Analytics mindset

Digital assets

Note: It is recommended that the EYARC *Innovation mindset: Intro to blockchain* and EYARC *Analytics mindset: Introduction to the analytics mindset* modules be completed prior to completing this case.

Part 1: Blockchain and digital assets basics

Required

Read the following to enhance your knowledge of blockchain and digital assets.

Blockchain basics

The term *blockchain* refers to a form of distributed ledger technology that is maintained by multiple parties, some of whom independently verify transactions, essentially in real time. New transactions are bundled into blocks, which are added sequentially to an existing chain using cryptography, without the need for a central authority. The chain is governed by a consensus mechanism that provides rules for the blockchain users to follow when agreeing on whether a transaction is valid. These blockchain users are referred to as nodes, and each node holds a complete copy of the ledger. The ledger is updated and distributed across all nodes in real time.

Blockchain technology is often used to track the ownership and transactions of assets that can be digitally represented on a blockchain. Digital assets include cryptocurrencies, such as bitcoin, that serve primarily as a medium of exchange or as a store of value and other assets that serve as digital representations of real-world assets (often referred to as asset-backed tokens), such as fiat currencies (i.e., as legal tender whose value is backed by the government that issued it), inventory, property or securities. Further, some digital assets may provide holders with some form of utility (often referred to as utility tokens), such as access to a good or a service from an identifiable counterparty.

Blockchains may be public or private. Public blockchains, such as the bitcoin blockchain, do not require permission to participate. That is, they allow anyone to use them to send or receive digital assets, view digital asset transactions of others and become a node. Private blockchains are mostly permissioned, meaning they provide closed access to a network that can be built for use by a single organization or by many organizations (often referred to as consortium blockchains).

Cryptography refers to secure information and communication techniques derived from mathematical concepts and a set of rule-based calculations called algorithms to transform messages in ways that are hard to decipher. These deterministic algorithms are used for cryptographic key generation and digital signing and verification to protect data privacy. In the context of blockchain technology, cryptography involves the creation of public key and private key pairs, which are mathematically linked. The public key can be shared with counterparties, like a bank account or a routing number, but a private key is only known by the originator (unless it is exposed, or the originator decides to share it).

Ownership of digital assets is associated with a public address, which represents the hash of a public key and is a string of unique alphanumeric characters. The transparency of transactions varies by blockchain.

For example, on the bitcoin blockchain, anyone can see the details of all transactions, including the amounts and public addresses of the parties to the transactions (but not their identities). Other blockchains, both public and private, may provide a higher level of anonymity so that users are not able to view the amounts or public addresses of the parties to the transactions.

The private key is typically stored on hardware or software known as a digital wallet. When the holder of a digital asset wishes to transfer that digital asset to another network participant, the holder uses its digital wallet to initiate a transaction and broadcast it to the blockchain network, indicating the amount and the public addresses of both parties. The holder digitally signs the transaction using the private key.

The message or transaction is signed, or hashed, prior to being broadcast to the network and it is then validated by a validating node, often referred to as a validator, miner or staker, using a deterministic algorithm. In the validation process, the validator verifies, through cryptography, that the transaction could only have been created by the holder of the mathematically paired private key, without ever knowing the private key. The validator then aggregates a group of transactions into a block and links the block to the existing blockchain, or distributed ledger. This group of transactions is then broadcast to other nodes that participate on the blockchain, thus validating that there is a consensus. On some blockchains, such as bitcoin, the validator receives newly issued digital assets as a reward and sometimes gets transaction fees, or additional digital assets, from the participant that initiated the transaction.

Entities may secure the private key themselves, often referred to as self-custody, or they may use a third party, such as a custodian or exchange, to maintain custody of the private key. These third parties may use a single public address to hold and transact digital assets for a large number of customers, often referred to as commingled accounts, rather than maintain a separate public address for each customer. Further, private keys can be contained in cold storage (e.g., offline, air-gapped hard drive) or in hot storage (e.g., a cloud-based application).

