRS 13 *Fair Value Measurement* observable inputs are those "developed using market data, such as publicly available information about actual events or transactions, and that reflect the assumptions that market participants would use when pricing the asset or liability". | • Identify the principal and active market for cryptocurrencies, where multiple marketplaces exist.<br>• Determine the measurement date and time.<br>• Obtain independent prices from market sources and compare those with the prices used by the |

| | | |
|---|---|---|
| | Where assets include largely observable inputs, auditors may compare cryptocurrency holdings against observable market prices in the principal market for that asset. As such, it may be possible to 'mass re-price' cryptocurrencies using computer assisted audit techniques. Such audit tools are appropriately tested for accuracy prior to use on audit engagements.<br><br>Auditors may also consider involving an auditor's expert in line with the provisions of ISA (UK) 620 *Using the Work of an Auditor's Expert*. | entity. As part of that procedure, auditors 'shall consider the relevance and reliability of the information to be used as audit evidence, including information obtained from an external information source.' (ISA (UK) 500 (Para. 7)).<br><br>Further guidance relating to an auditor's use of external information sources as audit evidence is provided in ISA (UK) 540 (Para. A127 – 129). |
| Fair value of assets using significant unobservable inputs, including model-based and alternative approaches, is inappropriately determined. | It is not expected that a revaluation approach would typically be followed for cryptocurrencies held as intangibles that do not have observable inputs.<br><br>Given the complexity associated with valuing level 3 (illiquid and difficult to value) assets, auditors may involve experts in determining the fair value of the cryptocurrencies in accordance with ISA (UK) 620. | • A bespoke revaluation may be required, given the cryptocurrency's nature. That would typically include understanding and evaluating the valuation methodology, and assessing whether all inputs (including relevant methods, assumptions and data) have been identified.<br>• In using the work of an expert for the purposes of the audit, as per ISA (UK) 620 (Para. 12), auditors evaluate the qualifications, skills and experience of the expert, the relevance and reasonableness of the conclusions of the expert, as well as any significant assumptions and valuation methods applied. Auditors also evaluate the completeness and accuracy of any source data involved in the valuation. Para. A33 - 39 of that standard provides examples of specific audit procedures to assist in this process. |

### Impairment considerations

Under IAS 38, cryptocurrencies held as intangibles are subject to the impairment requirements of IAS 36. Where the subsequent measurement basis the entity has selected requires an impairment test, an assessment of the entity's impairment analysis is key.

An important consideration with respect to impairment is the commingling of cryptocurrency tokens, ie, whether it is possible to analyse for impairment across cryptocurrency classes. In general, it would not be appropriate to do so as each unit (or fractional unit) of a crypto asset held by the entity is its own unit of account for assessing impairment. That is because entities can typically sell or otherwise dispose of each unit (or fractional unit) separately. As such, it is not appropriate to evaluate different crypto assets such as Bitcoin and Ether, or multiple units (or fractional units) of a single crypto asset that have different carrying amounts for impairment as a group.

When performing audit procedures to evaluate an entity's impairment assessment of cryptocurrencies, procedures auditors may perform include:

- Obtaining an understanding of the entity's policies and procedures to monitor the reasonableness and consistency of the application of impairment triggers across similar intangible assets with indefinite-lives (ISA (UK) 315 (Para. 19 – 27)).
- Obtaining an understanding of and testing the entity's approach to tracking the carrying value and acquisition date and time of the cryptocurrencies acquired in various separate or individual transactions, including how that is factored into the impairment analysis (ISA (UK) 540 (Para. 22 – 25)).
- Testing the accuracy of the cost basis and evaluating the reliability of the source of the fair-value information. For fair-value accounting estimates, guidance for auditors' consideration of the relevance and reliability of source information is provided in ISA (UK) 540 (Para. A128).

