Journal of Forensic and Investigative Accounting
Volume 15: Issue 3, Special Issue 2023

Bitcoin and Beyond: Crypto Asset Considerations for Auditors/Forensic Accountants

Daniel Dupuis
Debbie Smith
Kimberly Gleason
*Yezen Kannan**

Introduction

The market for digital assets is evolving rapidly, with new coins, instruments, and exchanges emerging on a continual basis. Technological changes in financial markets, such as the widespread use of blockchain technology and the use of digital assets—including cryptocurrencies for financial transactions—require auditors to reconsider the nature of the audit function (Broby and Paul, 2017). Blockchain technology poses many opportunities for the accounting profession, including vetting parties to transactions, advancing real-time accounting, incorporating artificial intelligence into the process of auditing, and providing assurance related to smart contracts. The Big Four accounting firms have made substantial investments in technology to facilitate the audit of cryptocurrencies. In fact, many large accounting firms offer client solutions that provide assurance regarding digital transactions. The subtitle of a November 2020 KPMG report is "Crypto assets have arrived," and Deloitte (2021) states, "It is becoming common for financial statements to show material cryptocurrency balances and to reflect the results of cryptocurrency transactions." Accordingly, the leading accounting firms, including Grant Thornton, Ernst and Young, KPMG, and PricewaterhouseCoopers, have announced a scalable hybrid-cloud platform to audit digital coin holdings and transactions and are currently active in management consulting targeting digital coin issues.

Arguing for more extensive coverage of digital assets in accounting courses, Smith (2018) states, "Keeping up with the pace at which cryptocurrencies change is a challenge for educators, especially since the technical nature of this subject can seem intimidating." Likewise for practitioners, accountants may not be as comfortable as they would like with virtual coins and other digital assets, and the microstructure of these assets. Audits reviewed in 2019 by the Canadian Public Accountability Board (CPAB) had deficiencies in seven of eight audit files involving clients with digital asset exposure, including auditors lacking an adequate understanding of audit approaches, failure to evaluate the reliability of information regarding digital assets provided by management and exchanges, and failure to obtain sufficient audit evidence related to claims regarding crypto assets (CPAB, 2019). Regarding inspections of auditors of clients with substantial virtual currency holdings, the PCAOB notes: "Observations from these inspections indicate the need for a greater focus by some auditors on the identification and assessment of the risks of material misstatement to the financial statements related to crypto assets, as well as the planning and performing of an appropriate audit response" (PCAOB, 2020).

There have also been surprises even for auditors regularly dealing with clients and their digital asset holdings: Friedman LLP resigned as the auditor of Tether in 2018—a stablecoin claiming to be backed by the U.S. dollar—upon discovering that new coins were being printed without USD reserves (Hochstein, 2018). In another instance, the U.S. auditor of FTX, Armanino, is defending a lawsuit due to FTX's lack of reserves (Conlon et al., 2022; Sor, 2022). On November 11, 2022, the third largest crypto exchange, FTX, filed for bankruptcy due to a severe liquidity crisis. Ultimately, the losses exceeded $7 billion (Tautman, 2022). Furthermore, one-fifth of all Bitcoin is lost simply because holders were careless with their passwords, a fact that should give accountants pause when assessing the risk associated with digital assets (Krause, 2018).

Given that auditors are tasked with ensuring that financial statements are free of material misstatements (fraudulent or not), evaluating the effectiveness of internal controls, and identifying illicit activity in the course of the client engagement,

*Department of Finance, School of Business Administration, American University of Sharjah, Sharjah, United Arab Emirates; Associate Professor, Asian Institute of Management, Manila, Philippines; Department of Accounting, Cleveland State University, Cleveland, OH USA; Department of Finance, School of Business Administration, American University of Sharjah, Sharjah, United Arab Emirates; Department of Accounting, Zayed University, Dubai, United Arab Emirates; respectively.

and given that products and services in crypto asset markets are continually evolving through a sequential process of innovation and regulation, auditors potentially confront an ever-changing landscape of liability from clients with significant digital holdings. As stated by U.S. Treasury Secretary Janet Yellen on February 11, 2021, "I see the promise of these new technologies, but I also see the reality: cryptocurrencies have been used to launder the profits of online drug traffickers; they've been a tool to finance terrorism (BBC, 2021)."

There are few papers providing a holistic explanation of digital assets, blockchain transactions, and the considerations required by these assets; we seek to fill the void in the literature.

The analysis proceeds as follows. We first describe the background content regarding the nature of digital assets and transactions using decentralized networks. We next address the current accounting treatment of digital assets, describe the breadth of business transactions that are particularly susceptible to malfeasance when conducted with digital currency, discuss potential liability from business relationships, evaluate fraud risk factors for auditing, review the effects of crypto assets on management assertions for audit clients with digital holdings, and assess the effects on internal control from the perspective of the COSO framework. We then describe several innovations in digital finance that are currently under development and may pose complexities for auditors, including central bank-backed digital coins, privacy coins, initial coin offerings, crypto secrecy jurisdictions, and dark web transactions.

Review of Digital Assets

1. Taxonomy of Money and Digital Assets

The concept of money has evolved over millennia, from the Rai stones of Yap Island to Roman coins, the early Chinese paper IOUs to the U.S. dollar, and recently, digital coins that do not require a physical form. The development of currencies from paper fiat to digital necessitates an aggregate perspective. Tokenization is defined as "the act of turning an asset, good, right, or currency into a representation with properties that suffice to attest to and transfer ownership." Tokenized systems rely on the recognition of a payment object, physical or not, such as stones, coins, paper or digital currency, non-fungible tokens (NFTs), etc. Account-based currencies, on the other hand, are rooted in the verification process – commercial bank accounts are a good example. Dupuis et al. (2021) discuss the taxonomy of money to distinguish four main categories: cash (USD, euros, yen, etc.), digital private coins (Bitcoin, Ethereum, etc.), deposit accounts (bank accounts) and central bank forms of money (foreign exchange reserves, settlement accounts and central bank digital currencies, aka CBDCs).[1,2] We focus on the nascent type, digital coins. From an accounting perspective, CBDCs represent a minor innovation, but digital coins like Bitcoin, Monero, Litecoin, and Dogecoin introduce a clear and present danger in the auditing process. Therefore, we primarily focus on digital coins.

There are over two thousand cryptocurrencies in existence, but many are get-rich-quick schemes or attempts at riding the wave of digitalization with little or no use-of-case scenarios. Of the top 20 virtual coins, Bitcoin is the front-runner, with Ethereum a close second. Other virtual currencies (Litecoin, Dogecoin, Cardano, etc.) jockey for position to fill the list. All share certain attributes: they are private (no issuing authority), digital (no physical form), decentralized (transactions processed by multiple computers, aka miners, as opposed to a single server), mostly transparent (anyone can see the transaction details) and anonymous (no name or identifier).

Non-fungible tokens (hereafter NFTs) have recently gained traction in the media and can be considered a new class of digital asset. Any amount of NFTs can be divided or merged (Voshmgir, 2020); in other words, ownership of the underlying asset can be fractioned. To facilitate understanding, we can pretend to create an NFT for the famous painting, "Mona Lisa." The painting remains at the Louvre and can be viewed (or copied) at will, but the creator (Da Vinci) can also sell the "right" to the original painting in a contract, written on paper, and separate from the underlying work of art. The NFT "rights" will differ for various assets, and the NFT paper contract can be sold independently from the painting as a separate asset—the tokenization part. In the digital world, NFTs exist for a large sample of chattels (art, digitized pictures, videos, collectibles, avatars, music, etc.). From famous tweets to digital art, they enshrine ownership in the form of a non-fungible (cannot be replicated) token recorded on a blockchain (generally ERC-20, Ethereum's blockchain). The NFT craze

[1] See also Bech and Garratt (2017) for a detailed explanation of the money flower and the associated categories.

[2] CBDCs, while digital, are issued by central banks and follow the same rules as traditional fiat without requiring a paper form. While many countries are presently considering or developing a digital currency, China is ahead of the curve and has even started distributing the e-yuan for public consumption.

is such that one of Elon Musk's famous tweets has sold for $1.1 million, while Jack Dorsey, Twitter's co-founder, sold his first tweet as an NFT for more than $2.9 million. While the NFT guarantees ownership of the tweet, the tweet's existence cannot be assured; if Twitter disappears, so does the underlying asset. Similarly, if the Louvre burns with the Mona Lisa, the Da Vinci contract (as an NFT) loses its value. Other notorious non-fungible tokens include a "six inches by three inches" patch of skin located between the elbow and shoulder of tennis player Oleksandra Oliynykova that sold for $5,000, giving the purchaser the right to "commission a tattoo or temporary body art."[3] The craze reached a peak with the minting and sale of an NFT for the digital art "Everydays: The First 5000 Days" by Beeple. The NFT was auctioned at Christie's for the paltry sum of $69 million and is presently used as wallpaper on many desktop computers … for free.[4] While the token is non-fungible, the digital art itself can be copied at will, in the same way that anyone could paint a similitude of the Mona Lisa—without claiming it as an original. From an auditing perspective, the NFT is a new type of digital token that can be considered an asset, but its valuation remains unclear.

