Client-level Exposure to Cryptocurrency and Auditor Responses*

Beatriz García-Osma, Hoang Nhan Ha,
W. Robert Knechel and Thi Thuy Dung Nguyen†

This draft: September 2023

Abstract

Auditors increasingly face issues that transcend the formal boundaries of the firm. In an era of technological revolution and where authoritative accounting and auditing guidance are yet to develop, auditors may lack the necessary knowledge and expertise to navigate novel and complex issues. In this study, we examine auditor responses in such settings by focusing on client exposure to cryptocurrency. We construct and validate a novel text-based measure of client-level exposure to cryptocurrency and the nature of such exposure. Using this proxy, we document an association between client exposure to cryptocurrency and audit pricing and reporting decisions. We also provide evidence of heightened audit-office demand for crypto-related skills.

Keywords: Cryptocurrency, Audit Fees, Auditor Conservatism, Audit Reporting Lag, Critical Audit Matters, Job Postings, 10-K Filing

*We are grateful for helpful comments from Baptiste Colas, Juan Manuel García-Lara, Maria Gutiérrez Urtiaga, Encarna Guillamón-Saorín, Bing Guo, Paulo Maduro, Lauren Cunningham and Phillip Lamoreaux (2023 Auditing Section Midyear Meeting Doctoral Consortium), Gabriel Pereira Pundrich, Quoc Tuan Ho and workshop participants at the University of Florida, the 2023 PRICIT Doctoral Workshop, the EAA Congress 2023, the Machine Learning for Textual and Unstructured Data Seminar (IESE Business School), and the XVII International Accounting Symposium. We acknowledge financial support from the Ministry of Science and Education (PID2019-111358GB-I00 and TED2021-129861B-I00) and Comunidad de Madrid (Programa Excelencia para el Profesorado Universitario, convenio con Universidad Carlos III de Madrid, V Plan Regional de Investigación Científica e Innovación Tecnológica, EPUC3M12).

†Beatriz García Osma, Hoang Nhan Ha, and Thi Thuy Dung Nguyen are from the Universidad Carlos III de Madrid. W. Robert Knechel is from the University of Florida. **Corresponding authors**: Hoang Nhan Ha (E-mail: nha@emp.uc3m.es) and Thi Thuy Dung Nguyen (E-mail: dnguyen@emp.uc3m.es). Calle Madrid 126, 28903 Getafe (SPAIN)

1 Introduction

Auditors provide assurance that financial statements are presented in accordance with generally accepted accounting principles (GAAP)(PCAOB, 2015), reducing shareholders' information risk (Knechel, 2016, 2021). However, the scope of the audit has steadily broadened over time, encompassing issues that require knowledge and evidence gathering beyond the formal boundaries of the organization.[1] The growing reliance on external service centers (e.g., cloud computing), electronic banking systems, or blockchain applications blurs the boundaries between the organization and its external environment (Frey, Adams, Pfeffer and Belmi, 2023), increasing exposure to counterparty risk and becoming a growing concern for auditors. In a fast-changing world, these challenges become steeper as auditors must conduct the audit without the guidance of established accounting and auditing standards.[2] In this paper, we examine how auditors respond to this growth in counterparty risk, absent authoritative guidance, by focusing on clients' exposure to cryptocurrency risk.[3]

Cryptocurrency imposes new challenges and risks for auditors. These challenges involve all phases of the audit, from risk assessment to evaluating and testing internal controls over data integrity to planning and gathering substantive evidence to support management assertions (Vincent and Wilkins, 2020). This makes cryptocurrency an ideal setting to examine our question. Audit processes that are adequate for the audit of assets and liabilities clearly delimited by organizational boundaries may not apply to assets that breach these boundaries for a number of reasons. First, the pseudo-anonymous nature of transactions involving crypto

[1] Organizational boundaries are generally any demarcation between the organization and its environment (Santos and Eisenhardt, 2005).

[2] Knechel (2013) argues that accounting standards establish a uniform way of measuring and reporting a result among various companies while auditing standards provide a process to verify the outcome. However, the assurance level in each engagement with differences in client complexity and idiosyncratic factors might exceed the minimum requirement of standards, suggesting that professional judgment, audit expertise, and experience are crucial to meet market demand.

[3] The term *"cryptocurrency"* excludes smart contracts, non-fungible tokens, or stablecoins, i.e., while our measures may capture some broader blockchain-enabled activity, our focus is on cryptocurrency. We provide more details of measure development and validation in Section 3, specific keywords in Table A.1.

assets obscures the true identities of client's counterparties, thereby exposing clients to the risk of non-compliance with know-your-customer (KYC) and anti-money laundering (AML) provisions (PCAOB, 2020). Consequently, auditors face difficulties in identifying related parties and understanding the nature of such transactions. This, in turn, heightens the risk that financial statements may be vulnerable to material misstatements, omitted disclosures, or transactions with unknown related parties. Moreover, the nature of record-keeping, whether conducted inside or outside blockchain, such as in trading platforms, presents challenges in obtaining audit evidence using traditional procedures. Additionally, blockchain activities require specialized internal controls that may be difficult to design, implement, and assess, both within the reporting entity and also related to third-party websites and platforms.

Second, the values of crypto assets are difficult to verify and have high volatility. The price of cryptocurrency can vary across international markets and exchanges. Exchanges are not centralized, and each exchange has its own supply and demand dynamics and trading volume. This opens them to manipulation, as evidenced by recent scandals such as FTX. Our own manual examination of crypto-related critical audit matters (CAMs) demonstrates that there are subjective and complex audit areas that are not solely associated with the accounting and disclosure of digital currency held. Rather, these areas are also connected to the recognition and measurement of crypto mining revenue, the valuation of mining machines, and the appropriate accounting treatment of equity instruments issued. The lack of market-based pricing mechanisms exacerbates valuation issues. Volatility increases the risk of errors in financial reporting, particularly when values are not updated regularly to reflect changes.

Compounding these challenges is the absence of authoritative guidance and clear industry practices for the accounting and auditing of crypto assets. Existing accounting standards do not necessarily reflect the unique characteristics of these assets, leading to greater discretion and errors in reporting and disclosures. Inconsistent measurement and reporting of cryptocurrency and crypto assets across clients due to a lack of accounting guidance, jointly with lack of auditing guidance, increase the inherent and control risks associated with an audit.

Traditional audit procedures may not adequately reduce detection risk to an appropriate level. Auditors may lack the necessary technology to audit clients' crypto-related businesses and require specialized expertise in areas such as cryptography, distributed ledger technology, valuation, and related legal and regulatory frameworks, including requirements related to KYC and AML provisions. Indeed, anecdotal evidence suggests that auditors need assistance from professionals (i.e., IT professionals and internal valuation specialists) with skills and knowledge in potentially problematic uses of blockchain. These experts aid, for example, in assessing specific internal controls pertaining to the generation and storage of private cryptographic keys, concerning the digital assets process carried out at custodial sites.

Therefore, many of the challenges that auditors face are beyond the traditional boundaries of the firm and transcend the mere holding of crypto assets. Importantly, crypto-related business is increasingly material, and it is foreseeable that other assets and businesses may soon emerge that share similar fundamentals. Therefore, regardless of the potential rise or fall of specific types of crypto assets, the ambiguities, novelties, and complexities encountered in auditing these new classes of assets are expanding and likely to remain.

To provide evidence on auditor responses, we construct a measure that captures multiple dimensions of cryptocurrency exposure at the client level. Our method follows recent studies that have developed text-based measures at the firm-year level by combining human reading and machine learning with intensive validations.[4] We define client *exposure* as the proportion of discussion in sections "Item 1 Business" and "Item 1A Risk Factors" of annual reports (10-K filings) from the EDGAR database from 2008 to June 2023 that are devoted to the topic of cryptocurrency.[5] We choose these parts of the 10-K to quantify client exposure to cryptocurrency because such regulated disclosure captures the most comprehensive information about the main business and risks faced by a company (SEC,

[4]See, e.g., the recent work of Hassan, Hollander, Van Lent and Tahoun (2019); Sautner, Van Lent, Vilkov and Zhang (2023); Hassan, Hollander, van Lent, Schwedeler and Tahoun (2023)

[5]We collect all 10-Ks filed from 2008, the year that Bitcoin was introduced by Nakamoto and Bitcoin (2008). Since 2013 marks the initial detection of cryptocurrency exposure within our dataset, we have retained observations spanning from fiscal years 2013 to 2022 for our regression analysis.