**Ownership and Control**

Risk assessment procedures are required to identify and assess the risk of material misstatement due to fraud or error and to design procedures to respond to

these risks (ISA (UK) 315 (Para. 13)). In this regard, the approach to crypto assets is no different to the audit of any other financial statement line items, albeit the risk of material misstatement for the rights and obligations assertion may be higher and may be considered significant in line with the provisions of the aforementioned standard.

Due to the inherent pseudo-anonymity of blockchain technology, obtaining sufficient, appropriate audit evidence relating to the sole ownership and control of a digital wallet will be one of the most challenging aspects of an audit of cryptocurrencies. Although the blockchain ledger may provide the public address of the transacting parties and the amount of value exchanged, the technology may not provide any information concerning the identity of the counterparty or their appropriate recognition or classification in the financial statements. As a result of this and following the provisions of ISA (UK) 330 (Para. 8), auditors test the effectiveness of certain processes and controls around cryptocurrencies, because substantive procedures alone are not usually adequate to obtain sufficient, appropriate audit evidence relating to the rights and obligations, and existence assertions.

### Confirmations

Certain operations of blockchain technology can obviate the need for third-party intermediaries for the execution of transactions. That can limit the information available to prove ownership of the cryptocurrencies (an analogy is no bank confirmations for a government issued currency). That may present certain challenges for auditors, since:

- in designing further audit procedures to be performed, auditors are required to 'obtain more persuasive audit evidence the higher the auditor's assessment of risk' (ISA (UK) 330 *The Auditor's Response to Assessed Risks* (Para. 7)); and
- audit evidence over ownership 'in the form of external confirmations received directly by auditors from confirming parties may be more reliable than evidence generated internally by the entity' (ISA (UK) 505 External Confirmations (Para. 2)).

For entities with self-custody of their cryptocurrencies, confirmations of information or balances may not be possible or appropriate, unless the source of the information provided can be shown to be independent of the source of the information being audited. Where confirmations are obtained in line with ISA (UK) 505, auditors need to understand the operational and security aspects of the relevant blockchain, the relevant nodes being used by the audited entity, and the nodes being used by the third parties providing the confirmation.

Confirmations can be obtained for entities that use third party custodians. It is worth noting that confirmations would only verify that a wallet holds certain cryptocurrencies. They would not on their own generally be sufficient to verify ownership or control over the assets.

### Private Key Management

Private keys and public keys are generated when a wallet address is established. Unlike a bank account where passwords can be changed (and hence provide auditors with audit evidence that only a specified number and stated group of people have access to a bank account through knowledge of such passwords), crypto asset wallet private and public keys are permanent. Consequently, for an auditor to obtain sufficient, appropriate audit evidence over the number and names of people who are stated as having access to the private key, it is likely that audit evidence will be obtained relating to the design, implementation and operating effectiveness of controls to restrict access to the keys from inception of the wallet to the end of the audit period.

First and foremost, auditors gain an understanding of the number of private keys (or shards thereof) in existence, and who can gain access to these. Ideally a private key would be split into different parts (or shards) so that no single person has unilateral transaction authority access to a wallet. Auditors therefore know how keys are split and used in a similar manner to multiple passwords (or factors) being required in a traditional banking environment. Inspection (as defined in ISA (UK) 500 (Para. A18 – 20)) and reperformance (as defined in ISA (UK) 500 (Para. A24)) may be some of the steps an auditor will perform in addition to enquiry and/or observation.

In practice, auditors invariably need to be present to observe key and wallet generation ceremonies and conclude on the operating effectiveness of controls implemented in the ceremony to provide audit evidence as to the number of key shards generated in the first instance, and who has access to them. From this point onwards, auditors obtain audit evidence over the operating effectiveness of the private key management lifecycle controls to determine that keys (or shards thereof) have been adequately safeguarded against unauthorised disclosure to other person(s), wittingly or unwittingly, or removed, altered or destroyed without a clear rationale.

Auditors test the operating effectiveness of controls where they plan to use the results of the controls testing to modify substantive procedures. There could be instances where it is not possible for auditors to test the operating effectiveness of key generation and management controls throughout the key lifecycle, such as where the:

- entity neglects to inform auditors about relevant events related to the generation and management of the key;
- entity uses another professional to observe a key generation ceremony; and
- auditor is taking on a new entity and replacing a previous auditor.