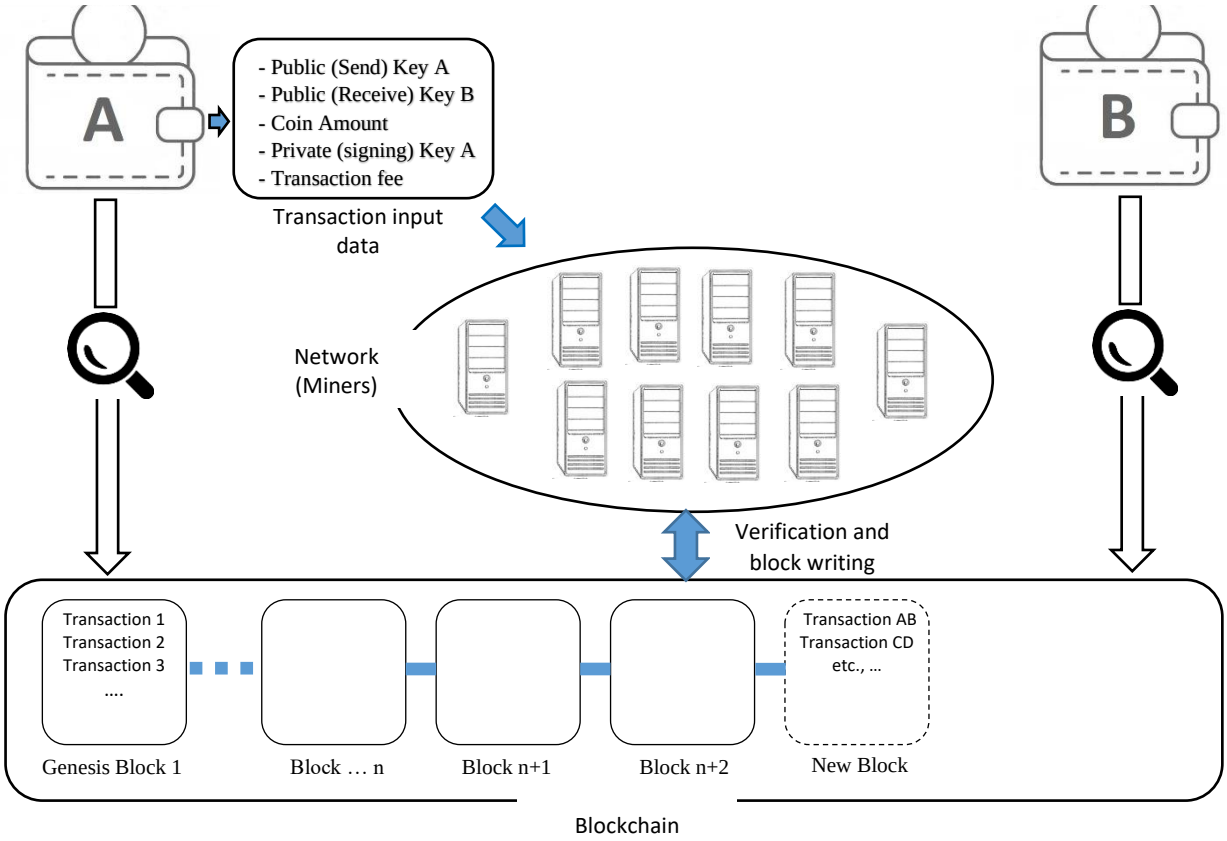
1.1. Anatomy of a Digital Coin Transaction

To verify and analyze a firm's digital coin holdings, auditors must first familiarize themselves with the microstructure of a cryptographic transaction, as it differs significantly from centralized ledger mechanics. The first step in the process is the conversion from fiat (dollar, euro, etc.) to digital coin, also known as the on-ramp procedure. There are three main gates to obtaining cryptocurrencies: organized exchanges, over the counter (OTC) trades to exchange fiat for virtual currencies, and "mining," where the controlling algorithm literally creates the coins.

Organized exchanges (i.e., Coinbase, Binance, Bitfinex, Kraken, etc.) are generally Know Your Client (KYC) compliant and function similarly to stock exchanges. Clients identify themselves, deposit fiat, and buy digital coins in the open markets. Alternatively, OTC transactions are private and anonymous, thus reducing traceability. Dupuis and Gleason (2020) describe in detail a transaction between two individuals completing a purchase of Bitcoin against $100,000 without even knowing the counterparty's name. The traders simply exchanged "send" and "receive" public keys, counted the money, and parted. This type of transaction should be rare in the corporate world but nevertheless exists as a possibility, complicating the work of the auditor who has no record of the transaction except in the form of a blockchain entry; hence the necessity to understand the anatomy of a digital trade. Figure (1) provides a graphical view of a (slightly simplified) trade in virtual coins.

[3] See https://bleacherreport.com/articles/10000555-tennis-player-oleksandra-oliynykova-sells-patch-of-skin-on-right-arm-as-nft-for-5k for details.
[4] See https://www.nytimes.com/2021/03/11/arts/design/nft-auction-christies-beeple.html for details.

Figure 1: Anatomy of a Digital Transaction



In the depiction above, agent A wants to send some coins to agent B. The transaction originates from a "wallet." In crypto terms, a digital wallet is like the billfold carried in one's pocket. The common understanding that the coins are "sitting" in wallet A is an oversimplification—the wallet does not hold the actual coins. The wallet is an anonymous data file containing an access identifier (password) and public and private keys. The public key is a unique alphanumerical chain like a mailbox address. Providing the key to a counterparty indicates the address where coins can be sent or received. For example, the string: "0202a406624211f2abbdc68da3df929f938c3399dd79fac1b51b0e4ad1d26a47aa" could be the receiving address for agent B. The private key is a cryptographic signature, encrypted prior to being broadcast, and should be guarded jealously in its unencrypted form. Private keys are available to view (and download) in most wallets, but few users keep a secured record (possibly due to ignorance). Private keys can be used to retrieve coins directly from the blockchain, bypassing the wallet; the equivalent of handing out paper currency from a physical billfold.

A digital wallet could be compared to a magnifying glass; the wallet simply consults the blockchain to ascertain coin ownership, using the cryptographic keys as a search instrument. The ownership data resides on the blockchain (not in the wallet!), and like a portal into a magical world, the wallet is simply the tool used to enter the blockchain to retrieve the information. Even if the wallet is lost (forgot your password?), the coins can be retrieved from the blockchain if the private keys assigned to all transactions were recorded. Since a digital wallet is merely a repository for strings of digits, it can take many forms. The most common are "hot" wallets; internet-based, accessed through a website, some allowing the downloading of private keys (e.g., Exodus) while others do not (most exchange wallets like Binance). Alternatively, "cold" wallets are considered more secure and do not connect to the web; they can take the form of a flash drive or simply a piece of paper inscribed with the precious private keys. Anything with a writing surface (digital or physical) can be a cold wallet; for example, a metal coin (e.g., Casascius physical bitcoins) with the private key written on an embedded piece of paper, covered with a tamper-proof hologram.[5]

[5] See https://news.bitcoin.com/last-month-casascius-physical-bitcoin-owners-redeemed-the-highest-number-of-coins-in-3-years/ for details.

As per Figure (1), if agent A wants to send coins to B, the application linked to wallet A will create an input data file containing the following information: the address or public "send" key of A, the public "receive" key of B, the coin amount and the transaction fee (often determined by the system). Finally, the application will add the encrypted private key of A, which is the equivalent of a digital signature. In a centralized system, the data packet would be sent to a unique consolidated ledger to be processed, with debits and credits tabulated as required. Most major cryptocurrencies (with the notable exception of XRP) function on a decentralized network. The data packet from wallet A is broadcast to thousands of computers called miners; their first purpose is to consult the blockchain and ascertain that sender A does, in fact, own the coins. Since there are no individual identifiers, the miners simply link the coins to the sender's wallet. Next, all miners will compete to write the data in a new block; only one will "win" and receive the transaction fee as well as a mining reward (denominated in newly-minted coins). The value of the reward follows a predetermined algorithm and shrinks by half every cycle (roughly 210,000 blocks for Bitcoin, or every four years). The deflationary algorithm is the reason the total amount of BTC will never surpass 21 million coins; the computation is asymptotic. Finally, the winning miner writes the data into the new block, linking it to the chain containing all previous transactions.

The newly minted blockchain is broadcast to all miners, and the cycle repeats. Agent B's wallet is now on record as the recipient of the transacted coins.

Note that most blockchains (except for Monero, Zcash, and a few others) are public, transparent, and open to scrutiny by anyone with a computer (Dupuis and Gleason, 2020). Multiple software applications allow the unrestricted retrieval of the entire transactional dataset, all the way to the genesis block. The path taken for all trades can thus be viewed easily, with a caveat; there are no identifiers (except the encrypted private keys) in the data. For example, an auditor can trace all the coins to a wallet but has no idea who owns it. Thus, anonymity is one of the main reasons behind the reluctance of regulatory authorities to allow corporate entry into the digital coin markets. The dilemma is obvious—if a wallet has no name or identification, how can an auditor prove ownership? Who actually owns the coins? As with bearer securities, the owner is whoever knows the password to the wallet!

1.2. Ownership, Custody, and Valuation of Virtual Tokens

Determination of ownership and security is relatively easy for direct private buyers but is problematic at the corporate level. The world of cryptocurrencies abounds with horror stories of investors losing all their funds because the wallet holder disappeared or lost access. According to Chainalysis, a digital tracking firm, close to 20% of all Bitcoin ($12 billion at the current price of $30,000/BTC) is lost permanently. An amplified quandary exists at the corporate level; if a single director maintains the firm's wallet access codes, the disappearance of just one individual can cause irreparable damage to the company. On the other hand, shared access will increase the probability of fraud or theft. In 2018, Gerald Cotton, founder, and CEO of Quadriga CX (a cryptocurrency exchange), died while traveling in India; taking with him the passwords to all of the investment fund's wallets that contained client digital currencies lid at more than CDN$ 250 million.[6] Since these coins were in a comingled exchange wallet, client funds were not segregated. The access to Cotton's laptop was also encrypted, and to date, no coins have been recovered. Similarly, the Mount Gox debacle of 2013 highlights the vulnerability of corporate control in the virtual coin era; the exchange was apparently hacked, and $460 million in client funds disappeared.[7] A cursory glance at the news provides dozens of similar stories; self-custody is clearly an issue in the world of digital assets.

All wallets, hot or cold, are devoid of identity, and auditors cannot ascertain ownership. Furthermore, KYC, the key to Anti Money Laundering (AML) compliance used by banks to meet requirements of the 1970 Bank Secrecy Act (Xu et al., 2021), cannot be verified. In response, the business community was relatively quick to devise a solution: third-party custodians. Firms such as Gemini, Coinbase Custody, Fidelity Digital Assets, and many others have developed safekeeping tools and undergone certification under various regulatory regimes. Since the 2021 price surge and the recent increase in institutional interest for major digital currencies, powerhouse banks like Goldman Sachs, JPMorgan, and Citi have also indicated their desire to enter the fray.[8] While third-party safekeeping might alleviate some auditors' concerns, other issues may arise: the custodian's insurance coverage, security protocol, and choice of cold or hot storage also require detailed investigation.

[6] See https://www.bbc.com/news/world-us-canada-47203706 for details.
[7] See https://www.wired.com/2014/03/bitcoin-exchange/ for details.
[8] See https://www.coindesk.com/goldman-sachs-to-enter-crypto-market-soon-with-custody-play-source for details.