2011), and are directly related to the concerns and responsibilities of the auditors. We also decompose the nature of cryptocurrency exposure by quantifying four cryptocurrency business activities (production, transaction, mining, and investments) as well as five cryptocurrency risks (regulation, business, operations, cybersecurity attacks, market risks, and peer risks). This allows us to examine a broader set of clients rather than focusing exclusively on clients that have a direct investment in cryptocurrencies.[6] Regarding investment, we identify not only direct cryptocurrency holdings but also indirect investments in cryptocurrency funds.[7] Client exposure to cryptocurrency could also be driven by their production and operations, such as trading platforms that offer a marketplace for digital assets, loans and equity (such as reflected in decentralized finance contracts) (Bourveau, Brendel and Schoenfeld, 2023; Knechel, Maex and Park, 2023).[8]

Using our proxies, we first examine auditor pricing and reporting decisions. We find that client exposure to cryptocurrency is positively associated with audit fees and greater auditor reporting conservatism, as measured by the likelihood of issuing a going concern audit opinion and longer audit reporting lag. This evidence is as expected and further validates our measures. Specifically, a one-standard-deviation increase in the client-level exposure to cryptocurrency translates into a 1.0% to 1.1% fee increase, 0.4% to 0.6% increase in the likelihood of issuing a going concern opinion, and about a 0.2 increase in the number of days to finalize the audit engagements. Besides, auditors also respond with a higher proportion of cryptocurrency-related critical audit matters. We also find positive and statistically significant results of cryptocurrency topic exposure with auditor responses, confirming that an auditor

[6]For example, we identify firms with mining as their main business, such as Marathon Patent Group Inc., whose business focuses completely on Bitcoin mining. The firm has $1,495,402 in Bitcoin mining revenue in the year 2018, which contributes to 95% of its revenue but holds $0 Bitcoin on its balance sheet.

[7]For example, U.S. Global Investors does not hold any cryptocurrency but has an (equity method) investment in Galileo Technology and Blockchain Fund of $283,000 on June 30 2018, resulting in challenges in preparing the consolidated financial statement because, as noted in its 10-K the "Company's proportional share of the fund's net income or loss, which primarily consists of realized and unrealized gains and losses on investments offset by fund expenses, is recognized in the Company's earnings."

[8]For example, Bakkt remarks in their 10-K for the year 2021, that they provide a digital asset marketplace in which "Cryptoassets held in a custodial capacity on behalf of our customers are not included in our balance sheet, as we do not own those crypto assets and they do not exhibit the characteristics of assets as it relates to our consolidated financial statements."

reacts to multidimensional cryptocurrency business and risk exposure. It provides more granular evidence consistent with the aggregated exposure measures in the main analysis and highlights that auditors tailor their responses based on the nature of clients' cryptocurrency involvement. We further explore the role of underlying volatility in cryptocurrency in explaining our findings. We find that audit fees are higher in periods of greater volatility in the underlying cryptocurrency market. Based on the job posting data, we also provide preliminary evidence that an audit office seeks more new hires with crypto-related skills when having more clients exposed to cryptocurrency. The findings provide initial indications that advancements in technology have significantly influenced the audit profession.

We examine the role of a novel channel in explaining our results: the lack of authoritative guidance in accounting and auditing. In the absence of regulation, our manual data collection reveals that large audit firms issue internal guidance years ahead of regulatory action and standardization. This guidance is published and publicly available, potentially to increase its visibility and to legitimize auditors' proposed solutions. Our evidence suggests that the extent of internal guidance is associated with increased audit costs and audit reputation and expertise, likely driven by audit investments and additional audit efforts that are passed on to clients, resulting in greater audit fees. Our evidence also indicates that guidance eventually lessens subjectivity, difficulty, and complexity in the audit, as we find a lower ratio of critical audit matters related to cryptocurrency.

We make several contributions to the literature. First, while cryptocurrency has been investigated in the finance literature, this prior work largely examines cryptocurrency pricing.[9] Most closely related to our work are Anderson, Fang, Moon and Shipman (2022) and Cheng, Davis, Huang and Ma (2022), which are the first attempts to understand accounting and

[9]For example, work by Pagnotta and Buraschi (2018) and Biais, Bisiere, Bouvard, Casamatta and Menkveld (2020), agrees that network factors influence price dynamics. Cong, Li and Wang (2019), and Sockin and Xiong (2020) argue that prices of cryptocurrency depend on the miners' problem (linked to the marginal cost of production), while Liu and Tsyvinski (2021) fails to confirm this link between prices and production factors. In addition, one group of papers confirms the relationship between cryptocurrency prices and fiat money (Athey, Parashkevov, Sarukkai and Xia, 2016; Schilling and Uhlig, 2019; Jermann, 2018).

auditing for cryptocurrency. We diverge substantially from those papers, both in research question and method. While they manually identify material cryptocurrency holdings on firms' balance sheets by searching relevant keywords from footnotes, our measure captures more nuances of client exposure to cryptocurrency, resulting in a sample that captures not only firms holding cryptocurrency but also other crypto-related business activities.[10]

Our study extends the evidence on audit pricing for crypto-holding firms in Cheng et al. (2022) to cryptocurrency exposure more broadly and examines the role of lack of guidance separately from other risk factors studied in greater detail in the literature. Our findings are timely because they contribute to a growing literature stream that examines digital assets, accounting choices, and disclosure of cryptocurrency by assessing how auditors respond against a backdrop of a lack of official guidance.

Second, we construct and validate a novel measure of cryptocurrency exposure. We contribute to the growing strand of literature that extracts economic information from text-based data such as earnings calls and financial reports as 10-K and 10-Q filings. We add to this literature by focusing on crypto-related texts and investigating whether they convey information about client-level exposure to cryptocurrency. Our methodology and measures can be easily deployed to examine other narratives to suit alternative research questions.

Third, our results also speak to the literature on how technological evolution reshapes skills and knowledge requirements in the audit profession (Fedyk, Hodson, Khimich and Fedyk, 2022; Commerford, Dennis, Joe and Ulla, 2022; Law and Shen, 2020). While these studies focus on artificial intelligence and its adoption in audit engagements overall, our study examines the demand for specialized skills needed to audit clients exposed to cryptocurrency. Our empirical evidence provides preliminary insights that auditors must tailor their expertise

[10]For example, we have 132 client-year observations for the fiscal year of 2020, which is significantly higher than only 24 firms in (Anderson et al., 2022) and 10 firms in Cheng et al. (2022)'s samples. Our full sample covers 806 client-year observations from 2013 to 2021 (and 1,055 observations up to the fiscal year 2022) (see Table IA.6), compared to 135 in Anderson et al. (2022) and 33 in Cheng et al. (2022). Anderson et al. (2022) provides a sample of firm-quarter cryptocurrency holding observations from 2013 to 2020, so we select only quarters 4 from their sample to count for comparability with our firm-year level data.

and human capital demand to address emerging issues outside an auditor's prior domain of expertise. Although our setting is specific to cryptocurrency audit challenges, the findings could potentially generalize to other settings where auditors keep pace with novel technological developments by rapidly developing new specialized knowledge relevant to clients' idiosyncratic businesses. Our evidence also speaks to the emerging literature on auditor's quality signalling and reputation building, which finds that auditors publish in practitioners' journals (Downar, Ernstberger, Koch and Prott, 2021). We document and provide novel evidence on the publication of technical reports in the absence of regulation and authoritative guidance.

Fourth, current work finds that blockchain applications shape internal corporate governance (e.g., Yermack (2017); Chod, Trichakis, Tsoukalas, Aspegren and Weber (2020)). Our study expands this view, looking at the external auditor. Our findings are novel in that we focus on whether cryptocurrency exposure requires more skeptical audit behavior (rather than the positive effects of technological advances, which is the focus of much of the prior literature). The development of blockchain applications is incipient (World Bank Group, 2020), but cryptocurrency is one of the largest unregulated markets with a high proportion of illegal activities (Foley, Karlsen and Putniņš, 2019) and high volatility (Liu and Tsyvinski, 2021). Our research confirms the critical role of auditors in facilitating public demand for investor protection even before regulators address the negative side of cryptocurrency. Although cryptocurrency is the paper's primary focus, our findings could be generalized in auditor responses to different crypto assets and emerging technological factors. Therefore, our work adds to the current debate and informs standard setters, practitioners, and academia about changes in auditors' responses to the impact of emerging technologies.

2 Background & Hypotheses development

Cryptocurrency is a digital asset that uses cryptographic algorithms to secure and verify transactions. The underlying technology that supports it is blockchain, an open and distributed

ledger where a history of transfers is periodically recorded and held. No centralized authority backs cryptocurrency. Instead, it is maintained by a decentralized system through a computer network worldwide. Cryptocurrency is created through "mining" processes, where miners use their computing power to solve complicated mathematical problems. Once a cryptocurrency is produced, it is stored in a digital wallet secured using cryptography. The wallet contains a private key, which is a unique identifier that enables the owner to access and transfer their cryptocurrency securely. Well-known cryptocurrencies include Bitcoin, Ethereum, and Ripple (Liu, Wu and Xu, 2019), but many cryptocurrencies are in circulation. Since Bitcoin was first introduced by Nakamoto and Bitcoin (2008), the global cryptocurrency market capitalization rocketed to nearly one trillion USD in its first decade (by 2018) and then tripled just three years after, reaching nearly three trillion USD in November 2021 contributed by over 800 cryptocurrencies.[11]