In the current environment, the most common scenario is where entities set up wallets without being audited, and then subsequently appoint their first auditor. Where work is performed by another professional, auditors may consider reviewing this work and assessing the ‘competence, capabilities and objectivity’ of the professional engaged and ‘appropriateness’ of work performed. This is in accordance with the provisions of ISA (UK) 500 (Para. 8), which relates to information prepared using the work of a management’s expert as audit evidence.

In instances where no work is performed by another professional, auditors use their professional judgement to determine what other additional procedures could be performed to gain sufficient, appropriate audit evidence over an entity’s sole ownership and control of the private key (or shards thereof). Note that this may not be possible, depending on the circumstances. Auditors may observe either:

- the entity transacting from the wallet based on their instructions, for example, by sending a small amount of crypto assets to another wallet being observed by the auditors; or
- the sending and receiving of messages in a technique known as 'key pair validation'. This validates that the public key is a valid cryptocurrency address that can perform transactions and that the private key is valid for the specified public address.

This will provide an understanding of the wallet structure and control procedures over wallet transactions. However, this does not necessarily give evidence relating to sole ownership and control of a wallet and therefore on its own is not a reliable source of substantive audit evidence. Obtaining evidence of sole ownership and control requires additional audit evidence.

If there are additional legal or regulatory requirements to obtain audit evidence relating to an entity's sole ownership and control of a wallet, and sufficient, appropriate evidence does not exist, auditors may consider requesting that the entity transfers the assets to new digital wallet(s), for which auditors have observed the key generation ceremony, and have been able to audit the controls relating to those new wallet(s) thereafter.

The following non-exhaustive list of procedures may assist an auditor to obtain audit evidence over the sole ownership and control of private keys from generation to the end of the audit period. Auditors use professional judgement to determine the sufficiency of procedures based on assessed risk factors.

- Reviewing controls documentation for key generation and key management during the audit period, and any control testing procedures performed by relevant parties to conclude on the operating effectiveness of these controls.
- Reviewing key generation scripts and software to determine the number of keys (or shards thereof) generated. If expertise exists in the audit firm, auditors may be able to perform these procedures. If not, a third-party expert could be engaged to do the same.
- Reviewing reconciliations and reconciliation controls from key generation to the end of the audit period to determine whether breaks are effectively investigated and resolved.
- Reviewing blockchain transactions from the generation of the wallet to the end of the audit period and obtaining evidence for transactions. Transactions are both sampled (in accordance with the requirements of ISA (UK) 530 Audit Sampling) and reviewed for any evidence that a third party may be using the wallet to transact. Tools are available to assist auditors in monitoring blockchain transactions. However, auditors assess the reliability of these tools before using information produced by them, which may create significant challenges regarding the reliability where publicly available and free to use blockchain explorers are used.
- For third-party custodians, obtaining confirmations as per ISA (UK) 505 and reviewing ISAE 3402 or US-style Type 1 SOC reports and assessing the sufficiency of procedures performed by service auditors as per ISA (UK) 402 can help provide assurance over the custodian and its control environment.

**Risks around accuracy of data**

Verifying the accuracy of data used in an audit of cryptocurrencies, including data obtained from blockchains where cryptocurrencies reside can be challenging. Auditors obtain an understanding of the accounting policies, including the relevant financial reporting standard and the recognition criteria, measurement bases, and the related presentation and disclosure requirements' as per ISA (UK) 540, as there are nuances in the classification and accounting treatment of transactions in the cryptocurrency sector. They also obtain an in-depth understanding of the IT infrastructure in place. Data extracted from blockchains can be transferred to and from other financial systems including the financial reporting system. As such, auditors consider risks relating to the accuracy of data extracted from the blockchain, as well as controls over the transfer of data to other financial systems, and the controls over financial systems themselves.