The valuation of digital coins can also be problematic. Even stablecoins have not reduced risk as expected. Jalan et al. (2021) compared the volatility and risk of stablecoins as compared to Bitcoin. Investors did not price the stablecoins as having lower risk, and the authors conclude that stablecoins do not offer a safe-haven in cryptocurrency. Valuation is also affected by price manipulation according to evidence presented by Peterson (2021).

At first glance, virtual currencies that are traded on an organized exchange might appear to follow the same rules as stocks: the closing market price on a specific day provides an anchor point.[9] Unfortunately, the closing price is not useful for anchoring cryptocurrency prices. Bitcoin trades on hundreds of exchanges with major price differences. The most striking example is the "Kimchi" premium on South Korean markets (i.e., Bithumb, Upbit, Korbit, Coinone, etc.), where BTC sometimes trades at a hefty price premium that reached 63% in the spring of 2017.[10] Obviously, if a firm chooses to manipulate asset values or profits and losses, management could select a market and price that suits their needs. Like the ownership dilemma, the business community now provides a possible solution in the form of indices: a specific coin index that amalgamates the last available price on multiple markets and computes an average devoid of a premium or discount bias. Among others, Coindesk, Bloomberg, Kitco, and CME (Chicago Mercantile Exchange) all provide quotes for Bitcoin and other crypto indices with various constituent markets. More recently, S&P Dow Jones Indices, a leading index provider, has launched a series of digital market indices that include the S&P Cryptocurrency MegaCap Index, Bitcoin Index, and Ethereum Index, thus possibly facilitating the audit process.

While the most popular coins trade on open exchanges, valuation predicaments can arise with OTC trades and direct purchases (with self-custody wallets) of coins trading thinly or even inexistent on regulated markets. Initial coin offerings and airdrops resulting from a hard fork (when a new variation on the original digital coin emerges) are also subject to a valuation dilemma. OTC trades and peer-to-peer purchases do not generate a traditional auditable receipt, and estimating the cost basis or potential profit is problematic at best. Furthermore, some coins are not traded in open markets and may be considered like illiquid assets for accounting purposes. The existing regulatory framework has yet to provide a standardized solution to address these situations.

2. Current Accounting Standards and Digital Assets

The accounting ecosystem in which digital assets reside is in a state of evolution. Hsieh and Brennan (2022) comment that "it is the "wild west" for entities with material positions in crypto assets just trying to figure out on their own how to best report these crypto asset-related transactions and balances within existing accounting standards." Vincent and Wilkins (2020) stated that "neither the Financial Accounting Standards Board (FASB), the Auditing Standards Board (ASB), nor the PCAOB have issued formal guidance for accounting or auditing cryptocurrencies. Thus, the profession was relying on concept statements, principle-based accounting, and non-authoritative information such as white papers and other accounting and auditing publications." The AICPA only recently took a proposed position on the treatment of crypto assets. Accordingly, we next summarize the recent milestones related to the accounting treatment of cryptocurrency.

As of May 2022, the FASB had not yet added digital assets to its technical agenda but was conducting surveys and collecting information on the topic (FASB, 2022). The FASB was referring accountants to the nonauthoritative guidance based on the December 2019 Practice Aid, updated in 2022 (AICPA, 2022) and released by the AICPA's Digital Assets Working Group. Crypto assets were generally accounted for under Intangibles – Goodwill and Other, in accordance with Topic 350, as indefinite, intangible assets. Crypto assets are initially measured at cost, are not amortized, should be evaluated for impairment at least annually, and should be written down to the lowest fair value within a period. Losses are recorded as a reduction in net income, but reversals in value are not recorded. The Working Group determined that crypto assets do not meet the definition of cash and cash equivalents because sovereign governments do not back them. The Working Group also determined that crypto assets do not qualify as financial instruments or inventory.

The International Swaps and Derivatives Association asserts that the current guidance is misleading because it does not faithfully represent the economics of crypt assets, and they argue that crypto assets should be accounted for at fair value. In March 2022, members of the FASB's Financial Accounting Standards Advisory Council stated that treating crypto assets as intangible "does not make sense and should be improved," and they advocate presenting the assets separately on the

[9] Using a closing price for valuation is a simple solution, tempered by the fact that some stocks can be dually listed on two different exchanges, but generally, arbitrage forces ensure that both prices are similar enough to preclude a riskless profit due to mispricing net of transactions costs.

[10] See the CoinDesk analysis at https://www.coindesk.com/bitcoin-analysts-kimchi-premium-distress-signal.

balance sheet at cost basis with additional disclosures (FASB, 2022)."

To better assess where cryptocurrencies interface with the financial statements, many in the accounting community have called for the FASB to take more assertive action. Seven members of the U.S. Congress said that "lack of thoughtful and carefully developed authoritative guidance from the FASB threatens the ability to create accurate and consistent financial reporting of a large and fast-growing financial asset class."

Accordingly, in January 2023, the Digital Assets Working Group of the AICPA issued updates to its 2019 guidance, with a comprehensive practice aid for accountants and auditors related to digital assets, and on March 23, 2023, the FASB released new proposed standards related to, specifically, fungible digital assets (i.e., it did not take into account assets such as NFTs). The AICPA guidance reiterated its 2022 argument regarding the status of digital assets as intangible assets with indefinite lives, which should be recorded at cost, and subject to impairment (AICPA, 2023). For auditors, the 2023 AICPA guidelines address the recent FTX scandal, using the comingling of client funds and related party transactions extensively practiced at FTX as an example of the hazards auditors face in verifying the existence of digital asset holdings, valuation of less liquid digital assets, and the assessment of internal controls (AICPA, 2023). The 2023 AICPA practice aid has also come under fire for generating confusion and providing "non-answers" with item Question 25, which addresses SEC comments regarding lender de-recognition of cryptocurrency in a short-term lending arrangement, illustrating that many issues still remain unresolved (Ho, 2023). According to Section IV of AU Chapter 2 in the practice aid:

> Unlike traditional markets, the market for digital assets does not close, and an entity may inappropriately value its digital assets at times of the day that are not consistent across reporting periods and not in accordance with its valuation policies. This, in combination with the significant intra-day volatility of digital assets, could result in a material misstatement of valuation (Deloitte, April 25, 2023).

At the September 6, 2023, FASB meeting, the presentation of crypto assets and recognition of gains and losses was affirmed with only minor adjustments. The Board did not provide guidance on crypto related commissions and acquisition fees and did not include additional guidance on fair value measurement (Topic 820). This lack of guidance means that the initial acquisition of the asset could be priced differently from fair value depending on the terms, therefore requiring a change in book value on acquisition even though the fair value of the asset did not change (Deloitte, March 27, 2023). The update is effective for fiscal years beginning after December 15, 2024, with early adoption permitted. Thus, fair value was not required in 2023.

The 2023 FASB proposed standards are consistent with the AICPA in that it recommends cryptocurrency as intangible assets with indefinite lives but argues that cryptocurrency should be recorded at fair value rather than historical cost (Cohn, 2023). Further, the proposed FASB standards recommend recording cryptocurrency separately from other intangible assets on the balance sheet, and changes in fair value recorded separately on the income statement (Heaslip, 2023).

To date, there has yet to be a consensus worldwide on what kind of asset class digital coins represent. IASB staff recommends considering cryptocurrency as an intangible asset according to IAS 38, Intangible Assets, and for cryptocurrencies held for sale, Inventories (IAS 2) should apply. The Association of Chartered Certified Accountants (ACCA) notes that digital assets are not counted as cash under IAS 32 and IAS 7 (ACCA, 2021). The reasoning is that first, they are not "readily exchangeable" for goods and services, as they are not (at present) accepted as legal tender, and their use as a medium of exchange is not sufficiently widespread; and second, they exhibit substantial price volatility. Furthermore, crypto assets are neither debt nor equity and thus cannot be considered financial instruments.[11]

Under GAAP, another issue arising from financial reporting is the status of crypto holdings as intangible assets rather than investments. The volatility of cryptocurrency generates a bias in that losses yield write-downs, but gains cannot be revalued. Under IFRS (but not GAAP), because some digital coins trade in an active market, they can be revalued; ACCA (2021) points out that there are issues yet unresolved regarding the treatment of revaluation gains and losses. In any event, to record crypto asset holdings at fair value, the valuation of digital coins is required. For more liquid digital coins such as Bitcoin or Ethereum, valuation may be less complicated, but for less liquid coins, valuation poses a challenge and remains such even after the recent FASB proposal and AICPA guidance updates.

[11] They are also not considered inventory because they are not held for use during the ordinary course of business (unless the entity is a broker-dealer).

In an interesting development, on June 9, 2021, El Salvador adopted Bitcoin as a second national legal tender in addition to the U.S. dollar (thus formalizing Bitcoin as a currency) on which capital gains are not taxed (in other words, Bitcoin in El Salvador can no longer be treated as an intangible asset). For the first time, a digital asset has been officially adopted as a currency, and the valuation, accounting, and auditing implications for entities in El Salvador or other countries that might later adopt a similar strategy are, yet, unclear (Gerard, 2021).[12]

In the U.S., IRS Notice 2014-21 addresses the tax treatment of digital assets for businesses and individuals. The IRS states that "Transactions involving a digital asset are generally required to be reported on a tax return." Accordingly, gains and losses associated with digital assets are taxable events. The IRS further states that "For federal tax purposes, virtual currency is treated as property."