Digital assets basics

Digital assets include any asset (tangible or intangible) that can be digitally represented on a blockchain, including:

- Cryptocurrencies serve as a medium of exchange and provide no other rights or privileges to the holder (e.g., bitcoin, Ethereum).
- Tokens provide rights or economic value, other than serving purely as a medium of exchange to the holder, e.g., utility, such as to access a good or service from an identifiable counterparty; or security, as in ownership rights in an entity, e.g., voting rights, or rights to participate in profits; or rights to payments in fiat currencies (including stablecoins* and non-fungible tokens (NFTs)).
- Digital representations of any “real-world asset” include raw materials, consumer and industrial products, real estate or financial instruments.

Entities may engage in various activities in the blockchain ecosystem and:

- Hold or transact using digital assets. These entities include investment funds, high-frequency trading companies, and entities that receive digital assets as payment for goods or services.

* For more information about stablecoins, see “Stablecoins – The next generation crypto asset,” EY 2020 Global Blockchain Summit (Day 2 noon session), https://pub.ey.com/public/2019/1911/1911-3312324/global-blockchain-summit/home/day2.html, April 2020.

- Hold or facilitate trading of digital assets on behalf of customers. These entities include digital asset exchanges, broker-dealers and custodians.
- Create or issue digital assets for sale or distribution to third parties. These entities typically do this through initial coin offerings, airdrops, direct sales or exchanges, or other means.
- Use blockchain-based business models. These entities include validators, payment service providers, platform providers and digital wallet providers.
- Operate or participate in blockchain processes or consortiums. These entities leverage blockchain technology to process or record transactions relevant to their financial reporting.

Analytics mindset

Digital assets

Part 2 Section 1: Accounting for cryptocurrencies

Note: For the purpose of our case study, we are focusing our discussion on cryptocurrency digital assets.

US GAAP does not specifically address a holder's accounting for cryptocurrencies. The accounting, therefore, must be evaluated based on the nature of the asset, the type of investor and how the asset is held. Entities may hold their cryptocurrencies directly or indirectly through a third party, such as a custodian or an exchange, that may control access to the entity's cryptocurrency holdings. For this part of the case, let's assume that we are assessing the classification and accounting for cryptocurrencies that are directly held by the company and that company is not an investment company.

Required

Answer the following questions and provide support for your responses.

1. Under US GAAP, what do you think cryptocurrencies (such as bitcoin) are classified as?
   a. Cash and cash equivalents
   b. Financial instruments
   c. Inventory
   d. Intangible assets
2. Based on your classification, how would they be measured?

Analytics mindset

Digital assets

Part 2 Section 2: Auditor’s responsibilities and audit risk assessment

Required

Read the following to enhance your knowledge of auditor’s responsibilities and audit risk assessment for digital assets.

Auditor’s responsibilities for digital assets

What does the accounting for digital assets mean for an auditor’s responsibilities?

- Differing accounting approaches pose a challenge for auditors, so efforts are underway to establish consistency across auditing practices globally.
- Accountancy bodies (such as the American Institute of Certified Public Accountants*[1] and the Center for Audit Quality) have launched working groups focused specifically on handling emerging technologies, including digital assets.
- While there are still obstacles to overcome before procedures and approaches are fully aligned, these are promising steps forward and, over time, we can hope to see gradual convergence.

Trust can be the most abused and misleading word in the world of blockchain. Inside the blockchain, you can trust the math. But risks are still present when integrating blockchain in the real world requiring trust but also verification. Many perceive that because blockchain transactions are considered immutable and based on cryptography (the math), there are no additional risks; however, this is not the case. For example, the math can validate the existence of a digital asset and imply ownership, but ownership can be compromised if the private key is stolen, lost or otherwise misappropriated. Let’s now discuss these additional risks.

Audit risk assessment

The risks associated with digital assets vary, depending on how an entity holds these assets or transacts with them. Auditors need to understand and evaluate controls around custody, either internal controls in self-custody situations or service organization controls (SOC) in third-party custody solutions.

To appropriately identify and assess risks of material misstatement and to design audit procedures that respond to the identified risks, an auditor needs to obtain an understanding of the entity’s activities involving digital assets, including the following:

- The entity’s business purpose for holding or transacting digital assets
- The types of digital assets held or transacted by the entity (e.g., bitcoin)

* See non-authoritative guidance available in the AICPA Practice aid titled, Accounting for and auditing of digital assets..