2.1 Accounting for cryptocurrencies

Cryptocurrencies are new and complex, and there is no current conceptually-grounded approach for accounting for these assets (Barth, 2022; Hombach and Sellhorn, 2022; Schipper, 2022). This creates uncertainty with respect to adequate reporting, plausibly leading to a diversity of treatments where managerial incentives may play a role in generating opportunistic rather than informative recognition and disclosure. Until 2022, the primary emphasis of accounting and auditing discussion in professional guidance centered on how to account for and disclose the holdings of reporting entities. However, as of 2022, this focus has expanded to include custodial services, whereby reporting entities may not hold cryptocurrencies but instead function as custodians responsible for safeguarding crypto assets (similar to a bank or a broker for more traditional financial assets). The risks associated with safeguarding crypto assets held on behalf of platform users are not new, as reports of significant amounts of stolen

[11] See Figure 1. According to Duggan (2022), the first real-world transaction involving Bitcoin took place on May 22, 2010, when 10,000 BTC were paid for two Papa John's pizzas priced at about 25 USD.

crypto assets from cryptocurrency platforms have been documented since 2018 (Hester, 2022). Further, there has also been a recent increase in transactions involving crypto coins (e.g., crypto lending) and other forms of crypto assets (e.g., stablecoins, non-fungible tokens) in which clients must use significant accounting judgment.[12]

Involvement with crypto assets is multifaceted. Clients may hold crypto on their financial statements for various purposes, such as acquisitions or investments, mining activities, using them as a form of payment for goods or services, engaging in crypto trading on secondary markets, and investing in initial coin offerings (ICOs) and early-stage blockchain projects (Anderson et al., 2022; Luo and Yu, 2022).[13] Against this growth in crypto, the lack of authoritative guidance has created a demand for guidelines on measuring and reporting cryptocurrency (Manning, 2021). Figure 2 provides a timeline of accounting guidance and discussions in response to this demand. Big4 accounting firms and AICPA have issued public non-authoritative guidance and documentation on accounting for cryptocurrency under IFRS and/or GAAP frameworks, resulting in a switch from evaluating crypto holdings at fair value to indefinite-lived intangible assets under ASC 350, *Intangibles—Goodwill and Other* in firms balance sheets. In particular, crypto assets are initially measured at cost and then subsequently evaluated for impairment prior to derecognition.

The increasing prevalence and rapid evolution of crypto assets have attracted significant attention from regulatory bodies in recent years. Notably, in May 2022, the FASB unanimously voted to add digital asset accounting to its technical agenda (Lugo, 2022), highlighting the growing importance of these assets and suggesting that accounting regulation would follow swiftly. In line with this, the FASB has proposed an accounting standard update (ASU) on the accounting for and disclosure of crypto assets. The exposure draft is open for a 75-day public comment period starting in February 2023.

[12]Complex accounting challenges can emerge as a result of the growing popularity of various crypto transactions, such as Simple Agreement for Future Tokens (SAFT), token issuance through an Offshore Foundation or a Decentralized Autonomous Organization (DAO), and the utilization of tokenized assets.

[13]To facilitate payments by using cryptocurrencies, clients may take a hands-off approach to keep crypto off the books by converting in and out of crypto to fiat currency by themselves or via third-party vendors.

Given the absence of specific IFRS or GAAP accounting standards for cryptocurrencies, the accounting profession currently relies on concept statements, existing standards, and non-authoritative guidance to account for cryptocurrencies.[14] As a result, there is a level of subjectivity in selecting and applying the appropriate accounting choices, leading to inconsistencies in classifying assets as long or short-term and classifying the subsequent cash flows from converting cryptocurrencies into fiat currencies. These inconsistencies can distort investors' evaluation of clients' assets, profitability, and cash flows (Luo and Yu, 2022).[15]

Because crypto-related business activities expand beyond the mere holding of cryptocurrency, the traditional bounds of the scope of accounting and auditing are also expanded. For example, audit clients may safeguard crypto assets on behalf of their customers. As the number of entities offering cryptocurrency transaction services and asset safeguarding through direct or third-party means has increased, the Securities and Exchange Commission (SEC) issued Staff Accounting Bulletin No. 121 (SAB 121).[16] SAB 121 requires a reporting entity engaged in custodial activities, whether directly or through a third party, to record a liability for safeguarding and a corresponding asset at the fair value of the crypto assets being safeguarded. To reflect crypto assets on- or off-balance sheet, clients need to consider several factors related to the rights and obligations of both customers and custodians, the ability of customers to access the private key, and contractual terms with the sub-custodian.

[14]For instance, MaughanSullivan LLC also added the following to their audit reports 2021 10-K of Creek Road Miners when they provided a rationale for adding accounting for and disclosure of cryptocurrency assets as a critical audit matter:" *Researching accounting and disclosures by other companies in the industry, consultation with other subject matter experts and researching authoritative literature and standards...*"

[15]The case of MicroStrategy Inc. presented in Figure IA.2 is illustrative. Given high market volatility, Phong Le, President and CFO of MicroStrategy, argued in a letter to the FASB that the accounting treatment under ASC 350 of their Bitcoin as an intangible asset, *"...does not accurately reflect their financial condition and results of operations"* because the impairment charges cannot be reversed and they are holding Bitcoin as an investment (Le, 2021). MicroStrategy argues that the disconnect between reporting and the underlying economics confuses users, does not permit estimating the entity's current and future prospects, and provides a non-GAAP reconciliation that reverses the impairment losses of digital assets (see Figure IA.3).

[16]This bulletin specifically deals with the accounting practices for reporting entities that are involved in safeguarding crypto assets on behalf of their customers. Affected reporting entities would be the entities that operate a trading platform, provide services wallet to customers, provide digital asset payment and trading services, and accept crypto assets as collateral. These activities entail unique risks and uncertainties related to the safeguarding of crypto-assets, including technological, legal, and regulatory risks. Consequently, these risks have a substantial impact on the operations and financial condition of the entity.

2.2 Auditing for cryptocurrencies

Auditing transactions involving crypto assets challenges traditional aspects of audit planning, risk assessment, audit procedures, and resource allocation. As noted, a salient difficulty lies in the notion that crypto transactions expand the boundaries of the client. First, due to the anonymous nature of transactions involving crypto assets. Anonymity obscures the identities of clients' counterparties, thereby exposing clients to the risk of non-compliance with know-your-customer (KYC) and anti-money laundering (AML) provisions (PCAOB, 2020). Moreover, cryptoasset-related transactions may be recorded outside the blockchain (e.g., where information on clients' transactions is in the trading platforms' system). In such cases, obtaining sufficient and appropriate audit evidence becomes a hurdle. In addition, understanding the internal control mechanisms governing financial reporting becomes complex for auditors in these situations because of the third-party storage involved.

Given the lack of prior research on this topic, to understand the actual challenges faced by auditors, we reviewed a number of audit reports to identify critical audit matters (CAMs) related to cryptocurrency.[17] Table 1 provides a summary of financial statement assertions, along with the audit procedures utilized during the course of an audit. Tests related to control over the IT environment and over the digital assets process are emphasized since digital assets are provided through private cryptographic keys stored using third-party custodial services at multiple locations that are geographically dispersed. Our examination of crypto-related CAMs confirms this notion and indicates that the testing of the valuation or allocation assertion can be a particularly challenging task for auditors.

The second substantial challenge for auditors is that cryptocurrency increases the need for automation in audit procedures and adequate resources to complete the audit engagement.

[17] A CAM is defined as any matter arising from the audit of the financial statements that was communicated or required to be communicated to the audit committee and that (i) relates to accounts or disclosures that are material to the financial statements and (ii) involved especially challenging, subjective, or complex auditor judgment.

These new assets build on difficult-to-audit technology, arguably unknown to auditors using traditional audit procedures and, in some cases, potentially beyond their technological capabilities. Anecdotal evidence suggests leading audit firms have invested in specialized audit tools to compare records of digital asset holdings to public blockchain records. PwC designed Halo tools to provide assurance services for entities engaging in cryptocurrency transactions (PWC, 2019). Meanwhile, KPMG's Chain Fusion aims to manage crypto and traditional assets over blockchain networks (KPMG, 2020). EY also provides an innovative tool, the "EY Blockchain Analyzer" for the purpose of helping auditors gather automated audit evidence on the completeness and accuracy, existence, and rights and obligations of digital assets and understanding the business through analytical reviews (Ernst & Young, 2019) and continue to invest heavily in blockchain through its second-generation of Smart Contract & Token Review (Eric Minuskin, 2022). In addition, auditors also engage IT professionals and internal valuation specialists possessing specialized expertise and knowledge in cryptography, distributed ledger technology, and valuation to assess specific internal controls and test assertions related to crypto assets.

2.3 Hypotheses development

2.3.1 Audit fees and auditor report lag

Extant research shows that risk factors are priced in audit fees (Hay, Knechel and Wong, 2006; Simunic, 1980).[18] In response to increased risk, auditors may increase audit quality through additional efforts to reduce detection risk, leading to greater audit fees. In addition, auditors may reassess client risk (its likelihood of survival and performing profitably) as well

[18]A battery of risk factors are documented in previous audit fees literature such as client attributes, auditor attributes, and engagement attributes (see, for a review, DeFond and Zhang (2014); Hay et al. (2006)). For example, high discretionary accruals, lack of conservatism, internal control deficiencies, high short interest, political connections, high free cash flows, poor credit ratings, unethical business practices, client losses, modified opinions, public ownership, and for IPOs, bankruptcy, and litigation disclosures are documented in prior audit fees research.

as auditor business risk (for example, litigation and reputation costs arising from a client failure) and decide to charge a risk premium (DeFond and Zhang, 2014; Simunic, 1980).