### IT General Controls (ITGCs)

The starting point for validating the accuracy of data is a thorough assessment of the ITGCs around the node connected to the blockchain, other relevant systems and the wider IT environment following the requirements of ISA (UK) 315 (Para. 25 – 26). Appendix 5 of the standard sets out considerations for understanding an entity's use of IT in its system of internal control. Para. 5 of the Appendix recognises that entities may use emerging technologies such as blockchain but states that 'while emerging technologies may be seen to be more sophisticated or more complex compared to existing technologies, auditors' responsibilities in relation to IT applications and identified general IT controls (in accordance with the ISA) remain unchanged.'

The IT environment in an entity that has its main operations in a blockchain environment is usually considered to be complex. This complexity may be compounded where management introduces an interface between the blockchain and financial reporting system. In this case, auditors carefully consider the implications on their IT risk assessment. There are overarching risks such as those relating to the cybersecurity environment that threaten an entity's policies and procedures for safeguarding private keys, and ultimately control and ownership, of cryptocurrencies.

Auditors also take care to adequately document all work performed in all areas. This includes their assessment of ITGCs and any Information Prepared by the Entity ('IPE') procedures. The technical and complex nature of the blockchain can add difficulty to the process of documentation, particularly if the audit team is unfamiliar with how the technology works. Training programmes and the use of specialist to demonstrate how audits of cryptocurrencies should be documented are therefore important considerations.

There are two likely outcomes from the assessment and testing of ITGCs:

- ITGCs appear to be designed, implemented and operating effectively and the 'IPE' generated by the system can be used as a source of audit evidence. In this case auditors confirm the accuracy and completeness of data extracted from the IT systems as per ISA (UK) 500 (Para. 9); or
- there are deficiencies in the ITGC environment, and the IPE from the systems cannot be used.

Deficiencies arise predominantly from:

- inadequate control of privileged access rights; and
- inadequate change management, including not maintaining a log of changes made to the IT environment.

In the event of the above deficiencies, auditors address the following key risk scenarios:

A. **Unsophisticated user changes data:** This scenario would be a change to data (insert, update or delete) by a user without the knowledge to update the data in all relevant IT repositories and would only change it in one.

B. **Sophisticated user changes the datasets:** A user with sufficient knowledge (such as a programmer or member of the senior management team) who either changes the data in all IT repositories or deploys code to achieve this.

Key risks over the accuracy of data extracted from financial systems may include the following.

| | Risks | Risk Scenario |
|---|---|---|
| **1** | Data is modified in product tables which are used for the creation of general ledger entries which materially impact the financial statements. | **A** |
| **2** | Data is modified in multiple tables (for example the product and ledger tables) which materially impacts the financial statements. | **A and B** |
| **3** | Multiple opposite trades are processed to net off the user balance but affect revenue. | **B** |

| | | |
|---|---|---|
| **4** | Fictitious accounts are used to create trades and inflate revenue. | **B** |
| **5** | The entity's crypto trading account balances are inflated to generate additional trading volumes from these accounts. | **B** |
| **6** | Back-end code is modified to affect trades and modify revenue. | **B** |
| **7** | **User account balances are modified directly, and the balances used to trade with a material impact on financial statements.** | **A and B** |

### Blockchain explorers

A blockchain explorer is a software application that enables users to query a particular blockchain such as Bitcoin and Ethereum, and extract, visualise and review blockchain transactions and/or network metrics. It uses Application Programming Interfaces (APIs) and a blockchain node (computer system on the network) to retrieve data and arranges it in a readable format. Blockchain explorers can also be used to trace balances in wallet addresses.

As suggested by ISA (UK) 540 (Para. A82), 'obtaining audit evidence in an unbiased manner may involve obtaining evidence from multiple sources.' Public blockchain explorers have generally not been independently tested to validate that data is generated completely and accurately. Where possible, it is helpful to compare a single transaction across different blockchain explorers to confirm that identical information is retrieved. This approach is only relevant where the blockchain in question has several explorers available, which is mainly the case for larger and more well known blockchains. Where only one explorer exists, the results generated by the explorer may not be reliable.

