

Crypto Overview

Basics of cryptocurrency businesses

The rapid penetration of Decentralized Finance (DeFi)

Into the world economy has led to the rapid emergence of FinTech companies in segments such as A) crypto-currency mining, B) custodian of digital assets and C) payment processors. Consequently, the interest of investors is increasing in these sectors which increases the necessity and involvement of the Independent auditors to audit their financial statements.

Audit of crypto companies involves unique challenges, including testing of complex technology and compliance of regulatory frameworks. This article provides a structured approach on the audit of crypto companies, focusing on key areas like IT general controls (ITGC), IT application controls (ITAC), revenue, and compliance.

Crypto Company Types

Most of the cryptocurrency companies can be summarized into 3 broad categories; These are blockchain validators, cryptocurrency custodians, and payment processors.



Crypto Company Types



Validators

We sit down with you to understand your needs, but also your experience in dealing with designers and contractors.



Custodians

As crypto use grows, payment processors help businesses accept digital currencies easily.



Payment Proc.

Knowing these crypto companies is key to navigating digital finance and making smart choices.

01

Crypto Validators

A cryptocurrency validator is a company that participates in the validation and verification process of transactions on a blockchain network. Validators are integral to the security and integrity of decentralized blockchains, using the raw computational requirements used in Proof of Work (Mining) or holding cryptocurrency in a more restrictive wallet Proof of Stake (Staking), where validators are using these consensus mechanisms to confirm and adding new blocks to the blockchain ledger. In return for validating blocks and transactions, the company receives a portion of the new minted cryptocurrency and cryptocurrency transaction fees as contribution.

02

Crypto Custodian

A cryptocurrency custodian company (“Custodian”) is a company that provides secure storage solutions for the holders of digital assets to safely hold large amounts of cryptocurrency. These companies tend to offer additional services such as the ability to trade cryptocurrencies with other users or staking.

The Custodian can act as an exchange where users can trade cryptocurrencies directly with one another or through an order book system. This exchange itself acts as an intermediary, handling the matching of buy and sell orders. These companies earn fees on each transaction performed by users on the exchange.

03

Crypto Payment Processing

As the use of cryptocurrency for payments grows, crypto payment processors play a vital role in enabling other businesses (i.e. merchants) to accept and manage digital transactions. These companies offer services that enable businesses to accept cryptocurrency payments, either by integrating crypto payment gateways or providing tools for easy conversion of crypto to and from fiat.

Custodians & Their Functions



Crypto Validators 2 WEEKS



Crypto Custodians 1 WEEK



Payment Processors 3 WEEKS



Integration Phase 2 WEEKS

Fees, Transactions & Rules



Validators

\$1,000



Review

\$2,000



Payments

\$2,500



Compliance

\$5,000

Audit Challenges



Given the different types of cryptocurrency companies there are, many different and varied audit challenges may occur. Below is the useful summary for stakeholders of crypto companies to evaluate adequacy of the auditor involved in the audit of these crypto companies.

Audit team Competence

For every engagement, the challenge starts with acceptance and continuance. The major challenge is whether the firm has the capabilities and the competence to audit cryptocurrency client. Cryptocurrency concept may be roughly equivalent to fiat at the highest level, but the underlying technology and transaction make it quite complex to understand and audit. There are several considerations the need to be taken into account when determining whether to accept a new audit client and/or continue with the existing cryptocurrency related assurance engagement:

- Does the engagement team have the training and experience to perform an audit of a crypto currency client from the above specific segments? Each segment of crypto sector requires different skills and focus areas;
- Does the client's management have the appropriate experience and competency to allow for a proper audit? How can you get a high-level comfort prior the accepting the engagement?
- Does the audit team have IT specialist who can lead in the tech side of the audit and communicate with client's IT team on scoping and testing strategies?
- Does the audit team have legal expert (in-house or external) who can assist in understanding the compliance and regulatory requirements?

ITGC

A key challenge in auditing crypto clients is the technological environment of the entity. This is critical to the audit as cryptocurrency is entirely reliant on technology, coupled with the large volume of transactions and/or a large dependence on other service providers. Accordingly, the precise ITGC scoping of list of software that are used in key crypto processes is critical.

The audit should include risk assessment, evaluation/testing of controls on significant risks (such as digital revenue and cryptocurrency assets), controls over manual entries (from the IT system to the financial statements). Its rebuttable presumption that only substantive audit testing will not be the adequate audit procedure to audit the large volume of transactions.