- Whether the entity maintains custody of its digital assets or whether a third party has custody of the assets
- Whether a third party that has custody of the assets stores them in segregated or commingled public addresses, and whether the third party has an appropriate service organization control (SOC) report
- How the entity transacts with its digital assets (e.g., peer-to-peer trades on the blockchain, trades on a digital asset exchange) and whether such transactions are traceable to the blockchain

The following are examples of audit risks relating to cryptocurrency assets mapped by audit assertion:

Risks	**Completeness**	**Existence and occurrence**	**Rights and obligations**
Risks related to a company’s books and records			
All transactions are not recorded	■		
Digital assets recorded do not exist		■	
Transactions recorded did not occur		■	
Entity may not own the digital assets (e.g., owned by a related party)			■
Risks related to blockchain itself			
All transactions are not recorded on the blockchain	■		
Private key has been lost or destroyed; no longer has access			■
Private key has been stolen or inappropriately accessed (i.e., misappropriation of assets)		■	
Risks related to the use of data from block explorers			
Block explorers do not accurately extract or display information	■	■	■

To explain further for risks that might not be as easily understood:

- All transactions are not recorded: While the risk of understatement is usually not the principal audit risk for an asset account, there should be consideration whether management did not identify or disclose the complete population of its public addresses.
- Entity may not own the digital assets (e.g., owned by a related party): An entity might not have sole ownership rights over the digital assets because other entities and individuals (such as related parties) have knowledge of the private key or are otherwise able to assert ownership rights over the same digital assets.

Risks related to the use of data from block explorers

- Block explorers do not accurately extract or display information from a blockchain: Blockchain explorers are an external data source and might be unreliable. In addressing this risk, management might have controls that directly address how blockchain explorers function or have reliable off-chain evidence of digital asset transactions, and have effective controls over the initiation and recording of the transactions. For example, it may be reasonable for management to conclude that its reconciliation controls provide a basis for determining that the information from the blockchain explorers (and blockchain) is reliable.

Analytics mindset

Digital assets

Part 3: Understanding public blockchain data

Background

- Your client has provided you with a table of its cryptocurrency transactions (bitcoin) that occurred on March 1, 2018, for its wallet at the address: 17A16QmavnUfCW11DAApiJxp7ARnxN5pGX.

Transaction ID	Block	DD.MM.YYY time	Value	Running balance	Sent/ received
5a60cf5712521d0dc57c0cb56f493126c6d7967b78ee6cc9ac28c7b77bffb2c7	511417	01.03.2018 04:54	0.09761362	273.938403	Received
3c25b98df1d2ce6a7cce227f4300e28c93141ad98cdf4f4d8f07955b79f7abf1	511418	01.03.2018 05:02	-0.04125702	273.9001168	Sent
3a69317f65e4ef0c73a242c9c4ae125a7c27e0f23397be7652e65d409a156ea1	511418	01.03.2018 05:02	0.0271139	273.9413739	Received
66a8dd8135d7655207b17ee5a0279ab0184987105b8c51cb79233d3d0835dbf9	511418	01.03.2018 05:02	-0.01465857	273.91426	Sent
c22e31c0010acadf1c9457593379b496b0f0a65d25df3bdea19b7453bf67cc68	511418	01.03.2018 05:02	0.01877822	273.9289185	Received
3bb36c8afe021b031b4bac846f56e4b17ba25e5cc208ea8a450a97535c29a86b	511419	01.03.2018 05:04	0.00042844	273.9005453	Received
4c5ff27fa0c0e20d3d55dd94f065c9258208e339c0b02c403c8c3c6587781db6	511420	01.03.2018 05:28	0.05636806	273.9177608	Received
7cad2ead30accb9f4f0dbd4511f755589e4efd42fb44e9d6daaf231d49c46fb3	511420	01.03.2018 05:28	-0.09210298	273.8613927	Sent
f533bbf1e47ed31a14a5a4ce80907d0aa28b271147fb6e098e92d5b1e732e774	511420	01.03.2018 05:28	0.00587873	273.9534957	Received
96b536a276c1add2e511837a20f67dc1bfa547e004397a4e4743406349ed2f0d	511420	01.03.2018 05:28	0.07450548	273.947617	Received

- Tools often referred to as block explorers are commonly used to access and analyze information from a public blockchain. These tools display the contents of a public blockchain and allow users to examine the details of individual blocks (e.g., all transactions included in a block), individual transactions (e.g., the transaction amount, the sender's public address, the receiver's public address) and information about specific public addresses (e.g., the balance as of the point in time that the information is accessed, details of all transactions).