3. Variety of Business Transactions

When one thinks about the typical crypto audit client, a bitcoin mining firm, or a visible company like Tesla holding bitcoin on the balance sheet comes to mind. However, audit clients may confront many scenarios related to client exposure to digital coins, and digital coin transactions suggest heightened skepticism due to the anonymity associated with cryptocurrency. In addition to holding digital coins on the balance sheet and making and accepting payment using digital coins for goods and services, firms publicly traded on U.S. exchanges currently engage in activities such as paying interest on debt, raising capital through Initial Coin Offerings (ICOs), generating cryptocurrency revenues from mining and selling cryptocurrencies, using digital coins as collateral for loans, extending dividends with cryptocurrency, paying executives with cryptocurrency, earning gains on cryptocurrency derivatives, using cryptocurrency as payment in acquisitions and other intercorporate investments, trading crypto assets, or some combination of activities. The city of Miami adopted a plan to use Bitcoin to pay employees with Bitcoin and allow residents to pay their property taxes in Bitcoin (Feuer, 2021; Slisco, 2021). Even after the collapse in Bitcoin pricing, the city's mayor, Frances Suarez, tweeted in January 2023 that he still receives his salary paid in Bitcoin (Brown, 2023). As an example of the breadth of crypto asset activity by a single audit client of Hay and Watson LLC, First Bitcoin Capital Corporation (First Bitcoin, 2021) discloses several activities in its registration filings:

> On December 31, 2018, the Company entered into an agreement to issue 600 million BIT tokens, a digital currency, to Kronos Advances Technologies Inc. (Kronos), a Company trading on the OTC Pink Open Market in the United States of America, in exchange for a $1 million convertible promissory note. The note bears simple interest at 5% per annum, matures on December 31, 2023, and is convertible to common shares of Kronos at any time after June 30, 2019, at a price per share that is 80% of the market price at the time of conversion. (Collateral for a loan)
>
> During the year ended December 31, 2018, the Company entered into an agreement whereby Medical Cannabis Payment Solutions, Inc., a company trading on the OTC Pink Open Market in the United States of America, issued 2,000,000 common shares to the Company in exchange for a project analysis and technical information on WEED tokens. The shares were recognized as payment for consulting services with an initial fair value of $76,000. (Payment for services)
>
> The Company holds five million common shares of Singlepoint Inc., a company trading on the OTCQB Venture Market in the United States of America. The shares were acquired on August 3, 2017, through the exchange of one million WEED coins, a digital currency which was recorded at nominal value. (Payment in an acquisition)
>
> On August 2, 2017, the Company approved a 10% quarterly dividend to its shareholders of record as of September 12, 2017, to be paid with the digital currency TeslaCoilCoin ("TESLA coin"). (Payment of a dividend)
>
> On July 22, 2019, the Company entered into an agreement with Digital Asset Monetary Network Inc. (DigitalAMN), a company traded on the OTC Pink Open Market in the United States of America, whereby the Company transferred 1 billion First Bitcoin (BIT) coins, a digital currency, to DigitalAMN in exchange for 10,000 shares of DigitalAMN's Series BB Convertible Preferred Stock. (Payment in an intercorporate

[12] Whether El Salvador's adoption of Bitcoin as a second national legal tender, after September 7, 2021, will be effective in attracting remittances from abroad in a country where only 45% of residents have internet access remains to be seen.

investment)

During the year ended December 31, 2017, the Company issued 3,415,924 common shares in trust as compensation for third parties who had "mined" the Company's BIT digital currency and traded the BIT digital currency for the Company's BITCF digital currency. (Payment to employees)

On February 6, 2006, the Company acquired mining rights to mineralized property in the Pacaraima region in Southern Venezuela. Acquired rights included the Cerro Trompa Mine located eight kilometers northeast of Icabaru and other mining properties, including the San Miguel, Mosquito and Zapata Mines. On November 18, 2016, the Company exchanged its mining rights for one billion KiloCoin, a digital currency valued at $398,000, and recognized a gain on exchange of $38,000 (Payment for mining rights)

Payable to related parties includes $11,849 due to the Company's Chief Executive Officer (December 31, 2017 - $197,500) and $4,848 due to a company owned by the Company's Chief Executive Officer (December 31, 2017 - $4,848). During the year ended December 31, 2018, the Company recognized a gain on settlement of amounts due to the Company's Chief Executive Officer of $205,102 (2017 - $154,179) as a result of being settled with 20,000 Bitcoin Futures (XBU) digital currency (December 31, 2017 – 2,000 XBU). (Executive compensation)

4. Liability from Business Associates

In making client acceptance and continuation decisions, auditors must evaluate their engagement liability arising from inherent risk (the risk of failure to detect a material misstatement due to factors unrelated to internal control failures) and business risk (the potential loss of value to the auditor arising from being named in litigation if the client goes into distress due to factors beyond the scope of the audit). Many of the inherent risk factors associated with client digital asset exposure are straightforward: transactions are complex, such as clients issuing their own tokens to raise capital that is not traded on an organized exchange, generating uncertainty about the valuation of the tokens. However, other sources of inherent risk are not as immediately apparent. For instance, Bit Digital's 2020 Annual Report illustrates inherent risk arising from the inability of the company to screen counterparties through the blockchain due to the nature of the technology:

> … because of the pseudonymous nature of blockchain transactions we may inadvertently and without our knowledge engage in transactions with persons named on (the Office of Foreign Asset Control) OFAC's Specially Designated Nationals (SDN) list. Our Company's policy prohibits any transactions with such SDN individuals, but we may not be adequately capable of determining the ultimate identity of the individual with whom we transact with respect to selling bitcoin assets. Moreover, federal law prohibits any U.S. person from knowingly or unknowingly possessing any visual depiction commonly known as child pornography. Recent media reports have suggested that people have imbedded such depictions on one or more blockchains. Because our business requires us to download and retain one or more blockchains to effectuate our ongoing business, it is possible that such digital ledgers contain prohibited depictions without our knowledge or consent.

Clients are also exposed to the risk of being named in litigation because of client bankruptcy. As an example of digital asset-related business risk exposure, Riot Blockchain (Riot, 2021) states:

> The trading prices of our common stock have appeared at times to have been correlated with the trading prices of bitcoin. Specifically, we have experienced adverse effects on our stock price when the value of bitcoin has fallen, and we may experience similar outcomes if our stock price tracks the general status of that cryptocurrency. Furthermore, if the market for bitcoin company stocks or the stock market in general experiences a loss of investor confidence, the trading price of our stock could decline for reasons unrelated to our business, operating results, or financial condition. The trading price of our common stock could be subject to arbitrary pricing factors that are not necessarily associated with traditional factors that influence stock prices or the value of non-cryptocurrency assets such as revenue, cash flows, profitability, growth prospects or business activity levels since the value and price, as determined by the investing public, may be influenced by future anticipated adoption or appreciation in value of cryptocurrencies or blockchains generally, factors over which we have little or no influence or control.

Following the establishment of Bitcoin, an increasing number of firms have begun to hold significant digital asset

balances, including Tesla, MicroStrategy, Paypal, Overstock.com, and Square Inc. Providing a quality audit for these clients becomes more of a challenge in the presence of significant virtual instruments and transactions, through all audit phases and starting from the client engagement phase.[13] From the initiation of the client engagement, auditors need to be able to evaluate whether the cryptocurrency transactions are significant and part of the business of a client. As per Craig-Bourdin (2018), regarding the assessment of client integrity and engagement:

> If the auditor identifies significant cryptocurrency transactions that are outside the normal course of business, the auditor is required to evaluate whether it gives rise to significant risks, inquire of management about the nature of these transactions and whether related parties could be involved, and whether the business rationale (or the lack thereof) suggests that they may have been entered into to engage in fraudulent financial reporting or to conceal misappropriation of assets. The auditor is also required to remain alert to the possibility of instances of non-compliance or suspected non-compliance with laws and regulations, including money laundering or other illegal activities.

The AICPA (2020) has also provided a guide on the risks associated with digital assets. They point out that auditing firms should be concerned with developing their knowledge base to perform quality audits of digital asset accounts and blockchain transactions when making client acceptance and continuation decisions and make hiring decisions that bring in employees with a sophisticated knowledge of cybersecurity and information technology. Liu (2020) argues that audit firms should also provide extensive, regularly updated training material to enable their staff to keep up with rapid developments in regulations and technology. Poorly informed management also poses hazards to auditors due to weak recordkeeping and internal controls, and auditors need to assess client integrity given that the complexity of crypto asset transactions may facilitate illegal activities. Auditors should consider the influence of crypto assets on internal controls and the assessment of management integrity in client acceptance decisions. Smith (2020) projects that "as emerging technologies such as blockchain, robotic process automation, and artificial intelligence become more prevalent, the potential risk of performing an inadequate risk assessment process will continue to increase." The AICPA (2020) notes that continuing assessment of how a client uses digital assets and tests of the client's controls are essential for client consideration decisions, particularly if the client self-stores digital assets rather than using a third-party custodian. In its 2023 update, the AICPA reiterated the importance of auditors in identifying client noncompliance with AML regulations (AICPA, 2023).

5. Fraud Risk Factors

As of May 2020, the PCAOB has provided guidance for the auditors of clients with significant or material cryptocurrency holdings, as follows:

> Some of those issues may involve fraud: 'In identifying fraud risks, the discussion among the key engagement team members about the potential for material misstatement due to fraud may include, for example: the risk of management override of controls over the private keys, which may result in misuse or misappropriation of holdings of crypto assets by those who control the keys; the susceptibility of the financial statements to material misstatement through transactions with related parties; the related parties' identified may be difficult to ascertain because of the pseudonymous nature of transactions involving crypto assets.'

Bit Mining LTD (Bit Mining, 2021) describes the risk of fraud arising from the microstructure of crypto asset transactions in its 2021 Annual Report:

> Cryptocurrencies that are represented and trade on a ledger-based platform may not necessarily benefit from viable trading markets. Stock exchanges have listing requirements and vet issuers; requiring them to be subjected to rigorous listing standards and rules and monitor investors transacting on such platform for fraud and other improprieties. These conditions may not necessarily be replicated on a distributed ledger platform, depending on the platform's controls and other policies. The laxer a distributed ledger platform is about vetting issuers of cryptocurrency assets or users that transact on the platform, the higher the potential risk for fraud or the manipulation of the ledger due to a control event.

Auditors should have a strong understanding of the cryptocurrency purchase and usage cycle of their audit client as

[13] Audit quality is the "market assessed joint probability that a given auditor will both discover a breach in a client's accounting system, and report the breach (DeAngelo, 1981, p. 186)."

well as brainstorm at the beginning of the audit (the planning phase) to identify and incorporate the unique features of cryptocurrency in their initial risk assessment (inherent, fraud and control risks) and incorporate crypto asset procedures into their audit programs to be able to detect and report on any material misstatements, whether due to error or fraud. Unlike holdings of other financial assets which are grounded in legal contracts, in digital form, or as a hard copy (such as mortgages, bonds, or shares of equity), cryptocurrency holdings are verifiable primarily through third-party custodians who are liable for misstatements, or through private keys that are accessible in self-directed wallets—the ability of auditors to verify accounts is thus in part a function of the reliability of the blockchain.