As the scoped list of software for testing could be massive list, auditors should consider relying on SOC reports (SOC 1 or SOC 2) of those software providers and focusing only on adequacy of Complementary User Entity Controls (CUECs).



Private Keys



Due to the electronic nature of cryptocurrency, make them more vulnerable to theft or loss, particularly due to the private keys' susceptibility of losing or stolen. The audit should focus points on how private keys are handled and secured, assess the access and authorization regarding 3rd party digital wallets and exchange platforms where private keys are held by another entity, the transaction approval process regarding crypto asset transfers, and assess the transactions recorded to the blockchain to check for any discrepancies in the custodian's systems.

Securities



There are challenges regarding the securities classification of cryptocurrency stem from the evolving regulatory landscape, uncertainty in legal classifications, the inherent complexities of crypto assets, and the lack of clear guidance on how cryptocurrencies should be classified for financial reporting purposes.

Blockchains



To view the cryptocurrency blockchain, auditors will typically use tools called blockchain explorers to review the information recorded on blockchain ledgers. Auditors should perform procedures such as performing the background check to ensure they are designed and operating effectively to extract the relevant and accurate information from the blockchain.

Mining



Cryptocurrency mining on Proof of Work currencies, such as Bitcoin, involves the substantial use of computational power to validate transactions and secure the blockchain networks. The recognition of mining rewards (often issued in cryptocurrencies) will need to be assessed through inventory, intangible assets, and revenue recognition criteria. Most of the miners join the Pools which complicates the work of the auditor to obtain the reliance on the amount allocated from the Pool to participating entity.

Staking



In contrast to Proof of work currencies, Proof of Stake cryptocurrencies, such as Ethereum, involves locking up a certain amount of cryptocurrency to support the operations of a blockchain network in exchange for staking rewards. Auditors should verify the cryptocurrency within the staked wallets and verify the staking rewards received. Auditors should also check for penalties or slashing events that might result in a loss of staked assets to ensure it is properly documented and accounted for.

Processing payments

Similar to other industries, auditors need to review how payment processors record revenue, especially for transaction fees, or fiat-crypto conversions, and confirm its compliance with the treatment under IFRS 15. Due to the large number of transactions, auditors will need to analyze controls over batching and settlement processes, and, with respect to fraud detection, monitor transactions for irregular patterns or unauthorized activities. Due to the volatile cryptocurrency prices, auditors will need to assess the adequacy of real-time conversion mechanisms to minimize exposure risk. Subject to full control reliance on the system, the auditor might consider using Big Data analytical tools which enhances the audit procedures. Finding the nail in haystack is almost impossible with old school substantive audit testing

Agent vs Principal



Critical judgment is required in determining whether the company is the principal or the agent in transactions between customers. There should be an evaluation on the presentation of revenue on a gross or net basis based on whether the company controls the cryptocurrency provided before it is transferred to the customer (gross) or whether it acts as an agent by arranging for transactions between users of the exchange or from a supplier (net).

Mining and staking might involve third-party providers (e.g., staking-as-a-service). Auditor should review agreements to determine who controls the asset including who holds the risk of penalties or slashing.

Impairment of Mining Equipment



As per IAS 36, at the end of each reporting period, an entity is required to assess whether there is any indication that an asset may be impaired.

Cryptocurrency mining equipment is particularly prone to impairment as the equipment's performance deteriorates faster overtime due to the increasing computational power requirements overtime, fluctuating energy and highly volatile cryptocurrency prices, and technological obsolescence.

Compliance



Regulatory variability and compliance requirements further complicate audits, especially if the entity is operating in multiple jurisdictions. As cryptocurrency is a developing industry and the recent scandals in the news, regulators and governments around the world are continually implementing new laws and regulations to crack down on potentially fraudulent or criminal activities.

Auditors should obtain an understanding of the jurisdictions of client operates in, and what are regulatory requirements to operate in those countries such as licensing, “Anti-money laundering” and “Know your customer”. These will likely necessitate the involvement of Compliance legal experts to properly address and audit the compliance risk.

Conclusion



Competent auditors and quality procedures are required to do an effective audit of cryptocurrency companies. They will need to be on top of the complex technological environment within these companies, challenges in auditing the financial reporting, and changes regulations surrounding the cryptocurrency industry.

Contact us



PKF ANTARES PROFESSIONAL CORPORATION

info@pkfantares.com

www.pkfantares.com

Tel: +1 403 375 9955