Required

1. Blockchair is a block explorer. Using this block explorer, the transaction ID and the wallet address, check to see if each transaction exists on the bitcoin blockchain and if the value of each transaction (number of tokens) differs from the client data.
2. What are your findings?
3. What are your perspectives about using a tool like this to audit these types of transactions?

Analytics mindset

Digital assets

Part 4 Section 1: Overview of the EY Blockchain Analyzer tools and using public blockchain data as audit evidence

Required

Watch and read the following to gain knowledge about the EY Blockchain Analyzer tools and use of public blockchain data as audit evidence.

EY Blockchain Analyzer

Watch this video to better understand the functionality of the EY Blockchain Analyzer.

Transforming the business lifecycle with EY Blockchain Analyzer
3:58
Transforming the business lifecycle with
EY Blockchain Analyzer

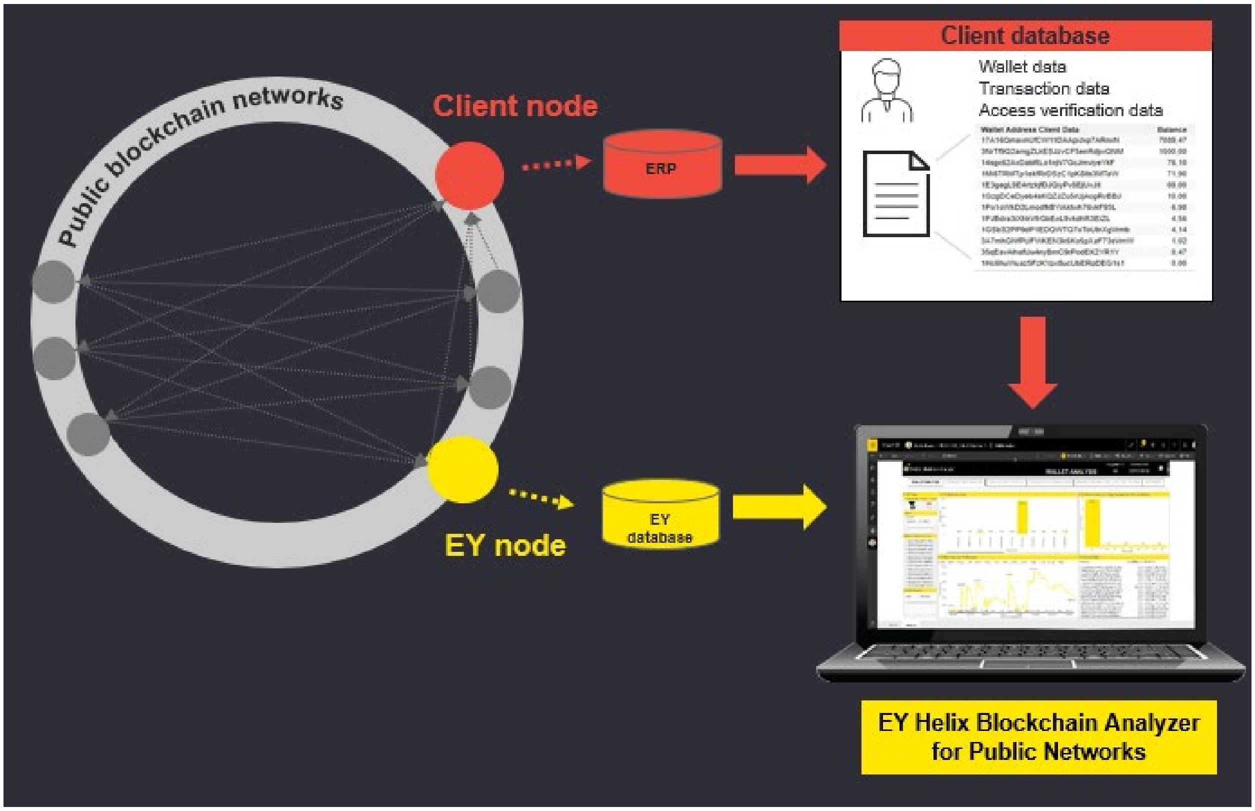
While there are a variety of EY Blockchain Analyzer tools available to EY professionals to provide services to clients, our focus today will be on the EY Blockchain Analyzer for Public Networks, which is designed primarily to facilitate and support audit teams in the reconciliation of data between the client's books and records and the public ledger. This tool is available to Assurance professionals in EY Helix, the EY global suite of data analytics tools.