Building on this prior work, we hypothesize that auditors price client-level exposure for a number of reasons. First, audit fees are expected to be influenced by the lack of authoritative guidance on accounting and auditing for cryptocurrency. This notion has not been thoroughly explored in prior work. Authoritative guidance serves as a technical justification constraint on auditors' decisions (Ng and Tan, 2003). Without such guidance, identifying material misstatements or conducting thorough reviews of client evidence is more challenging and inappropriate measurements and disclosure of cryptocurrency in financial statements may not be identified. Hence, we expect that lack of guidance poses a threat to audit work. Absent accounting guidance, auditors have to rely on available standards and invest more effort in finding solutions to defend clients' financial reporting decisions to regulators and others in case of an audit failure, seeking greater audit evidence and exerting more effort. In such cases, auditors must rely on concept statements, principle-based accounting, and non-authoritative information such as white papers and other professional accounting and auditing publications. Big4 accounting firms have published professional resources for various categories of cryptographic assets.[19]

Second, auditors may price the uncertainty over the bounds of the client's business risk

[19]PwC, Ernst & Young, Deloitte, and KPMG have all published guidance and alerts on the accounting considerations and reporting requirements for crypto assets. PwC issued its first guidance entitled "*Cryptographic assets and related transactions: Accounting considerations under IFRS*" in September 2018, with an update in December 2019. In August 2021, PwC released a crypto-assets guide for reporting entities under FASB, followed by an update in August 2022. Ernst & Young also provided guidance on this topic. They issued "*IFRS (≠) Accounting for crypto-assets*" in August 2018 and released guidance on "*Applying IFRS Accounting by holders of crypto assets*" in October 2021. In June 2022, they released accounting guidance for digital assets, including crypto assets. This is the first guidance from Ernst & Young to make references to FASB and highlight some issues reflected in SAB 121. Similarly, Deloitte published a financial reporting alert on the "*Classification of Cryptocurrency Holdings*" on July 9, 2018. Regarding the impact of cryptocurrencies on financial statements, KPMG offered its insights. They released their first publication,"*Institutionalization of crypto assets*," in November 2018, focusing on accounting and reporting. KPMG followed up with "*Cryptoassets – Accounting and Tax*" in April 2019. In March 2022, KPMG released "*Crypto asset accounting guidance urgently needed*" for reporting entities under FASB, with a focus on digital assets held by a custodian. They issued other alerts related to evaluating the custody of digital assets and accounting rewards earned by entities for staking their crypto intangible assets at later dates. Refer to Table IA.8 for more detail.

arising from cryptocurrency exposure. The risk associated with a client's business involving cryptocurrencies differs significantly from traditional assets, as it places the knowledge and evidence required by auditors outside the client's boundaries. Prior literature shows that client business risk may affect the audit process and pricing through audit risk and/or auditor business risk (Bell, Landsman and Shackelford, 2001; Stanley, 2011). Clients exposed to cryptocurrency have more discretion in accounting measurements, and plausibly, internal control systems are not fully updated to deal with these newly-created assets, implying higher inherent risk and, as a result, higher audit risk.[20] The underlying riskiness of clients stems not only from a history of volatility in cryptocurrency prices but also from the nature of blockchain design and transactions involving crypto assets. The anonymity of transactions related to crypto assets poses challenges for auditors in verifying counterparties, potentially exposing them to fraud or other illicit activities and thereby increasing the probability of significant misstatements. Furthermore, the immutable nature of blockchains makes it exceedingly difficult to reverse fraudulent or erroneous transactions.

Third, due to the technical complexities involved, auditors may charge higher fees to compensate for the cost of learning or innovating in accounting solutions. As the use of Bitcoin and other crypto and digital assets grows worldwide for investment, operational, and transactional purposes, auditors also invest in technology infrastructure and involve professionals with specialized skills and knowledge to assist them in auditing digital assets. In addition, auditors have to design new audit plans and procedures and keep updating audit programs according to their knowledge about crypto-related businesses (Vincent and Wilkins, 2020). These costs impact audit efforts and work.

Anecdotal evidence shows that auditors need assistance from professionals (i.e., IT professionals and internal valuation specialists) with skills and knowledge in cryptography,

[20]Particularly, auditors need to understand and verify the internal control over financial reporting that is designed and implemented at client sites and/or third-party entities. This includes understanding and verifying the generation and management of private keys and the reliability of blockchain information to be used as audit evidence, the client's personnel, or expertise to deal with crypto assets.

distributed ledger technology, and valuation to evaluate the sufficiency of audit procedures (see Figure IA.1). Apart from spurring greater efforts and employing staff with specialized skills and knowledge, auditors also invest in specialized software audit tools to compare records of digital asset holdings to public blockchain records.

Taken together, the above discussion predicts that client cryptocurrency exposure is associated with higher audit fees.

H1a: *Client cryptocurrency exposure is positively associated with audit fees.*

Consistent with prior research showing an incremental audit effort and the lack of auditor experience is correlated with audit report lag (Knechel and Payne, 2001), we expect cryptocurrency exposure to increase audit report delay. First, as summarized in Table 1, cryptocurrency introduces complex risks across multiple financial statement assertions, including valuation, existence, completeness, ownership and disclosure. These risks make financial statements vulnerable to material misstatements, omitted disclosures, and transactions with unknown related parties. Therefore, to adequately address these risks, auditors must exert additional effort with more extensive procedures to obtain sufficient appropriate audit evidence. Further, auditing cryptocurrency exposures may require specialized technical skills that audit teams lack. Without experienced staff with cryptocurrency expertise, auditors may struggle to address the unfamiliar and complex matters with appropriate judgment this emerging risk area introduces. Taken together, we propose the following hypothesis:

H1b: *Client cryptocurrency exposure is positively associated with auditor efforts.*

2.3.2 Auditor reporting

As a consequence of the aforementioned issues, we expect that auditors become more conservative in auditing clients exposed to cryptocurrency, increasing the likelihood that clients receive a going concern opinion. There is a reason to believe this may be true. Making decisions under conditions of uncertainty entails the estimation of risk, which then alters the

behavior of risk-averse individuals by behaving more conservatively (Lennox and Kausar, 2017). Previous studies report that auditors respond to greater estimation risk by being more conservative (Lu and Sapra, 2009; Hu, Xu and Xue, 2022). In particular, auditors issue more going-concern opinions, resign more often from audit engagements, and charge higher audit fees (Lennox and Kausar, 2017; Chy and Hope, 2021; Lu and Sapra, 2009; Hu et al., 2022). These strategies are costly, but they reduce auditors' potential litigation and reputation losses when facing high-engagement risk clients.

As an emerging issue that may even fit the "too difficult" box of accounting (Barth, 2022), cryptocurrency introduces complex risks and subjectivity across multiple financial statement audit assertions, which auditors must address through professional judgment and skepticism. Those characteristics of the audit coincide with the information auditors are required to communicate through critical audit matters (CAMs). CAMs provide insights into the nature, extent and resolution of matters requiring auditor judgment beyond going concern issues (Minutti-Meza, 2021). Auditors may thus use the CAM section as a complement to firms' reporting and going concern opinions to increase the usefulness of audit opinions. Furthermore, providing CAMs related to cryptocurrency might also play a forewarning effect to mitigate perceived auditor responsibility for CAM-related material misstatements (Kachelmeier, Rimkus, Schmidt and Valentine, 2020).

Given the above arguments and against the backdrop of an absence of authoritative guidance, uncertainty in the underlying bounds of the firms' business as well as the volatility of cryptocurrency and technological complexity, we expect that auditor reporting conservatism increases. We state two formal hypotheses:

H2a: *Client cryptocurrency exposure is positively associated with the probability of receiving a going-concern opinion.*

H2b: *Client cryptocurrency exposure is positively associated with crypto-related critical audit matters.*

2.3.3 Audit office hiring efforts

The above predictions are not without tension. While no prior work explores in detail whether crypto-related business changes auditors' behavior, existing empirical studies argue that public blockchains allow more accurate and real-time record-keeping (Yermack, 2017). Such transparency may lead to greater assurance and fewer tests needed during the audit or even reduce the role of auditors. Moreover, blockchain, the technology that underpins cryptocurrency, can make transactions more efficient, safer, and easier. It may benefit the auditors regarding data reliability and the real production of financial statements, implying greater audit efficiency. If these latter reasons dominate, we may not find evidence in support of our predictions. In fact, audit offices may react to greater cryptocurrency exposure by changing their hiring efforts and adapting to the new environment through changes in their investment in human capital. Indeed, given audit competence is an essential input for audit quality (DeAngelo, 1981), conducting an audit for a client involved in cryptocurrency may necessitate the engagement of professionals with distinct expertise in cryptocurrency and blockchain technology. This specialized knowledge is requisite for certain audit procedures, as evidenced by Microstrategy's Critical Audit Matter (see Figure IA.1).