Accordingly, auditors should practice professional skepticism regarding audit clients' cryptocurrency holdings, the legalities of digital operations and trades, and the soundness of the internal control framework over these transactions, including the information technology controls. Furthermore, the audit team needs to assess the adequacy of staff expertise, security controls, and protection in their investigation of third-party custody solutions. In addition, the anonymity provided by blockchain technology could potentially be used to disguise transactions with related parties, which constitutes another fraud risk factor, as companies might fail to fully disclose such transactions.

Additional sources of liability can arise when clients conduct significant business using cryptocurrency if, for instance, auditors lack the necessary expertise to evaluate the quality of the information technology utilized and the client's holdings are subsequently stolen by hackers or parties internal to the firm; or if a private key corresponding to a self-serve wallet is stolen or irretrievably lost due to poor internal control. Furthermore, the ability to verify digital deposits is complicated by the potential for entities to misrepresent ownership, as wallets are anonymous.

In addition to the risk of fraud, clients can also face counterparty risk in crypto asset trades, thus exposing themselves to money laundering charges - given the pseudonymous nature of the transaction. For firms that operate crypto-to-fiat asset exchanges or operations in which they facilitate the purchase of digital assets, new regulatory requirements may also be underway to prevent crypto asset laundering. The Financial Crimes Enforcement Network proposed new KYC requirements on cryptocurrency exchanges for transactions over $10,000 consistent with bank AML requirements. In addition, more extensive recordkeeping for transactions over $3000 for customers managing their own private keys has been proposed. Whether the Biden Administration will implement these regulations remains unclear (Young, 2021).

6. Management Assertions for Digital Assets

Even before the new millennium and prior to the establishment of Bitcoin by Nakamoto in 2008, the accounting profession experienced an underlying transformative change due to the widespread use of the internet and electronic data in financial transactions. Rezaee and Reinstein (1998) state that the advancement of innovations in technology, "… signal the end of the traditional audit." Auditors are required to conduct an audit, provide reasonable assurance on the accuracy of the client's financial disclosures, and express an opinion on the effectiveness of the firm's internal controls. However, few academic papers address the implications of crypto asset holdings for auditors. Broby and Paul (2017) exceptionally provide a technical overview of how distributed transaction and custody records present challenges for auditors. They state that audit risk "… is intensified when technological complexity is taken into account," such as the technology underlying blockchain transactions.

While conducting a quality audit auditors must investigate and provide evidence on management assertions regarding significant crypto accounts (existence/occurrence, completeness, valuation, rights and obligations, and disclosure and presentation), as well as firms' compliance with rules and regulations through their assessment of the effectiveness of a firm's information system. We next build upon Vincent and Wilkins (2020), who provide a proposed framework for audit procedures and additional consideration related to each of the management assertions by defining and discussing such assertions from a crypto asset perspective.

The management assertions are as follows:[14]

a. Existence/occurrence: The auditor must document persuasive evidence that the assets or liabilities reported in the financial statements exist at the balance sheet date, and those recorded transactions occurred during the given period.

Unlike tangible assets such as cash on hand or inventory, auditors cannot physically inspect cryptocurrency holdings or question a third party about the client's holdings (Croner-I, 2019). The digital tokens of audit clients will likely be held

[14] AS 1105: Audit Evidence, Paragraph .11; https://pcaobus.org/oversight/standards/auditing-standards/details/AS1105.

in a qualified third-party custodial account (such as BitGo, Coinbase Custody, Gemini, Kingdom Trust, or itBit) rather than in a private wallet.[15] With regard to crypto asset accounts, the auditors will only see the wallet held by the client, which is a direct reflection of the blockchain data. Since there is no identifier in the wallet, they cannot verify the identity of the wallet owner; the auditors only see the resulting keys identified with encryption that cannot be reversed-engineered. The auditor can see that wallet A has a certain number of coins and that the record is time stamped.

An auditor may consider walking away from clients who rely on self-serve wallets (rather than holding crypto assets with a custodian). If there is suspicion from the auditor's perspective that the client owns private wallets, there is a likelihood that a devastating loss could occur due to the client losing access to the account or a hacker obtaining the private keys and draining the account. If the client uses a third-party custodian for holding digital assets, the auditor may be able to get verification of existence if the client gives the auditor authorization. However, even if the client holds digital assets through a custodian, the comingling of assets (where coin ownership is recorded on a proprietary centralized system, off-chain) may complicate the verification process. The auditor must decide if the custodian's confirmation of the client's digital asset holdings is reliable and acceptable audit evidence (AICPA, 2020).

An alternative to a third-party custodian is for the client to divide the private key(s) using Shamir's secret-sharing schemes into six to seven multiple pieces held by the corresponding number of executives within the firm that can be used to reconstruct the keys.[16] Should the primary authorized executive holder die without a strategy to pass the key to another qualified individual within the organization, a governance structure must be in place as a control so that a certain proportion of the five to seven executives are present with their segments of the private key to authorize transactions. The auditor would then be able to (1) ensure that the individuals with the key or with segments of the key are informed about the relevant internal control procedures and (2) obtain some verification of the existence of digital coins held by the company.[17]

Another potential concern for auditors regarding the existence assertion arises when companies or funds with crypto asset holdings can falsely claim they are insured against loss or theft of crypto assets and then suffer a hack or some other security compromise. The likelihood of hacking depends on the physical security procedures set by the custodians (for example, cold storage and military-grade security protocols). Thus far, there are no examples of third-party custodians being hacked, although Ethereum wallets from an exchange were hacked in 2017, resulting in the loss of $300 million in ether. The regulatory oversight and security level of custodians is greater than that of crypto exchanges, as they are generally regulated under U.S. Treasury and state banking laws, but it is not unreasonable to believe that a custodian could potentially suffer from a sophisticated attack, causing the audit client to lose their crypto asset holdings. For instance, as stated in the annual report of Marathon Digital Holdings (Marathon, 2021), a Bitcoin mining company:

> Security breaches and cyberattacks are of particular concern with respect to our bitcoin. Bitcoin and other blockchain-based cryptocurrencies have been, and may in the future be, subject to security breaches, cyberattacks, or other malicious activities. A successful security breach or cyberattack could result in a partial or total loss of our bitcoin in a manner that may not be covered by insurance or indemnity provisions of the custody agreement with a custodian who holds our bitcoin.

Auditors should also identify that the exchanges on which clients purchase digital assets are reputable. Recently, a cryptocurrency exchange in Turkey, Thodex, was abruptly closed after misappropriating funds that were supposed to be used to buy cryptocurrency. The exchange went offline, and the founder of the exchange fled from Turkey to Albania in April 2021 with the proceeds of 400,000 customer accounts, transferring nearly $108 million offshore. Without knowledgeable staff and appropriate controls, audit clients may not realize that, due to fraudulent exchanges, they have not successfully purchased digital coins; a second major Turkish exchange, Vebitcoin, also collapsed (Ackerman, 2021).

Another significant digital asset fraud incident occurred in 2022 with FTX, an Antigua and Barbuda-incorporated cryptocurrency exchange founded in 2019 by Sam Bankman-Fried. At its founding, FTX was part of an investment fund, Alameda Research, run by Bankman-Fried's social companion, Caroline Ellison. Alameda Research continued to function

[15] A private, or "self-serve," wallet is a portal into crypto holdings that is available on devices such as a mobile web device accessible by a private key, where the user has direct access to their holdings. With private (non-public) wallets, only the owner of the crypto assets knows the private key. The sole responsibility lies with the owner of the crypto asset to keep track of the keys to the account. Custodial, or cold storage, wallets are held by an entity tasked with the responsibility of keeping the account secure.

[16] For more information on Shamir's secret schemes, see https://people.eecs.berkeley.edu/~daw/teaching/cs276-s04/22.pdf.

[17] The authors thank Bill Zhang, a consultant with Accenture, for this information.

as a "sister company" to FTX. The collapse of the exchange was triggered by the disclosure that Alameda Research had significant (approximately $5 billion) holdings of the FTX token, FTT, raising questions regarding leverage in the form of loans made by FTX to Alameda Research to "plug" losses using customer deposits at FTX. A rival exchange, Binance, then liquidated its holdings of FTT, yielding a catastrophic drop in the value of the token. After the assets of FTX were frozen by the Security Commission of the Bahamas, funds were then diverted from FTX through "unauthorized withdrawals." The FTX scandal highlighted the necessity of "proof of reserves," a mechanism through which the existence of customer deposits can be verified at any point in time (for a detailed review of the FTX scandal, see Conlon et al. (2022). Total losses at FTX exceeded seven billion dollars (Corinne et al., 2022). The U.S. auditor of FTX, Armanino, is defending its work against legal claims filed by customers of FTX (Sor 2022).

b. Completeness: "All transactions and accounts that should be presented in the financial statement are so included."

Auditors should be concerned that a client may improperly disclose digital holdings, whether intentionally or unintentionally. If intentional, customers may have incentives to hide or postpone recording certain transactions in the period they occur, although firms tend to overstate assets rather than understate them. An incentive to underreport (any material amount that could significantly reduce the informativeness of financial statements and the following decisions) could be to reduce or delay realized profits as a tax avoidance or deferral mechanism. Also, if the firm's management believes they will achieve their targets in a certain period, they may resort to a cookie-jar reserve method of earnings management, postponing or hiding crypto transactions and the ensuing gains until future periods.

Unintentionally, a firm may fail to record all digital asset transactions due to sloppy accounting or a lack of internal controls, resulting in omitted transactions that do not appear in the financial statements. Moreover, hidden assets in international firms could opportunistically be spent on activities that violate the Foreign Corrupt Practices Act. Auditors should conduct due diligence to ensure the quality of internal controls.

c. Valuation or allocation: "Asset, liability, equity, revenue, and expense components have been included in the financial statements at appropriate amounts."

A major concern for auditors regarding the valuation of crypto assets arises from the fact that the initial purchase price is not always evident (and whether they were purchased at a premium or not), and measures of current market values can be misleading. RIOT Blockchain's 2021 Annual Report provides evidence regarding issues that can arise from the valuation assertion, noting: "There are not well-regulated markets for bitcoin (or for other cryptocurrencies) and the industry is, in large part, dependent on underregulated third-party reporters to establish a market price for bitcoin."