EY Helix Blockchain Analyzer for Public Networks

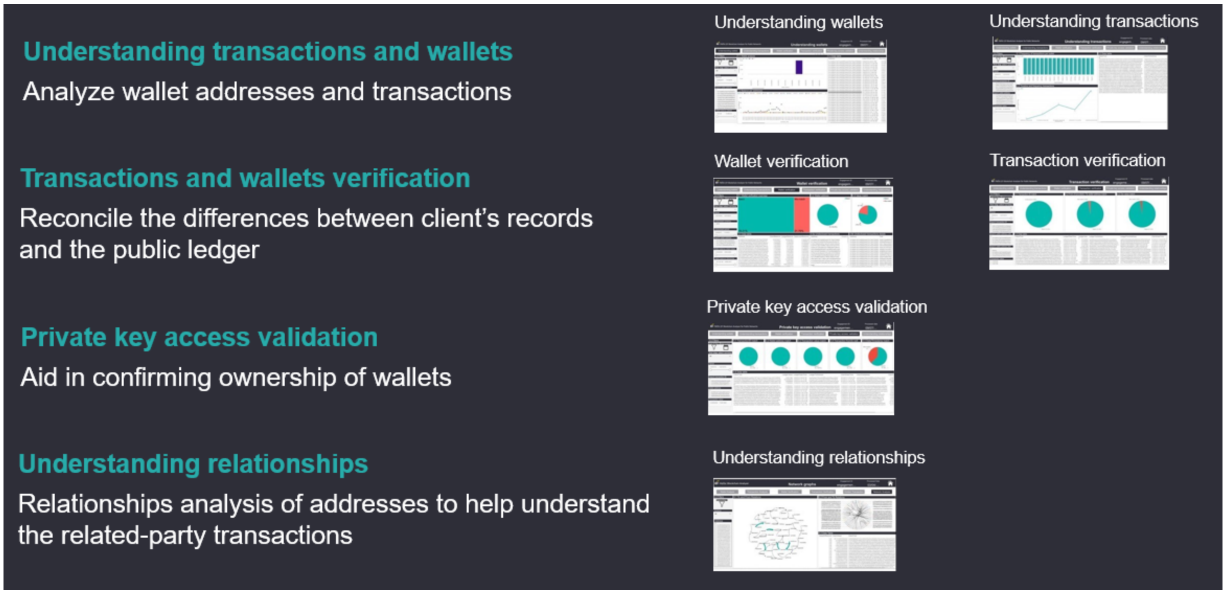
The EY Helix Blockchain Analyzer for Public Networks supports audit teams in certain assertions around digital assets on public blockchain networks. The analyzer obtains public blockchain data from an EY node that **independently** validates the authenticity of transactions, like other nodes on the public blockchain network. Public blockchain data obtained directly by EY and validated by the EY node is more reliable than evidence obtained from one or more third-party block explorers.

Using the analyzer enhances the firm's ability to obtain sufficient appropriate audit evidence by allowing reconciliation of **complete populations** of an entity's transactions with the information contained in the blockchain in a timely manner. That is, there is no need to manually reconcile individual transactions by using third-party block explorers. Using the analyzer also reduces or eliminates the need to use sampling techniques and allows EY to analyze complete populations for unusual trends or anomalies.

This visual can provide a helpful overview to see the flow of information.