Cryptocurrency represents an emerging risk that potentially extends beyond an auditor's existing domain of expertise. Hence, this need for specialized knowledge could stimulate the recruitment of new personnel adept in these areas.[21] In addition, this challenge also presents an opportunity, as both cryptocurrency and blockchain technology hold the potential to introduce novel business prospects for auditors. Hence, hiring more employees with crypto-related skills may help an auditor leverage those benefits. The hiring demand triggered by client exposure aligns with recent evidence of how an auditor with specialized technical skills (e.g., artificial intelligence) plays a pivotal role in supporting an auditor in the context of the technology revolution to enhance audit quality (Commerford et al., 2022; Fedyk et al., 2022).

[21]Table IA.2 provides a sample of actual crypto-related job postings in the posted year of 2022.

Although such demand could manifest at both national and local levels, the local offices are largely responsible for personnel assignment, client contracting, and many other strategic functions. Therefore, we propose our final prediction at the audit-office level:

H3: *Client cryptocurrency exposure is positively associated with the number of audit-office crypto-related job postings.*

Although we predict a positive relationship between client cryptocurrency exposure and auditor crypto hiring, such a relationship may not exist. An immaterial level of exposure may not require specialized expertise if the auditor's general knowledge suffices to address limited risks. Even if cryptocurrency exposure is material, it may be manageable without additional hiring by leveraging general audit expertise, audit firm guidance, and internal training. Cryptocurrency risks can potentially be addressed without adding crypto-specific roles. Auditors can also respond to crypto risks through means other than recruitment, such as increasing audit fees or taking more conservative reporting decisions.

3 Measuring client-level exposure to cryptocurrency

3.1 Data sources

We define client exposure to cryptocurrency as the proportion of discussion in sections "Item 1 Business" and "Item 1A Risk Factors" of annual reports (10-K filings) that are devoted to the topic of cryptocurrency.[22] To quantify client exposure, we build on the idea that regulated disclosures are the most comprehensive information source on organizational business and risks (SEC, 2011), which, in turn, are directly related to auditors' responsibility to express their opinion on the truth and fairness of financial statements. We focus on audited annual reports rather than other unaudited narratives commonly used in prior work (such as quarterly

[22]See Hassan et al. (2019, 2023) and Sautner et al. (2023) who define exposure as the proportion of conversation in the earning call devoted to the topics of interest.

earning calls) given our focus on auditors.[23] Audited annual reports are a comprehensive channel to disclose information, even if investors do not always appear attentive to their full content (Cohen, Malloy and Nguyen, 2020). In addition, because the development of cryptocurrency is still in its infancy (World Bank Group, 2020), building our measure on annual reports instead of earning calls also allows us to avoid potential biases from varied questions and answers as well as the ambiguous language used in these calls (Florackis, Louca, Michaely and Weber, 2022). Disclosures on Item 1/Item 1A sections are mandated by SEC regulation, requiring firms to provide an accurate description of firm operations and the most significant risk factors that apply to the company or to its securities "that make them speculative or risky" (Regulation S–K, Item 105(c), SEC 2005). This makes these sections the most relevant to have a clean setting and reduce measurement errors in topic classification.

We download all 10-K reports of companies from EDGAR and extract the fiscal year and central index key (CIK) from each filing. Our initial sample covers 118,116 unique 10-K filings starting from 2008, the first time Bitcoin was introduced by Nakamoto and Bitcoin (2008), up to June 7, 2023 which comprehensively covers fiscal years from 2008 to 2022. We then parse the text of Items 1 and 1A and remove observations with Items 1 containing less than three sentences and thirty words to mitigate measurement errors.[24] This leaves us with a sample of 106,887 firm-year observations. As 2013 is the first time cryptocurrency exposure was detected in our population, we then keep observations from fiscal years 2013 to 2022 to conduct our analysis.

We obtain data auditor profession on Lightcast (formerly Burning Glass Technology) in the U.S. from 2010 to 2023 following prior research questioning how technological advancement is shaping the labor market (Acemoglu, Autor, Hazell and Restrepo, 2020; Acemoglu and

[23]According to PCAOB AS 2710 "*Other Information in Documents Containing Audited Financial Statements*', auditors are required to read the other information in documents containing the audited financial statements and consider whether such information or the manner of its presentation is materially inconsistent with information appearing in the audited financial statements or contains a material misstatement of fact.

[24]As small firms might not be regulated to provide Items 1A, we do not remove those firms as we still keep their Items 1 to construct our measure.

Restrepo, 2020; Jiang, Tang, Xiao and Yao, 2021).[25] We started with a list of audit firms in Audit Opinion in Audit Analytics from the calendar year 2010. We manually matched the employers' names in Lightcast with the names of auditors in Audit Analytics and retrieved any job postings that mention crypto-related keywords in Table A.1. To minimize false positives, we retain only those jobs by audit offices with the same name and the same city in both Lightcast and Audit Analytics.[26] We then use the list of crypto-related keywords in Table A.1 to identify job postings (job descriptions) that match these specific keywords.

3.2 Identifying cryptocurrency discussion and keywords

We measure the extent of disclosure related to cryptocurrency in Item 1/Item 1A. To define keywords informative about cryptocurrency discussion, we use a list of self-evident keywords and their synonyms. Table A.1 lists them. They are extracted from cryptocurrency research and newspaper articles (i.e., Financial Times, Wall Street Journal, etc.). This list includes keywords linked with the top 20 crypto coins by market capitalization after keeping coins' names with unique meanings, the underlying technology, cryptocurrency synonyms, cryptocurrency characteristics, and type of funding using cryptocurrencies. We also conducted a human audit on a random sample of Item 1 and Item 1A to adjust the initial list of keywords.

With the initial keywords, we extract the context that keywords are mentioned and perform a human audit on a random sample of Item 1 and Item 1A on 10-K filings. Particularly, we manually read sentence triples surrounding keywords to ensure that our proposed keywords

[25] Researchers have favored this data in recent years because Lightcast uses a machine learning algorithm to real-time track nearly 40,000 online job boards and company websites to parse the information of job postings. This data meets the needs of measuring the audit human capital because after removing duplicated postings and standardizing, the job-level observations capture the name of the company, job title, location, salary range, and requirements for education, skill, or professional certificates. This data covers 60 to 70 percent of high-skilled and more than 80 percent of jobs requiring a Bachelor's degree and higher. In comparison to national survey-based data (e.g., Job Openings and Labor Turnover Survey), Lightcast covers more comprehensive at the location level (Hershbein and Kahn, 2018).

[26] Audit office is defined by matching audit name (AUDITOR_NAME), opinion city (AUDITOR_CITY) and auditor state (AUDITOR_STATE) in Audit Analytics. We also consider the changes in auditors' names by checking the auditors' PCAOB registration numbers (PCAOB_REG_NUM).

capture disclosures on cryptocurrency and eliminate misidentified keywords because some common keywords capture topics other than cryptocurrency. For example, we do not use some common words though they are often used in academic journals or newspaper articles to refer cryptocurrency to *"crypto," "cryptographic," "cryptography," "digital currency/ies,"*and *"digital assets."* This is because those above-mentioned keywords per se could refer to secure information and communication techniques or anything stored digitally like images, video, word documents, PDFs, graphics, and design files.[27] To avoid such misidentification, we replace those general keywords with specific keywords that link to crypto-related discussions. Our corrected keywords are *"crypto coin," "cryptocoin," "cryptography asset,"* and *"cryptographic asset."* By specifying unigrams into multiple keywords, we reduce the probability of a false positive and avoid the wrong classification of cryptocurrency discussion.

3.3 Cryptocurrency exposure measure

To gauge exposure to cryptocurrency at the client-year level, we count the number of keywords mentioning cryptocurrency and its synonyms in Item 1/Item 1A and divide it by the total number of words in each item.

$$\text{Crypto Exposure}_{it} = \frac{1}{B_{it}} \sum_{b=1}^{B_{it}} (1[b \in C]) * 10^4 \tag{1}$$

where $b = 0, 1, ..., B_{it}$ are the words in Item 1 ($CRYPTO\_BUS\_EXPOSURE$) or Item 1A ($CRYPTO\_RISK\_EXPOSURE$) of firm i in year t, B_{it} is the total number of words in Item 1 or Item 1A, $1[\cdot]$ is the indicator function, and C is the set of crypto-related words in Table A.1.

[27]We provide examples of sentence triples in Table IA.1 with typical excerpts of non-cryptocurrency topics. Mentioned by BroadVision Inc and Tel Instrument, Electronics Corp, *"Crypto"* or *"cryptographic"*, and *"cryptography"* refer to general security algorithms but not clearly link to blockchain technology. The term *"digital assets"* in Gaia Inc and Beyond Commerce, Inc. example, are digitized contents such as images, videos, and documents.

3.4 Cryptocurrency topic exposure measure

The second purpose of our measure is to understand the nature of cryptocurrency exposure by detecting and quantifying the specific activities and risks associated with each audit engagement. Understanding the client environment is essential for auditors as they must effectively identify and assess risks to address them with appropriate audit responses. In this regard, we follow the approach validated by recent studies (Hassan et al., 2019, 2023; Sautner et al., 2023) to classify the topic of each sentence triple and calculate the topic exposure at each item 1/1A. A sentence triple is a set of three consecutive sentences in which the middle sentence contains the keyword(s) related to cryptocurrency.