Further, as the FASB presently classifies digital coins as "indefinite-life intangible assets," cryptocurrency holdings are subject to impairment based on a significant decline in value below the purchase price. The difficulty in identifying the exact purchase price, under the backdrop of speculative, volatile, and inconsistent market values, causes issues in determining gains or losses and recognizing impairments. For instance, Tesla and Microstrategy will face substantial impairment charges due to their economically significant Bitcoin holdings; the net gain for Tesla for the first quarter of 2021 was reduced by $27 million because of their digital exposure, and MicroStrategy announced losses of at least $285 million on their Bitcoin holdings (Hamacher, 2021).

Consistent with the valuation of illiquid assets, many crypto assets are thinly traded and highly volatile, thus adding another layer of difficulty to verifying and assigning an appropriate value. Furthermore, the price of Bitcoin varies by jurisdiction. For instance, crypto asset prices on South Korean exchanges reflect a "Kimchi" premium compared to other exchanges because of capital controls in South Korea; if a company wants to inflate the value of assets, it can do so by recording the transactions based on the South Korean prices.

Another issue arising from the valuation assertion is that auditors might need more information to determine that certain digital coins are worthless. For example, Dogecoin, a parody coin with no actual use-case scenario, created solely to illustrate the absurdity of speculation in worthless digital coins, has recently reached $0.68 per coin due to repeated tweets by Elon Musk. Auditors should question the legitimacy of client digital coin holdings and verify that all coins are fairly priced on organized exchanges to ascertain value. Further, exchange frauds, such as Thodex, could undermine confidence in digital assets, causing a sharp, sudden decline in their value.

d. Rights and obligations: "Auditors are required to verify that the client controls rights to the assets, and liabilities

are obligations of the company at a given date."

The ownership assertion requires the auditor to evaluate client controls over the initiation and authorization of digital asset transactions, such as the location of private keys, the number of users required to authorize transactions, and the segregation of duties in the authorization process (AICPA, 2020). Within the rights and obligations assertion, an auditor should be careful when engaging with a client who owns self-serve wallets, as previously mentioned. Companies with significant virtual holdings should implement a custodial solution. Nevertheless, crypto assets may still pose challenges for auditors even if the client uses a custodial solution because a firm could indicate that they own crypto that was previously applied for payment in an off-book or OTC trade. Related party transactions increase the risk of malfeasance.

e. Presentation and disclosure: Auditors must attest that the components of the financial statements are properly classified, described, and disclosed. Given that the accounting standards for crypto assets are not fully developed, evaluating presentation and disclosure may also be problematic for auditors. New regulation or regulatory changes could impact audit clients through the financial consequences associated with restatements as illustrated in the Bit Digital 2021 Annual Report (Bit Digital, 2021):

> Because there has been limited precedent set for the financial accounting of cryptocurrencies and related revenue recognition and no official guidance has yet been provided by the Financial Accounting Standards Board, the Public Company Accounting Oversight Board or the SEC, it is unclear how companies may in the future be required to account for bitcoin transactions and assets and related revenue recognition. A change in regulatory or financial accounting standards could result in the necessity to change our accounting methods and restate our financial statements. Such a restatement could adversely affect the accounting for our newly mined bitcoin rewards and more generally negatively impact our business, prospects, financial condition, and results of operation. Such circumstances would have a material adverse effect on our ability to continue as a going concern or to pursue our business strategy at all, which would have a material adverse effect on our business, prospects or operations as well as and potentially the value of any cryptocurrencies we hold or expect to acquire for our own account and harm investors.

Riot Blockchain also describes a potential problem with the lack of clear guidance regarding crypto revenues obtained from mining activities:

> Fair value of the cryptocurrency award received is determined using the quoted price of the related cryptocurrency at the time of receipt. There is currently no specific definitive guidance under GAAP or alternative accounting framework for the accounting for cryptocurrencies recognized as revenue or held, and management has exercised significant judgment in determining the appropriate accounting treatment. In the event authoritative guidance is enacted by the FASB, the Company may be required to change its policies, which could have an effect on the Company's consolidated financial position and results from operations.

7. Integration of Digital Assets into the COSO Framework

Most auditors assess internal control over financial reporting with the COSO Framework. Accordingly, there are five internal control components to achieve these objectives: the control environment, risk assessment, control activities, information and communication, and monitoring. The auditor must examine the client management's assessment and summary of the effectiveness of design and effectiveness of the internal controls and disclose the auditor's findings, in accordance with SOX 2002. Liu et al. (2019) argue that auditors will have to rely more on internal controls to provide assurance for firms that are using permissionless blockchain transactions.

Digital assets are relevant to the COSO framework in several ways. For the control environment component, there should be ongoing development of human resources internal to the firm and an informed and empowered board of directors, including the audit committee, so that the client management team is aware of activities and policies related to digital assets. Multidivisional training is necessary to facilitate the transfer of information between the accounting and finance functions. The auditor should evaluate the ability of the management team and internal audit function to deploy data analytics to detect any anomalies in blockchain transactions and ensure that adjustments are made. The auditor should conduct analytical procedures to assess the quality of the internal controls and note the "tone at the top" regarding transparency and ethical considerations. Auditors should ensure compliance with any new KYC regulations for clients engaged in cryptocurrency mining or facilitating crypto-to-fiat exchange.

In the risk assessment component, management should ensure that risk identification and analysis related to digital asset exposure occurs, and auditors should verify that management is cognizant of risks, including price risk due to volatility of digital assets or illiquidity. Firms should be continually evaluating exposure to various digital assets. Further, security risks require ongoing monitoring and assessment by qualified personnel across divisions reporting to the board of directors and management team. The security of private keys should be maintained, and potential risks to third-party custodians should also be considered. The auditor should assess whether the client has adequate protection against a security violation or other catastrophic event resulting in the loss of digital assets and recommend the use of an entity, such as Chainalysis or Kroll, with experience in private investigation of the theft of digital assets, should such an event occur.

Control activities are also critical, including policies, procedures, and security protocols to ensure the safe custody of digital assets and prevent the improper recording of transactions. The firm should conduct ongoing risk assessments and implement controls to mitigate or reduce exposure to identified risk.

Communication (both internal and external) between management, the audit committee, the internal audit function, the finance function, and the external auditor should be informative and frequent. The auditor should ensure that there is a forum available in which staff can report concerns regarding activities related to digital assets. Finally, ongoing monitoring of transactions involving digital assets, the external evaluation of processes for accounting for digital assets and reporting and follow-up on both design and operation deficiencies in processes involving digital assets should occur. However, as the industry evolves in terms of the development of internal controls, criminals also develop their tactics, as explained by Bit Mining LTD:

> Several errors and defects have been found previously, including those that disabled some functionality for users and exposed users' information. Exploitations of flaws in the source code that allow malicious actors to take or create money have previously occurred. Despite our efforts and processes to prevent breaches, our devices, as well as our mining machines, computer systems and those of third parties that we use in our operations, are vulnerable to cyber security risks, including cyber-attacks such as viruses and worms, phishing attacks, denial-of-service attacks, physical or electronic break-ins, employee theft or misuse, and similar disruptions from unauthorized tampering with our mining machines and computer systems or those of third parties that we use in our operations.

Regarding controls to protect the security of digital asset holdings, The 9 Inc.'s 2021 annual report states (The 9 2021):

> Cryptocurrency transactions are entirely digital and, as with any virtual system, are at risk from hackers, malware, and operational glitches. Hackers can target cryptocurrency exchanges and cryptocurrency transactions, to gain access to thousands of accounts and digital wallets where cryptocurrency is stored. Cryptocurrency transactions and accounts are not insured by any type of government program and all cryptocurrency transactions are permanent because there is no third party or payment processor. Cryptocurrency like Bitcoin has suffered from hacking and cyber-theft as such incidents have been reported by several cryptocurrency exchanges and miners, highlighting concerns about the security of Bitcoin and other cryptocurrencies, and therefore affecting their demand and price. Also, the price and exchange of cryptocurrency may be affected due to fraud risk. While cryptocurrency uses private key encryption to verify owners and register transactions, fraudsters and scammers may attempt to sell false cryptocurrencies. All the above may adversely affect our operation and the economic return of our cryptocurrency mining business.
>
> Currently, our Bitcoins received from the Bitcoin mining pool are stored in our Bitcoin electronic wallet. The wallet is designated to have a dedicated multi-signature system. It takes approval from a majority of signatories to transfer Bitcoins out from our wallet. Six of our management level employees were assigned as the signatories of such an electronic wallet. Each signatory holds an electronic private key password. To ensure the password will not be forgotten or lost by the signatory, each password is kept in a safe box at a bank. The safe boxes are registered under the accounts of two of our wholly owned subsidiaries. Despite our efforts and measures to ensure the safety of our cryptocurrencies and the transactions, there can be no assurance that such efforts or measures are effective. We may still suffer from cryptocurrency hacking and fraud and the economic return of our cryptocurrency mining business may be materially and adversely affected.

8. Innovations in Digital Asset Markets and Considerations for Forensic Accountants

The market for digital assets is rapidly changing, and ongoing innovations might further complicate the auditor's work. We thus provide insights into such cryptocurrency innovations that can raise the liability associated with client engagement—the implementation of Central Bank Backed Digital Coins, hedging instruments, Initial Coin Offerings, innovative spins on traditional financial statements (fraud schemes), the creation of new dark web tools, the emergence of sophisticated privacy coins, and the establishment of crypto secrecy jurisdictions.

a. Central Bank Digital Coins (CBDCs)

Several central banks have announced the intention to establish their own digital coins to use as legal tender including the Marshall Islands and Sweden. China began testing its central bank digital coin, the Digital Yuan, in April 2020 and has expanded throughout China (Benzmiller, 2022). The form of CDBC enacted could impact the auditor's perception of risk and would vary by which type (wholesale or retail CBDC) that would be implemented, depending on whether the digital coin takes the form of an account (through the central bank, which would retain account information and identities) or as tokens, where a bank would act as an intermediary and clear transactions with the central bank on behalf of their client.[18] Regardless of the form central bank digital currencies may take when introduced, auditors need to acclimate to evaluate financial statements for clients with CBDC transactions.