EY Helix Blockchain Analyzer for Public Networks key features



Understanding transactions and wallets

Analyze wallet addresses and transactions

Transactions and wallets verification

Reconcile the differences between client's records and the public ledger

Private key access validation

Aid in confirming ownership of wallets

Understanding relationships

Relationships analysis of addresses to help understand the related-party transactions

Understanding wallets
Understanding transactions
Wallet verification
Transaction verification
Private key access validation
Understanding relationships

Using public blockchain data as audit evidence

EY has performed procedures to support the ability of audit teams to use transaction-related information from certain public blockchain networks as audit evidence (the EY node). EY utilized its blockchain and cryptography resources to help evaluate these public blockchain networks. It is the responsibility of each audit team to read the evaluation for each relevant public network and determine the degree to which information from the blockchain contributes to the overall body of evidence for an assertion. These evaluations are updated periodically.

Each public blockchain network evaluation includes:

- A description of how transactions are initiated, recorded, processed and reported in the blockchain
- Identified risks that, if not addressed by controls within the blockchain, could affect the reliability of the transaction-related information in the blockchain
- Identified controls within the blockchain that are designed to mitigate the identified risks
- Procedures to evaluate whether the identified controls have been implemented within the blockchain

Public blockchain networks that EY has evaluated include:

- Bitcoin
- Bitcoin Cash
- Bitcoin SV
- Litecoin
- Dogecoin
- Ethereum
- Ethereum Classic
- XRP

Analytics mindset

Digital assets

Part 4 Section 2: Addressing audit risk through use of the EY Helix Blockchain Analyzer for Public Networks

Required

You were provided with an overview of example audit risks (i.e., what could go wrong) that are present when using public blockchain data to audit cryptocurrency assets.

Risks	Completeness	Existence and occurrence	Rights and obligations
Risks related to a company's books and records			
All transactions are not recorded	🟩		
Digital assets recorded do not exist		🟩	
Transactions recorded did not occur		🟩	
Entity may not own the digital assets (e.g., owned by a related party)			🟩
Risks related to blockchain itself			
All transactions are not recorded on the blockchain	🟩		
Private key has been lost or destroyed; no longer has access			🟩
Private key has been stolen or inappropriately accessed (i.e., misappropriation of assets)		🟩	
Risks related to the use of data from block explorers			
Block explorers do not accurately extract or display information	🟩	🟩	🟩

1. Identify if there are any example audit risks that might not be addressed by use of the EY Helix Blockchain Analyzer for Public Networks.
2. Explain why.

Analytics mindset

Digital assets

Part 5: Audit of Digital Assets Inc.

Section 1: Understanding the company's cryptocurrency transactions, your audit tool and your data

Required

Read the following to prepare for your audit of Digital Assets Inc.

Understanding the company's cryptocurrency transactions

Your client, Digital Assets Inc., allows customers to pay invoices in bitcoin, a common cryptocurrency that makes up approximately 50% of the market cap of all cryptocurrencies (as of May 2021). In order to scope your audit, you will need to know more about their cryptocurrency transactions. Some of the questions that you would ask your client include:

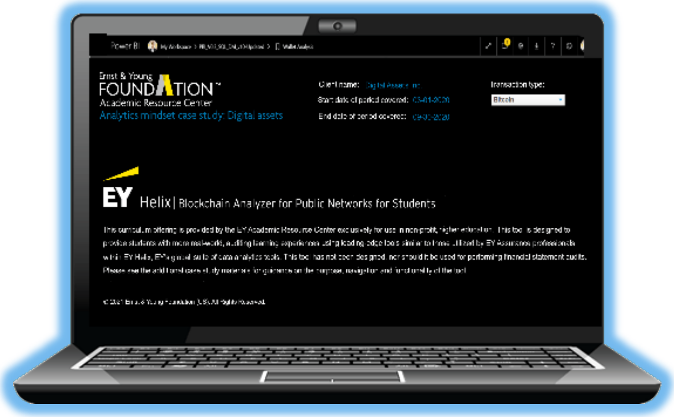
- What do they do when they receive bitcoin from their customers? Do they typically hold the bitcoin for a period of time, or do they convert it promptly into fiat currency?
- Do they use their bitcoin to make any payments to their suppliers, employees or any other stakeholders?
- Are they transacting with any other cryptocurrency?
- Do they transact peer-to-peer or over public exchange?
- How frequently do they transact?
- Do they maintain their own digital wallets and private keys or do they utilize a third-party custodian?
- What controls do they have around transaction initiation?
- What controls do they have around private key security?