We use an iterative process starting with a limited set of seed words generated by human reading and then expanding it to explore new keywords and validate the set of keywords until satisfying a threshold of classification agreement between human and machine classification in the training set. In this way, the algorithm incorporates human expertise and judgment with machine learning to ensure that the classification is not only economically meaningful but also clear and applied on a large scale of data. It should be noted that the use of machine learning here is to support us in exploring potential keywords rather than solely relying on it. While machine learning is able to explore several keywords, it also generates terms that are seemingly unrelated to the topic of interest. Therefore, we make the final decision in selecting the most relevant keywords to use in topic classification. We detect four main topics of business activities in Item 1: *(1) production, (2) transaction, (3) mining, (4) investments* and five risk topics in Item 1A: *(1) regulation, (2) business operations, (3) cybersecurity attacks, (4) market risks, and (5) peer risks* and their topic-specific keywords.

To streamline the analysis process, we extract sentence triples surrounding cryptocurrency keywords to ensure the necessary context to infer the topics of cryptocurrency. More specially, we collect 17,127 sentence triples in Item 1 and 8,229 in Item 1A. After excluding duplicated

discussions, we get 13,996 sentence triples in Item 1 and 6,696 in Item 1A, respectively.[28] We provide a detailed description of the procedure with specific details in the Internet Appendix B.

After having the topic-specific keywords and classifying all sentence triples, we then calculate the score of topic exposure at each item as the following equation:

$$\text{Crypto Topic Exposure}_{it}^{T} = \frac{1}{S_{it}} \sum_{s=1}^{S_{it}} (1[s \in C^{T}]) * 10^{2} \tag{2}$$

where S_{it} is the total number of sentence triples in Item 1 or Item 1A, $1[\cdot]$ is the indicator function, and C^{T} is the set of final keywords associated with one of the topic categories T shown in Table A.2 and Table A.3.

3.5 Validation

Validating a newly created text-based measure is crucial to establish its empirical credibility. We follow recent studies of Hassan et al. (2019), Hassan et al. (2023), and Sautner et al. (2023) to validate our measure in two main steps: (i) face validity by manually checking and updating the keywords in the context that they are mentioned and (ii) level validity by analyzing the variation of our measure across industries and years.

3.5.1 Face validity of cryptocurrency keywords

We use corrected keywords to measure cryptocurrency exposure at client-level observations following Equation (1). We re-audit by reading snippets around the keywords in the top 50 highest scores firms. Table IA.3 presents selected observations with scores of crypto-business exposure and typical snippets where validated keywords allow us to capture properly the discussion of cryptocurrency in Items 1.[29] The context surrounding keywords discussion of

[28] Duplicates are driven by sentence triples mentioning more than one keyword in its middle sentence.
[29] For firms with more than one observation at the top, we present the highest score.

various business activities implies that our measure captures multifaceted cryptocurrency businesses. For example, we detect Bitcoin holding in MICROSTRATEGY Inc (31-Dec-22), mining in MGT CAPITAL INVESTMENTS, INC. (31-Dec-20) and CLEANSPARK, INC. (30-Sep-22) that could be linked to the cryptocurrency accounts in the financial statements. More interestingly, our measurement also detects other activities such as mining cryptocurrency through a subsidiary (T-REX Acquisition Corp., 30-Jun-22), designing and distributing mining machines (MGT CAPITAL INVESTMENTS, INC., 31-Dec-20), online e-commerce marketplace (INTEGRATED VENTURES, INC. 30-Jun-18) that could be hard to detect from the financial statements. Overall, we review all snippets of the top 50 observations and double-check with the entire Item 1 to ensure that corrected keywords capture cryptocurrency exposure and the levels of exposure measured by such keywords are intuitively consistent with human reading.

We continuously use face validation by reading all snippets and Items 1A, where those snippets are exerted. Table IA.4 presents selected observations from the top 50. The discussions devoted to cryptocurrency risks cover several aspects, such as the unregulated nature of cryptocurrency, market volatility, cybersecurity, regulations, custody and security. Overall, face validity ensures that our keywords appear in the context of discussing cryptocurrency in both Items 1 and 1A. Measuring by corrected keywords, firms with the highest scores discuss cryptocurrency business and risk extensively in their annual reports.

We finalize the face validity at the keywords level. We sort keywords by their frequencies in Table IA.5 and then review each keyword in the context of sentence triples from top to bottom to ensure that keywords are not misclassified.

3.5.2 Time-series variation

After validating cryptocurrency keywords and the client-level measure, we analyze the scores at the year-level and industry-level to examine the properties of the exposure measures. We

first provide summary statistics across years in Table IA.6. Based on these results, we then plot the distribution of Items 1/1A mentioning cryptocurrency keywords in Figure 3 and the times-variations of measures in Figure 4.

In Table IA.6 and Figure 3, cryptocurrency discussions first appeared in 2013 with a small number and reached about 4.2% of the population, 249 clients in 2022. Notably, the year 2013 was also the first time that Bitcoin's prices were available on the CoinMarketCap (on April 28, 2013). The fully overlapped time scale of our measures and public data of Bitcoin prices confirms that our keywords identify cryptocurrency exposure properly during years that cryptocurrencies are publicly traded. The number and proportion of firms discussing cryptocurrency business reached the first peak in 2018 at 124, consistent with the spike observed in the cryptocurrency market capitalization in January 2018. This number then slightly decreased in 2019 before consistently increasing again from 2020 to 2022. The variation in cryptocurrency exposure and the number of firms exposed to cryptocurrency is consistent with the pattern observed in Figure 1. In addition, risk disclosures kept increasing throughout the whole period, suggesting firms' continuous awareness of heightened cryptocurrency risks during this time. After analyzing the general trend of cryptocurrency discussions, we exploit detailed times-series variations of cryptocurrency exposure. Figure 3 highlights the first positive time trends of average exposure scores from 2013 to 2018, indicating that our measures capture the substantial evolution of cryptocurrency.

After analyzing the general trend of cryptocurrency discussions, we exploit detailed times-series variations of cryptocurrency exposure. Figure 4 indicates that our measures capture the substantial evolution of cryptocurrency. In addition, the slight reduction from 2018 to 2019 and the upward in the last three years of both business and risk exposure measures also eventually reflect the main moments of the coin market cap. We then present variations in different topics. Although they are somewhat correlated, the divergence of our topic exposures suggests that our classification could be meaningful and capture different facets of cryptocurrency exposure.

3.5.3 Industry variation

Figure 5 compares the number of firms and the average values of cryptocurrency exposure among Fama-French 12 industries; more details are provided in Table IA.7. The largest number of client-year observations and highest mean values are shown in the Business equipment and Finance sectors. This is because even though the number of firms exposed to cryptocurrency business in *Business Equipment* and *Finance* is nearly equal, *Finance* has doubled non-exposed firms (about around 26,000 in both Panel A and Panel B, Table IA.7). Notably, the *Wholesale, Retail, and Some Services* sector is ranked highly in both panels. Except for the three mentioned sectors, the remaining sectors have a small number of firms exposed to cryptocurrency but with very high scores. Even untypical in each industry, a highly exposed firm could push the average score in its sector if the sector includes not many firms. We then review the snippets of business and risk disclosures and see that firms in *Business Equipment* are highly oriented to technology, while one-third of *Finance* firms are not involved in cryptocurrency business but are exposed to the competition from other firms. This concern could be found in Seacoast Banking Corporation of Florida's snippet on December 31, 2019 (see Table A.3): *"In addition, the widespread adoption of new technologies, including internet banking services, cryptocurrencies, and payment systems, could require substantial expenditures to modify or adapt our existing products and services as we grow and develop our internet banking and mobile banking channel strategies in addition to remote connectivity solutions."* In general, firms in industries that are more dependent on technology (*Business Equipment*; *Wholesale, Retail and Some Services*; and *Finance*) are more exposed to cryptocurrency business than other firms (*Oil, Gas, Coal Extraction and Products* and *Utilities*). Taken together, our measures based on validated keywords intuitively capture both the time series and industry variations of client-level exposure to cryptocurrency in several dimensions and by their compositions.

4 Empirical method

4.1 Client-level exposure to cryptocurrency and auditor responses

To examine auditors' response to client exposure to cryptocurrency, we estimate the following ordinary least squares (OLS) regression model:

$$Auditor\ responses_{it} = \beta_0 + \beta_1 * Crypto\ exposure_{it} + \beta * Z + \epsilon_{it} \tag{3}$$

where $Auditor\ responses_{it}$ is alternatively: (i) the natural logarithm of audit fees in year t ($LNAUFEES_{it}$), (ii) the number of days between a client's fiscal year-end and auditor signature date ($AUDITLAG$), (iii) an indicator variable that equals one if the auditor issues a going-concern opinion to the client in year t and zero otherwise (GCO_{it}), (iv) the percentage of CAMs mentioning cryptocurrency-related keywords ($CAMCRYPTO$). We follow Lennox and Kausar (2017) and Chy and Hope (2021) to measure GCO_{it} as a proxy for auditor conservatism. We also consider the proportion of CAMs mentioning cryptocurrency ($CAMCRYPTO$) because they refer to especially challenging, subjective, or complex auditor judgments, but caution should be applied when interpreting the results as the number of CAMs mentioning cryptocurrency keywords is small in our sample.