There is substantial speculation that both the commercial banking sector and the accounting profession face an existential threat under a wholesale CBDC regime. Thanks to the role of the central bank in administering accounts and settling transactions, as well as the transparency provided by the blockchain, there may be less of a need for assurance services. However, auditors still must ensure that financial statements are free of material misstatements and that internal controls are sound; in addition, they will continue to provide management consulting and tax advising. The profession also can respond by pioneering new artificial intelligence and machine learning protocols as new technical skill requirements.

Furthermore, for governmental accountants under the CBDC regime, auditors will be required to provide assurance regarding central bank controls. The tools used by central banks will certainly differ from fiat to digital money. Depending on the form of CBDC implementation (CBDC Popular or Wholesale), central banks may issue currencies through ICOs (initial coin offerings), requiring auditor oversight, or conduct liquidity injections through standard means of monetary policy, including debt purchases. Auditors must verify these transactions.

b. Capital Generation through Initial Coin Offerings (ICOs)

Audit clients may eventually raise capital by issuing new digital coins or initial coin offerings (ICOs), which may have unique features such as interest payments to holders or dividends. New coins that generate capital are potentially subject to regulation by the Securities Exchange Commission or a similar regulatory body; or as unregistered securities (Cohn, 2021). Clients seeking to raise capital through ICOs will require valuation, assurance, and tax advising services.

c. Dark Web Transactions

As auditors refine their practices to accommodate clients with substantial cryptocurrency holdings, a market for hacking services (used to steal digital assets) may arise on the dark web by noncompliant entities. For instance, nefarious agents could develop markets to launder money, using "dark pool" side transactions with related parties through underground networks such as noncompliant, darknet crypto asset service providers and exchanges. Van Wegberg, Oeremans, and Van Deventer (2018) review five cryptocurrency mixing and exchange services available on the dark web and show that illicit activities are still possible.

d. Privacy Coins

Several digital currencies, such as Monero, Dash, and Zcash, were specifically created to protect the anonymity of participants in transactions. These coins actively implement an obfuscated public ledger where any trader can transact without revealing the source, amount, and destination. Shielding the participants in a transaction requires active intervention by the beneficial owner, and while few organizations presently have the required knowledge to safeguard anonymity, additional coins with enhanced privacy features will evolve. It remains unclear whether the auditing profession is equipped to authenticate such transactions or provide assurances that the client is conducting legitimate trades.

[18] See Dupuis et al. (2021) for a full description of CBDCs across various jurisdictions.

e. Crypto Secrecy Jurisdictions and Jurisdiction Shopping

As stated by the Tax Justice Network (Economics, 2020), "A global industry has developed involving the world's biggest banks, law practices, accounting firms and specialist providers who design and market secretive offshore structures for their tax- and law-dodging clients." At present, auditors must vet their clients' bank accounts, operations, and related parties in offshore financial secrecy jurisdictions and weak corporate governance regimes such as the Cayman Islands, Bermuda, Luxembourg, Maldives, and the Marshall Islands. These jurisdictions currently provide managers with an opportunity to disguise the ultimate beneficial owner (UBO) of related party transactions to circumvent governance, tax, and disclosure requirements. Several countries presently indicate that they intend to transform themselves into crypto secrecy jurisdictions comparable to today's tax havens but offer more sophisticated secrecy services.

To the extent that auditors are unable to document their clients' compliance with tax or disclosure laws due to the existence of operations or accounts in these jurisdictions, they may face liability. For instance, the Marshall Islands is both a financial secrecy jurisdiction and a tax haven. Marshall Islands permits corporate incorporation at a very low cost within a matter of two weeks, does not cooperate with the Organization for Economic Co-operation and Development (OECD) on tax information exchange, accepts minimal governance guaranteeing the anonymity of directors, requires no financial disclosures of any kind, offers investment passports that can be obtained with minimal disclosure and without ever appearing physically in the country, and also provides its own central bank-backed digital coin.[19] To the extent that the United States JOBS Act exempts newly listed "Emerging Growth Companies" from many of the Sarbanes-Oxley governance and disclosure provisions, and as auditors may have difficulty receiving information from the central bank of the Marshall Islands regarding client crypto asset holdings or trace funds to related party transactions, the growth in and competition between crypto secrecy jurisdictions in the future may heighten the risk to auditors.

9. Conclusion

Businesses are increasingly holding crypto assets and using them in operations. This study highlights the broad effects of excess risk for auditors when clients have digital assets. Because of the anonymity associated with digital assets, forensic accountants need a strong understanding of crypto assets, the audit trail, the vulnerabilities in the transaction process, and how the information about crypto assets and cryptocurrency transactions exists within the firm. This article began with an overview of the digital asset industry from the perspective of business use and investigated the aspects of digital currency that suggest increased professional skepticism. The treatment of digital assets is, in general, reported as an intangible asset for non-financial industries; however, reporting guidelines are not formalized, and the guidelines are modified for the financial industry. Several stakeholders have called on regulatory agencies to address the matter formally and to modify the guidelines to better align the financial statements with the economic use of cryptocurrencies. Accountants should consult the FASB Meeting Handout (FASB, 2022), the most recent AICPA Practice Aid (AICPA, 2022), and the finalized FASB crypto standards that will be effective for 2024. The IASB staff recommends that cryptocurrency follow IAS 38, Intangible Assets, and for cryptocurrencies held for sale, IAS 2, Inventories.

There is a heightened risk in firms using cryptocurrency for transactions because of the limited audit trail, and the risk is augmented when cryptocurrency is used to pay for transactions such as compensation, acquisitions, dividends, or payment for contracts, especially when related parties are involved. Holding digital assets and using cryptocurrency for transactions creates risk and increases the possibility of litigation; unsuspecting business associates could be named in the legal filings due to blockchain or crypto assets.

The risk associated with digital assets requires consideration in every phase of the audit, from client acceptance and continuance to planning and evaluating evidence. This study demonstrates that accounting for digital assets requires expertise in every management assertion related to recording and auditing the assets in the firm's financial statements, and digital assets affect many areas of the internal control framework. The broad range of examples presented in this study of firm transactions with digital assets provides robust support for Deloitte's call for the FASB to reconsider the identification of digital assets as intangible because the applications represent core business transactions. The AICPA and PCAOB should consider providing audit expectations on the evidence for valuation of thinly traded digital assets. This article identifies several specific, ongoing innovations that the auditing profession should be vigilant about going forward, such as central

[19] An increasing number of U.S.-listed companies incorporate in the Marshall Islands (for more detail, see https://www.offshore-protection.com/marshall-islands-company-formation).

bank digital coins, dark web transactions, and privacy coins, that forensic accountants should continue to monitor.

Additional Resources

Cryptocurrency Technology Tools:

Anchain.ai Blockchain security and compliance tool, tracks potentially dangerous transactions: https://www.anchain.ai/

Anchain.ai software: (CISO) https://www.youtube.com/watch?v=nfbBm0MHTY&list=TLGGXLf54fhP37QwODA3MjAyMQ

Blockchain Intelligence Group: Blockchain forensics: https://blockchaingroup.io/ Software used by Blockchain Forensics (QLUE): https://www.youtube.com/watch?v=FRl0_D8x5P0

Blockchain.com: free transaction tracker for Bitcoin transactions. https://www.blockchain.com/explorer

IntoTheBlock: free transaction tracker for Bitcoin transactions. https://app.intotheblock.com/coin/btc?pid=blockchain&utm_source=blockchain_widget

Etherscan: Free transaction tracker for Ethereum: https://etherscan.io

Video Content

A simple explanation of Bitcoin. Explaining Bitcoin to a Fifth Grader (TEDxYouth@HPA) https://www.youtube.com/watch?v=-68ExnwrwgA

Considerations for internal auditors. Understanding Blockchain for Internal Auditors (PWC US) https://www.youtube.com/watch?v=fM3v5DI-zts

The current IFRS environment. Accounting for Cryptocurrencies Under IFRS https://www.youtube.com/watch?v=6p0e8deqqm8

Accounting information system considerations for auditors. Lessons From Two Years of Crypto Audits (Blackhat) https://www.youtube.com/watch?v=zNOfXu0n2pg

Review of Halo Cryptosolution Tool. Supporting the Audit of Cryptocurrency. (PWC) https://www.youtube.com/watch?v=MkJVD91G_Hw

Industry Resources

CPA Canada. Audit Considerations Related to Cryptocurrency Assets and Transactions. July 6, 2021. Available at: https://www.iasplus.com/en-ca/publications/cpa-canada/audit-considerations-related-to-cryptocurrency-assets-and-transactions

Audits Involving Crypto Assets. PCAOB. Available at: https://pcaobus.org/Documents/Audits-Involving-Cryptoassets-Spotlight.pdf

Accounting for and Auditing of Digital Assets. AICPA. Available at: https://www.aicpa.org/interestareas/informationtechnology/resources/blockchain/digital-assets.html

Blockchain and Internal Controls: The COSO Perspective. AICPA. Available at: https://www.aicpa.org/content/dam/aicpa/interestareas/informationtechnology/downloadabledocuments/blockchain-and-internal-control-the-coso-perspective.pdf

Accounting for Crypto Assets (Liabilities): Holder and Issuer Perspective. European Financial Reporting Advisory Group. Available at: https://efrag.org/Assets/Download?assetUrl=%2Fsites%2Fwebpublishing%2FMeeting%20Documents%2F19070814003075 84%2F06-03%20-%20EFRAG%20Board%20presentation%20Crypto-assets%20%28liabilities%29%20DP-160620.pdf&AspxAutoDetectCookieSupport=1

References

ACCA, 2021, Accounting for cryptocurrencies. Available at: https://www.accaglobal.com/gb/en/student/exam-support-resources/professional-exams-study-resources/strategic-business-reporting/technical-articles/cryptocurrencies.html.

Ackerman, G., 2021. Turkey's Cryptocurrency Boom Turns to Bust. Bloomberg. Available at: https://www.bloomberg.com/news/newsletters/2021-04-25/turkey-s-cryptocurrency-boom-turns-to-bust.

American Institute of CPAs (AICPA), 2020. Implications of the Use of Blockchain in SOC for Service Organization Examinations. Available at: https://www.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/implications-of-blockchain-web.pdf.

AICPA, 2022, "Practice Aid Accounting for and auditing of digital assets." June 30, 2022.

AICPA, 2023, "Accounting for and Auditing of Digital Assets." July 31, 2023. Accessible at: https://www.aicpa-cima.com/resources/download/accounting-for-and-auditing-of-digital-assets-practice-aid-pdf.