There are some independently tested blockchain explorer services available at a cost. If the audited entity has its own blockchain explorer service, it is unlikely that auditors will use it for audit procedures, unless, it has itself been audited and ITGCs have been tested. Once the integrity of the blockchain explorer has been confirmed, auditors can use the appropriate tool to retrieve data.

When extracting data from a blockchain, there are usually two options available to auditors, which are running their own nodes or using third party nodes. There are pros and cons associated with each option and auditors carefully consider which approach is most suitable when undertaking an audit.

Potential benefits and challenges of auditors running their own nodes on the network include:

| Benefits | Challenges |
|---|---|
| **Trust:** Auditors can obtain more reliable audit evidence as data can be directly extracted from the blockchain. | **Data storage:** Running a node requires a significant amount (gigabytes) of disk space for data storage as well as sufficient Random Access Memory (RAM) to process transactions. |
| **Privacy and security:** Running their own node ensures data privacy for auditors and allows them to process transactions themselves, without the involvement of third parties. | **Bandwidth:** Running a node is data intensive and there is a significant amount of data exchange required to process transactions. This includes downloading and uploading data. |
| **Autonomy:** Running their own node provides the ability to choose which protocol or blockchain to proceed with when a blockchain fork (change of protocol or split) occurs. | **Maintenance:** Some websites require the node to be running for several hours per day. It is recommended that nodes should be running 24 hours a day. |
| | **Costly:** Running a node is expensive as a significant amount of electricity is used to maintain and run the node. |

| | |
|---|---|
| | **Independence:** auditors running a node on the blockchain network could be considered to be operating the client's system, which could create independence problems. |

Using third-party nodes can provide the following benefit and challenges:

| Benefits | Challenges |
|---|---|
| **Simplified node management:** Third-party infrastructure providers offer user-friendly interfaces and tools that simplify the process of setting up and managing blockchain nodes. | **Reliance on third-party providers:** When using third-party infrastructure providers, auditors may become dependent on their services for the operation of their blockchain nodes. |
| **Scalability:** Third-party infrastructure providers typically offer scalable solutions that can handle a large number of nodes and transactions. | **Centralization:** Depending on the third-party infrastructure provider, nodes may be hosted in centralized data centres, which can undermine the decentralization and security of the blockchain network. |
| **Cost-effectiveness:** Running a blockchain node can be expensive in terms of hardware, bandwidth, and electricity costs. Using a third party could reduce these costs. | **Privacy and security concerns:** Third-party infrastructure providers may have access to sensitive client data, such as transaction details and smart contract code. |
| **Support and maintenance:** Third-party infrastructure providers usually offer support and maintenance services, including regular updates, security patches, and monitoring. | **Limited customisation:** Third-party infrastructure providers may have limitations in terms of customization and configuration options for the blockchain nodes. |

## NEXT STEPS

ICAEW's future work on digital assets will focus on facilitating debate and building understanding of the impact of blockchain and digital assets on the profession, including in the areas of audit and assurance, tax, corporate reporting and regulation.

This will involve collaborating with other stakeholders to understand the capabilities and issues and including:

- accountants working in business and practice and in small and large organisations, who can reflect the diverse range of experience across the profession;
- regulators, who are considering the risks attached to new technologies;
- governments and policymakers;
- educators and training providers, who are considering the future skills of accountants;
- technologists and blockchain experts, who are developing and maintaining the technology and who understand its strengths and limits;
- Service providers who are providing services in the digital asset ecosystem; and
- Other experts and professions who can contribute to discussions around digital assets.