$Crypto\ exposure_{it}$ is our variable of interest and is defined as the cryptocurrency exposure measure in year t. We also split $Crypto\ exposure_{it}$ into business exposure ($CRYPTO\_BUS\_EXPOSURE$) and risk exposure ($CRYPTO\_RISK\_EXPOSURE$) and their specific topics to document the association between firms' exposure to cryptocurrency and auditor' responses. If auditors respond to the firms' exposure to cryptocurrency by either increasing audit fees (H1a), increasing the audit reporting lag (H1b), or increasing the probability of issuing going-concern opinions (H2a) and the number of crypto-related CAMs in the auditor's reports (H2b), β_1 will be positive.

Z is the set of control variables previously found to be related to audit fees and auditor reporting behaviour. Specifically, prior work considers client attributes (size, inherent risk, profitability, leverage), auditor attributes (audit quality), and engagement attributes (audit report lag) (Hay et al., 2006; Carson, Fargher, Geiger, Lennox, Raghunandan and Willekens, 2013). Therefore, we control for client size, leverage ratio, cash flows from operation to total assets, return on assets, sale growth, the book-to-market ratio, an indicator if a firm reports a loss for the year, an indication of having any restructuring costs, an indicator of Big4 auditors, the number of business segments and geographic segments. We include 12 Fama-French industry and year fixed effects to control for unobserved factors that differ across industries and unobserved common factors that vary over time and cluster standard errors at the industry level. Finally, given that our client-level exposure to cryptocurrency may vary at the industry level, we cluster standard errors by industry to account for the concern that the residuals are serially correlated across clients in the same industry.

To test the hypothesis of auditor hiring efforts at the office level (H3), we estimate the following OLS regression at the audit office level:

$$\textit{Office hiring efforts}_{jt} = \beta_0 + \beta_1 * \textit{Crypto exposed clients}_{jt} + \beta * Z_{jt} + \epsilon_{jt} \tag{4}$$

where $\textit{Office hiring efforts}_{jt}$ is the natural logarithm of crypto-related job postings plus one in calendar year t of audit office j ($LN\_JOB\_POSTINGS_{jt}$), $\textit{Crypto exposed Clients}_{it}$ is alternatively the natural logarithm of clients having a positive value to either (i) $CRYPTO\_BUS\_EXPOSURE$, (ii) $CRYPTO\_RISK\_EXPOSURE$ plus one. We also include controls for the average (mean) traits of an office's client portfolio (Z_{jt}). β_1 is expected to be positive, suggesting that an audit office seeks more new hires with crypto-related skills when having more clients exposed to cryptocurrency.

4.2 Test of a possible explanation for auditor responses

We propose that auditors' responses to client-level exposure to cryptocurrency are due to the lack of authoritative guidance in accounting and auditing. This notion has not been thoroughly examined in previous research.[30]

To test whether the lack of authoritative guidance in accounting and auditing for cryptocurrency is a channel driving auditor response to client-level exposure to cryptocurrency, an ideal quasi-experiment could be a difference-in-differences estimator (DiD) where the issuance of official guidance on how to account for cryptocurrency is a treatment event. However, there is no variation in the amount of official guidance in accounting and auditing for cryptocurrency from regulatory bodies during our research period. We then searched for other guidance issued by accounting associations in the U.S. There is guidance issued by AICPA on December 16, 2019 (see Figure 2). Since our sample extends until the fiscal year end of 2020, using an event in 2019 could lead to biased estimation due to many macroeconomic factors driven by the COVID-19 pandemic. Hence, we decided not to use this event. Instead, we overcome this empirical challenge and indirectly test the mechanism by collecting the audit client-level guidance. The idea is that it could proxy for auditor awareness of cryptocurrency, a new risk factor that auditors have to proactively address through additional investment in audit competence through developing accounting and audit procedures and training staff. We exploit variation in the content of Big4's guidance on accounting for cryptocurrency and examine whether auditors with longer guidance experience any increase in audit fees and auditor conservatism following their issuance. We expect that an increased audit fees or greater audit conservatism report could capture audit responses to the lack of official accounting guidance in clients exposed to cryptocurrency.

[30]We also examine whether auditor responses to client-level exposure to cryptocurrency arise from the underlying client business risk. To capture changes in cryptocurrency volatility, we compute the ratio of changes in Bitcoin prices from year t to year $t-1$ to its price in year $t-1$ and create an indicator variable equal to one if this ratio is negative ($COIN\_DOWN_t$).

We test whether auditor responses are stronger when there is a lack of authoritative guidance by estimating the following OLS model:

$$\begin{aligned} \textit{Auditor responses}_{it} = \beta_0 + \beta_1 * \textit{Crypto exposure}_{it} + \alpha * \textit{Big4 guidance}_t \\ + \gamma * \textit{Crypto exposure}_{it} * \textit{Big4 guidance}_t + \beta * Z + \epsilon_{it} \end{aligned} \tag{5}$$

Auditor responses$_{it}$ is defined as in Equation (3). *Big4 guidance*$_t$ is the natural logarithm of the number of pages of guidance documentation available for clients. We consider the differences in guidance among Big4 accounting firms, so *Big4 guidance*$_t$ is a placeholder for each Big4's guidance.[31] We match audit firm guidance to client data using the fiscal-year end *after* the guidance issuance date. To illustrate this proxy, during our sample period from 2013 to 2022, EY issued its first guidance on accounting for crypto-assets in August 2018 and the second one in September 2019. The document containing the guidance is 24 pages and 29 pages long, respectively. Hence, $EY\_GUIDANCE_t$ equals 3.178 (the ln(24)) for all clients of EY whose fiscal year ends between August 2018 and September 2019. If an auditor issues additional guidance or financial reporting alerts during our sample period, then we update *Big4 guidance*$_t$ to reflect the most updated number of pages of guidance. As before, we also decompose *Crypto exposure*$_{it}$ into exposure in Item 1 "Business" and Item 1A "Risk Factors" and interact with each *Big4 guidance*$_t$ to test the prediction.

A set of control variables Z fixed effects are incorporated in the model as in the main model in Equation (3). Positive values of the interaction terms between *Crypto exposure*$_{it}$ and *Big4 guidance*$_t$ indicate that a Big4 auditor charges higher fees for their clients, exhibits a greater degree of conservatism in its reporting behavior, requires extended time periods to finalize audit engagements and issues more crypto-related CAMs after the issuance of their professional guidance.

[31] For a comprehensive list of Big4's guidance employed within our sample, please refer to Table IA.8.

5 Empirical findings

5.1 Sample selection and summary statistics

We obtain data from different databases, including COMPUSTAT, Audit Analytics, and EDGAR (10-K filings data). Although we parse all 10-Ks fillings from 2008 from the EDGAR database, 2013 is the first year cryptocurrency exposure is detected, therefore, we first filter all measurement output from 2013 to merge with other datasets. The intersection results in 33,000 firm-year observations for *audit fees*, *going-concern*, and *audit reporting lag* models from the fiscal year 2013 to 2022. Bitcoin prices (BTC-USD), used to measure cryptocurrency market volatility, are collected from Yahoo Finance starting on September 16, 2014 when data became available.[32]

The CAMs analysis covers fiscal years 2019 to 2022, yielding 7,718 client-year observations after merging the data. We select only clients containing the CAM section to calculate the ratio of crypto-related matters since the CAMs' requirements are effective for audits of large accelerated filers since fiscal years ending on or after June 30, 2019.

For the test of audit office hiring demand for cryptocurrency-skilled staff, we create the mean values of the client portfolios to proxy for audit office characteristics. We then merge this data with Lightcast job postings by employer names and year. Finally, we have 6,593 audit office-year observations from calendar years 2013 to 2022.

Table 2 presents descriptive statistics of our measures and the main variables in our regressions. All variables are defined in Table A.4. The distribution of cryptocurrency exposure measures is quite skewed, with mean values of 0.234 ($CRYPTO\_BUS\_EXPOSURE$) and 0.170 ($CRYPTO\_RISK\_EXPOSURE$) while the median values are zeros, consistent with our sample that such exposures are highly concentrated in a small proportion of clients.

[32]The sample size for models examining the underlying riskiness of client business in Table IA.9 is reduced to 25,590 client-year observations due to the availability of Bitcoin prices.

The skewed values are common in papers measuring specific information from textual data at firm-level (e.g., Hassan et al. (2019, 2023); Sautner et al. (2023) with conference calls data, and Florackis et al. (2022) with 10-Ks data). Other firms' characteristics vary in the range consistent with prior research using COMPUSTAT and Audit Analytics databases. For example, the average client in our sample has audit fees of $2.183 million, close to $1.96 million in Guo, Lin, Masli and Wilkins (2021), $1.899 million in Cassell, Drake and Dyer (2018). In addition, the mean of CAMs is 1.438 compared to 1.68 in Burke, Hoitash, Hoitash and Xiao (2022), our audit lag is about 66.4 days compared to 63.602 days in Guo et al. (2021) and 65.598 days in Cassell et al. (2018). Our mean of GCO is 0.0831, roughly 0.083 in Defond, Francis and Hallman (2018) and lies in the range between 0.069 in DeFond, Raghunandan and Subramanyam (2002) and 0.103 in Guo et al. (2021). Big4 auditors audit 59.7% annual reports in our sample, compared to 66.6% in Guo et al. (2021), and 64% in Defond et al. (2018).