Bech, M. and Garratt, R., 2017, Central bank cryptocurrencies, BIS Quarterly Review, p. 55–70.

Benzmiller, T., 2022, China's Progress Towards a Central Bank Digital Currency. Available at: https://www.csis.org/blogs/new-perspectives-asia/chinas-progress-towards-central-bank-digital-currency.

Bit Digital, 2021 Annual Report. Available at: https://www.sec.gov/Archives/edgar/data/1710350/000121390021018773/f20f2020_bitdigitalinc.htm.

Bit Mining, 2021 Annual Report. Available at: https://www.sec.gov/ix?doc=/Archives/edgar/data/1517496/000110465921050188/wbai-20201231x20f.htm.

British Broadcasting Corporation, February 11, 2021, U.S. Treasury: Yellen warns of 'explosion' of cybercrime risk. Available at: https://www.bbc.com/news/business-56021100.

Broby, D. and Paul, G., 2017, The financial auditing of distributed ledgers, blockchain and cryptocurrencies. Journal of Financial Transformation, 46:76-88. ISSN 1755-361X.

Brown, Albert, 2023, Miami Mayor Says He Still Buys Bitcoin Every Two Weeks, The Crypto Basic, January 20, 2023. Available at: https://thecryptobasic.com/2023/01/20/miami-mayor-says-he-still-buys-bitcoin-every-two-weeks/.

Canadian Public Accountability Board, 2019, Auditing in the Crypto-Asset Sector. Available: https://www.cpab-ccrc.ca/docs/default-source/inspections-reports/2019-crypto-inspections-insights-en.pdf?sfvrsn=9aa5c0d2_20.

Cohn, M., 2021, Companies investing in crypto may be in for a rude accounting surprise. Accounting Today. Available at: https://www.accountingtoday.com/news/companies-investing-in-crypto-may-be-in-for-a-rude-accounting-surprise.

Cohn, M., 2023, FASB approves crypto asset standard. Accounting Today. Available at: https://www.accountingtoday.com/news/fasb-approves-crypto-asset-standard.

Conlon, T., Corbet, S., and Hu, Y., 2022, The collapse of the FTX Exchange: The end of cryptocurrency's age of innocence. Working paper. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4283333.

Corinne R., Fanelli J., and Huang, V. G., FTX Founder is Charged with Fraud, WALL ST. J., December 14, 2022. Available at https://wsjshop.com/products/the-wall-street-journal-wed-december-14-2022.

Craig-Bourdin, M., 2018, Auditing crypto-assets: be bold but recognize the risks, say experts. CPA Canada. https://www.cpacanada.ca/en/news/accounting/the-profession/2019-05-24-crypto-auditing?utm_source=CPACanadaNewsletter&utm_medium=email&utm_campaign=MemberNews_20190610.

Croner-I, 2019, How can cryptocurrency be audited? Available at: https://library.croneri.co.uk/cch_uk/adi/655-6.

DeAngelo, L, 1981, Auditor size and audit quality. Journal of Accounting and Economics, 3(3):183–199.

Deloitte, 2018, Cryptocurrency, The challenge for accountants and auditors. Available at: https://ebra.be/wp-

content/uploads/2018/08/deloitte-presentation-for-ecrf-june-2018.pdf.

Deloitte, 2021, Perspectives: Corporates Investing in Crypto. Available at: https://www2.deloitte.com/us/en/pages/audit/articles/corporates-investing-in-crypto.html.

Deloitte, March 27, 2023, FASB Proposes Guidance on Crypto Assets, Heads Up, Volume 30, Issue 3.

Deloitte, April 25, 2023, AICPA Updates Practice Aid on Digital Assets, and Other Crypto Accounting Hot Topics, Heads Up, Volume 30, Issue 6.

Dupuis, D. and Gleason, K., 2020, Money laundering with cryptocurrency: Open doors and the regulatory dialectic, Journal of Financial Crime, 28(1): 60-74. https://doi.org/10.1108/JFC-06-2020-0113.

Dupuis, D., Gleason, K., and Wang, Z., 2021, Money laundering in a CBDC World: A Game of Cats and Mice., Journal of Financial Crime, forthcoming. Available at: https://privpapers.ssrn.com/sol3/papers.cfm?abstract_id=3793713.

Economics of Oppression and Exploitation The economics of harm and the harm of economics, 2020, Harmfuleconomics.org https://harmfuleconomics.org/financial-secrecy-index-2020/.

FASB, 2022, "Board Meeting Handout Accounting for Exchange-Traded Digital Assets and Commodities."

Feuer, Will, 2021. Miami Mayor Francis Suarez says he'll take next paycheck in bitcoin, New York Post, November 3, 2021. Available at: https://nypost.com/2021/11/03/miami-mayor-francis-suarez-to-take-next-paycheck-in-bitcoin/.

First Bitcoin Capital Corp, 2021 Annual Report. Available at: https://www.sec.gov/Archives/edgar/data/1795749/000121390020000436/f20fr12g2019_firstbitcoin.htm.

Gerard, D., 2021, El Salvador is printing money with Bitcoin. Foreign Policy. Available at: https://foreignpolicy.com/2021/06/15/el-salvador-bitcoin-official-currency-printing-money/.

Hamacher, A., 2021, Tesla and Microstrategy's Bitcoin Bet Brings Accounting Headache, Decrypt, Available at: https://decrypt.co/73749/tesla-microstrategys-bitcoin-bet-brings-accounting-headache.

Heaslip, K., 2023, New Jersey CPA Magazine. Available at: https://www.njcpa.org/stayinformed/news/njcpamag/issues/summer-2023.

Ho, S., 2023, AICPA Digital Asset Reporting Guide Punts on Lending Transactions, Thomson Reuters. Accessible at: https://tax.thomsonreuters.com/news/aicpa-digital-asset-reporting-guide-punts-on-lending-transactions/.

Hsieh, S. F., and Brennan, G., 2022, Issues, risks, and challenges for auditing crypto asset transactions. International Journal of Accounting Information Systems, 46.

Hochstein, M., 2018, Tether confirms relationship with auditor has dissolved. CoinDesk. Available at: https://www.coindesk.com/tether-confirms-relationship-auditor-dissolved.

Jalan, A., Matkovskyy, R., and Yarovaya, L., 2021, "Shiny" crypto assets: A systemic look at gold-backed cryptocurrencies during the COVID-19 pandemic. International Review of Financial Analysis, 78.

KPMG 2020 "Institutionalization of Cryptoassets." Available at https://kpmg.com/us/en/home/insights/2018/11/institutionalization-cryptoassets.html.

Krause, E., 2018, A Fifth of All Bitcoin Is Missing. These Crypto Hunters Can Help, The Wall Street Journal, Available at: https://www.wsj.com/articles/a-fifth-of-all-bitcoin-is-missing-these-crypto-hunters-can-help-1530798731.

Liu, S., 2020, New Guidance on Auditing Digital Assets. Internal Audit 360. Available at: https://internalaudit360.com/new-guidance-on-auditing-digital-assets/PCAOB.

Liu, M., Wu, K., and Xu, J. J., 2019, How will blockchain technology impact auditing and accounting: Permissionless versus permissioned blockchain. Current Issues in Auditing, 13(2), A19-A29.

Marathon Digital Holdings, 2021 Annual Report. Available at: https://www.sec.gov/Archives/edgar/data/1507605/000149315221006139/form10-k.htm.

Peterson, T., 2021, To the moon: a history of Bitcoin price manipulation. Journal of Forensic and Investigative Accounting, 13(2), 254–272.

PCAOB, 2020, Audits Involving Cryptoassets Information for Auditors and Audit Committees SPOTLIGHT. Available at https://pcaobus.org.

Rezaee, Z., and Reinstein, A, 1998, The impact of emerging information technology on auditing. Managerial Auditing Journal, 13(8), 465–471.

Slisco, A., 2021, Miami Passes Resolution to Allow Paying City Workers in Bitcoin in Attempt to Woo Big Tech, Newsweek, February 11, 2021. Available at: https://www.newsweek.com/miami-passes-resolution-allow-paying-city-workers-bitcoin-attempt-woo-big-tech-1568784.

Smith, S., 2018, Bring cryptocurrencies into the accounting classroom, Journal of Accountancy. Available at: https://www.journalofaccountancy.com/newsletters/extra-credit/cryptocurrencies-in-the-accounting-classroom.html.

Smith, S. S., 2020, Blockchains impact on risk assessment procedures. Journal of Forensic and Investigative Accounting, 12(1), 55–65.

Sor, J., 2022, "FTX US's Auditor Stands by Its Accounting Work for the Collapsed Exchange." Markets Insider, December 23, 2022. Available at: https://markets.businessinsider.com/news/currencies/ftx-bankruptcy-sam-bankman-fried-fraud-auditor-armanino-fraud-2022-12?op=1.

The9 Limited, 2021 Annual Report. Available at: https://www.sec.gov/Archives/edgar/data/1296774/000110465921043144/tm211771d1_20f.htm.

Trautman, L. J., 2022, The FTX Crypto Debacle: Largest Fraud Since Madoff? November 30, 2022. Available at SSRN: https://ssrn.com/abstract=4290093 or http://dx.doi.org/10.2139/ssrn.4290093.

Van Wegberg, R., Oerlemans, J. and van Deventer, O., 2018, Bitcoin money laundering: mixed results? An explorative study on money laundering of cybercrime proceeds using bitcoin, Journal of Financial Crime, Vol. 25 No. 2, pp. 419–432.

Vincent, N. and Wilkins, A., 2020, Challenges when auditing cryptocurrencies. Current Issues in Auditing 14 (1): A46-A58. doi: https://doi.org/10.2308/ciia-52675.

Voshmgir, Shermin, Token Economy How the Web3 reinvents the Internet. Shermin Voshmgir, BlockchainHub Berlin; 2nd ed. edition (June 5, 2020).

Xu, C., Liu, C., Nie, D., and Gai, L., 2021, How can a blockchain-based anti-money laundering system improve customer due diligence process. Journal of Forensic and Investigative Accounting, 13(2), 273–287.

Young, M., 2021. President Biden freezes FinCEN's proposed crypto-wallet regulations. CoinTelegraph. Available at: https://cointelegraph.com/news/president-biden-freezes-fincen-s-proposed-crypto-wallet-regulations.