## ABOUT ICAEW'S DIGITAL ASSET WORKING PARTY AND TECH FACULTY

The ICAEW Digital Assets Working Party (DAWP) was formed in February 2023 to share knowledge and influence policy around digital assets. It is a multi-disciplinary working party with experts across accounting, law, academia, regulation, and technology. It has workstreams focused on audit and assurance, financial reporting, the future of digital assets, regulation, and tax. This publication has been developed by the DAWP audit and assurance workstream which is coordinated by the ICAEW Tech Faculty and whose members include experts from BDO, Deloitte, EY, Grant Thornton (Cyprus), KPMG, and PwC (Hong Kong). This publication does not represent the views of individual firms.

ICAEW's Tech Faculty provides products and services to help ICAEW members make the best possible use of technology. It represents chartered accountants' technology-related interests and expertise, contributes to technology related public affairs and helps those in business to keep up to date with technology issues and developments. The faculty also works to further the study of the application of technology to business and accountancy, including the development of thought leadership and research. As an independent body, the tech Faculty can take a truly objective view and get past the hype surrounding technology, leading and shaping debate, challenging common assumptions and clarifying arguments. For more information on ICAEW's work on blockchain and digital assets visit ICAEW's Blockchain hub. To contact the faculty email techfac@icaew.com.

## APPENDIX 1 – WHAT IS BLOCKCHAIN

A blockchain is a type of distributed ledger that uses cryptography to secure and record transactions in a distributed database. That database is populated by a list of ordered records – the blocks – which is continually added to. Once added, it is extremely difficult (but not impossible) for records to be deleted or edited, and the blockchain therefore creates a high level of trust.

With blockchain transactions, there is no single computer that acts as the 'owner', on whom users must rely for accuracy. The records are distributed among blockchain participants, and a complex series of consensus and verification processes are used to arrive at an agreed-upon version of the ledger. This verification is performed by computer systems, or 'nodes', based on various protocols, the two most common being 'proof of work' and 'proof of stake'. The verification process differs slightly but the principle in both cases is that nodes compete to validate a block or write the next block in the blockchain. There are many blockchains that underlie cryptocurrencies, but the original and most famous one underpins the cryptocurrency Bitcoin and is called simply ‘the blockchain’.

There are three types of blockchain:

- Public, or permissionless, blockchains are decentralised. Anyone with a computer and internet connection can join the network and can read, and write to, the database. The Bitcoin blockchain is an example of a public blockchain.
- Private blockchains are partly decentralised. They are typically owned by a single organisation that is responsible for verifying users and giving them permissions on the network. That helps to ensure the privacy and confidentiality of information.
- Permissioned blockchains are a hybrid between public and private blockchains and are also partly decentralised. Management of the network – including protocols, access and permissions – is done by a consortium of trusted nodes. These blockchains also help to safeguard privacy and confidentiality as access is verified and restricted.

'Privacy coins' are worth mentioning as a type of cryptocurrency that present specific audit challenges. They are augmented with additional privacy-enhancing technological layers to facilitate anonymity and minimise traceability. That can be done through use of temporary or one-time use wallet addresses, or ‘mixers', which combine and mix transactions to hide individual transactions. Due to their anonymous nature, privacy coins are often used in criminal activities and are receiving strong scrutiny from regulators. In some jurisdictions, they are banned entirely.

When auditing a cryptocurrency, consideration is given to its underlying blockchain technology, and how that affects the nature of the cryptocurrency.

ICAEW is a world leading professional membership organisation that promotes, develops and supports over 166,000 chartered accountants worldwide. We provide qualifications and professional development, share our knowledge, insight and technical expertise, and protect the quality and integrity of the accountancy and finance profession.

As leaders in accountancy, finance and business our members have the knowledge, skills and commitment to maintain the highest professional standards and integrity. Together we contribute to the success of individuals, organisations, communities and economies around the world.

Because of us, people can do business with confidence.

ICAEW is a founder member of Chartered Accountants Worldwide and the Global Accounting Alliance.
www.charteredaccountantsworldwide.com
www.globalaccountingalliance.com.

Chartered Accountants' Hall
Moorgate Place, London
icaew.com

T +44 (0)1908 248 250
E generalenquiries@icaew.com

TECPLN15834