Asking appropriate questions to gain an understanding of their business and transactions will help you develop expectations about what type of transactions you might see. You will also need to consider what evidence you'll need to validate transactions in the balance sheet and income statement.

For the purpose of this case study, we are focusing on the evidence you need to gather with respect to the balance sheet accounts (a discussion of materiality and the documentation of your audit work are beyond the scope of this case). Therefore, you asked the client to provide data about their cryptocurrency wallets, plus a list of cryptocurrency transactions during the period from January 3, 2020 to December 9, 2020.

Your audit tool

The EYARC has developed a simplified tool specifically for student use in completing this case study. This simplified tool offers the basic functionality of the EY Helix Blockchain Analyzer for Public Networks. It is designed specifically for the classroom using TIBCO Spotfire® software. The tool will help you simulate real-world audit analytics procedures by using similar data, analyses and tools used by professional auditors. This tool has not been designed, nor should it be used, for performing financial statement audits. It should only be used for nonprofit, higher education purposes.



Ernst & Young FOUNDATION™
Academic Resource Center
Analytics mindset case study: Digital assets

Client name: Digital Assets Inc.
Start date of period covered: 03-01-2020
End date of period covered: 09-30-2020

Transaction type: Bitcoin

EY Helix | Blockchain Analyzer for Public Networks for Students

This curriculum offering is provided by the EY Academic Resource Center exclusively for use in non-profit, higher education. This tool is designed to provide students with more real-world, auditing learning experiences using leading edge tools similar to those utilized by EY Assurance professionals within EY Helix, EY's global suite of data analytics tools. This tool has not been designed, nor should it be used for performing financial statement audits. Please see the additional case study materials for guidance on the purpose, navigation and functionality of the tool.

© 2021 Ernst & Young Foundation (US). All Rights Reserved.

Access the EY Helix Blockchain Analyzer for Public Networks for Students with this link.

EY Helix | Blockchain Analyzer for Public Networks for Students

Your data

The EY Blockchain Team transferred the client-requested data into your analyzer tool and it includes the following:

- Wallet balances
- Transaction IDs

The data from the EY blockchain node for bitcoin has also been imported into the tool.

Note: Typically, the client also would provide a select sample of transactions that management initiated on behalf of the audit for the auditor to test for ownership (rights and obligations); however, this is not included for this case.

Analytics mindset

Digital assets

Part 5: Audit of Digital Assets Inc.

Section 2: Exploring the EY Helix Blockchain Analyzer for Public Networks for Students

Required

It’s time to explore! Open the analyzer and perform the following:

1. Home:
   a. Note your period of coverage already selected
   b. Note the transaction type already selected
   c. Read the disclaimer, privacy and copyright notice
2. Note the remaining dashboards and the ability to select buttons at the top of the tool or tabs at the bottom of the tool
3. Review each of the remaining dashboards:
   a. Note your filters:
      1. Change the period you are viewing for one tab (note that this will apply across dashboards)
      2. For the Understanding transactions tab, change the filter for the transaction type
   b. Note each analysis and what information is included in the analysis
   c. Select (mark) a data point and see how that selects data in the other analyses within that dashboard, use the Reset all markings button to deselect your selection or make another selection to change your selection (note that this will not apply across dashboards)
   d. Hover over a data point and see the tool tip
   e. Use an x-axis or y-axis slider to see how the data in the analysis changes
   f. Drag a side of the analysis to resize the contents relative to the other analyses in the dashboard

Analytics mindset

Digital assets

Part 5: Audit of Digital Assets Inc.

Section 3: Testing for completeness and existence

Required

As an auditor, you need to audit for certain assertions. Your first assertions are completeness and existence. In evaluating these assertions, you need to check if the given transactions exist and add up to the same end balance in the wallet. You also need to look for any unusual items (something suspicious or potentially risky).

1. Which of the analyzer tabs would you use? Explain why.
2. What are your findings?