Table 3 shows the correlations among measures of cryptocurrency exposure and cryptocurrency topic exposure. This table exhibits that both business and risk measures are highly correlated at the client level. However, there is a slight deviation between business topics and risk topics with some values below 0.5 in the topics of $CRYPTO\_CYBER$ and $CRYPTO\_PEERS$, suggesting that different topic exposures could capture different dimensions of cryptocurrency exposures. Table 4 presents pairwise correlations among variables in audit fees and going-concern models. The table shows that $CRYPTO\_BUS\_EXPOSURE$, and $CRYPTO\_RISK\_EXPOSURE$ are highly correlated, with a correlation coefficient is 0.89 and significant at the level of 5%. Regarding auditors' responses, audit fees are correlated to cryptocurrency exposures, but the signs of correlations are negative. GCO are positively and significantly correlated to both measures in Pearson's triangle; however, they only positively correlated to $CRYPTO\_BUS\_EXPOSURE$ in Spearman's triangle. To conclude, the two correlation tables are consistent with the idea that auditors are more conservative in audit reporting, but unclear how pricing behavior changes when clients are

exposed to cryptocurrency.

5.2 Main results

Table 5 displays the basic specification that regresses different auditor responses on the client-level exposure to cryptocurrency. The analysis covers the fiscal year from 2013 to 2022 for audit fees, audit reporting lag, going-concern opinions, and CAMs.

The coefficients presented in columns (1) for $CRYPTO\_BUS\_EXPOSURE$ and (2) $CRYPTO\_RISK\_EXPOSURE$ are positively significant at the level of 5%, indicating that audit fees are higher for clients exposed to cryptocurrency. Specifically, a one-standard-deviation increase in the client-level exposure to cryptocurrency translates into a 1.0% to 1.1% fee increase, supporting H1a. The results for our control variables align with those of previous studies (Guo et al., 2021; Cassell et al., 2018). Particularly, audit fees tend to increase for larger firms, restructured firms, and those audited by Big4 auditors. Conversely, fees are lower for clients demonstrating improved operating performance, including higher cash flows from operation, positive net income, and higher book-to-market ratios.

In columns (3) and (4), the client-level exposure to cryptocurrency is positively associated with audit reporting lag, with a one-standard-deviation increase in the client-level exposure to cryptocurrency predicting about a 0.2 increase in the number of days to finalize the audit engagements. This finding provides support for H1b.

Columns (5) and (6) of Table 5 examine going-concern opinions. The coefficients of crypto expose measures are positive and significant at the level 1%, implying that cryptocurrency exposure is associated with a higher likelihood of going concern opinions. A one-standard-deviation increase in the client-level exposure to cryptocurrency corresponds to a 0.4% to 0.6% increase in the likelihood of issuing a going concern opinion, consistent with H2a, that auditors issue more conservative opinions for cryptocurrency-exposed clients. Coefficients of control variables are consistent with previous studies (e.g., Guo et al. (2021); Cassell et al.

(2018)). For example, the findings show that going-concern opinions are more likely under conditions of diminished operating performance (low CFO, low ROA, high $LOSS$), increased leverage (LEV), and smaller client sizes ($SIZE$).

Columns (7) and (8) regress the proportion of CAMs mentioning cryptocurrency keywords in an audit report on the client-level exposure to cryptocurrency for the fiscal years 2019-2022.[33] These results pertain to H2b. It should be noted that the sample of CAMs was restricted to those reported by clients, as CAMs are not mandatory for all clients before December 15, 2020. Hence, we cannot distinguish between two types of clients, (i) clients with no CAMs report and (ii) clients with CAMs but no mention of cryptocurrency keywords. The coefficients on $CRYPTO\_BUS\_EXPOSURE$ and $CRYPTO\_RISK\_EXPOSURE$ are positive and significant at 1%, suggesting that the level of exposure to cryptocurrency is positively associated with the proportion of cryptocurrency-related CAMs.

In summary, the results demonstrate an auditor responds to client cryptocurrency risks by increasing fees, conservatism in reporting decisions, audit lag, and highlighting risks in CAMs.

To understand whether audit responses depend on the nature of exposure, we repeat the test by each topic of cryptocurrency exposure. Table 6 presents the regression of auditor responses on different business exposure topics. The coefficients on most cryptocurrency business exposure are positive and significant across the audit response variables. For example, an auditor may perceive greater audit challenges from transactions and mining compared to other business activities and adjust efforts and fees accordingly. The exceptions are $CRYPTO\_PRODUCTION$ and $CRYPTO\_INVESTMENTS$, which are insignificant for audit fees. The positive and statistically significant results are also shown in other

[33]CAMs have been introduced as the first significant change to the US auditor's report in over 70 years. A limited number of audit engagements in our sample have been subjected to the requirements of CAMs. This is because the regulation requiring auditors to communicate CAMs in their reports was effective in 2019. CAMs' requirements are effective for audits of large accelerated filers since fiscal years ending on or after June 30, 2019 and for audits of all other companies to which the requirements apply since fiscal years ending on or after December 15, 2020.

auditor responses, confirming that an auditor reacts to multidimensional cryptocurrency business exposure. It provides more granular evidence consistent with the aggregated exposure measures in Table 5. This highlights auditors tailor their responses based on the nature of clients' cryptocurrency involvement.

We extend the test to encompass various topics of cryptocurrency risk exposure in Table 7. Regarding audit pricing, all risk exposure topics except for columns (1) and (5) featuring coefficients of cybersecurity risks ($CRYPTO\_CYBER$) competition from peers ($CRYPTO\_PEER$) exhibit positive and significant associations. Regulation, operations, and market risk exposures exhibit the most pronounced fee reactions, with a 1.2% increase per standard deviation. It implies that an auditor views these risk topics as more material or challenging to audit. We also find positive, significant coefficients for risk exposure topics across the other auditor responses, including audit reporting lag, going-concern opinions, and CAMs. This further demonstrates how auditors respond to the nature of cryptocurrency risks.

Table 8 presents the results of the regression analysis using crypto-related job postings to test H3, which posits that audit firm offices with a greater proportion of cryptocurrency-exposed clients will seek to hire more auditors with expertise in cryptocurrency and blockchain technology. The positive, statistically significant coefficients on the cryptocurrency exposure variables in columns (1) - (2) provide empirical support for H3. The economic magnitude of the effects suggests that a percentage increase in the number of cryptocurrency-exposed clients at an audit office is associated with a 0.194 to 0.203 percentage increase in the number of job postings mentioning cryptocurrency, holding constant the control variables. The findings indicate that an auditor responds to having more cryptocurrency-exposed clients by trying to hire more auditors with expertise in this emerging domain. This is consistent with the hypothesis that an auditor recognizes the need for specific knowledge and skills to audit clients utilizing cryptocurrencies and blockchain technology properly. The findings provide initial indications that advancements in technology have significantly influenced the audit

profession. This is evident in their adjustments to hiring practices, which are in response to clients' increasing use of crypto-assets.

5.3 A possible mechanism explaining auditor response to client exposure to cryptocurrency

Table 9 presents regression results examining how the lack of authoritative accounting guidance affects auditor responses to clients' cryptocurrency exposure. The cryptocurrency exposure coefficients remain positive and significant, consistent with the main analyses.

Columns (1) and (2) show the results of how the lack of authoritative guidance may drive audit fees. Notably, the coefficients of the interaction terms were positive for all audit firms. However, only the interaction terms associated with EY guidance were statistically significant at 1% and 5% levels in columns (1) and (2), respectively. These findings suggest that, in comparison to other audit firms, EY increases fees to a greater degree for its cryptocurrency-exposed clients after issuing its own guidance.

Looking at audit reporting lag in columns (3) and (4), the interaction terms for PwC and EY guidance are significantly positive, while KPMG's is negative. It confirms the heterogeneity across audit firms in how they codify the guidance. For example, the guidance from EY and PwC takes a more detailed approach in their interpretation of the guidance compared to other firms. These two provide a greater number of illustrations and accounting methodologies for addressing cryptocurrency-related accounting matters.

The results regarding going-concern opinion issuance are provided in Columns (5) and (6). The interaction terms for PwC and Deloitte guidance are significantly positive, while KPMG's is negative. This suggests that even after releasing some guidance on cryptos, PwC and Deloitte maintain relatively more conservative auditor reporting for their cryptocurrency-exposed clients. In contrast, KPMG guidance appears to be associated with reduced conservatism.

We then estimate the effects of having audit firms' guidance on CAMs. Most of the coefficients on the interaction terms in columns (7) and (8) are negative and significant, indicating that the presence of audit guidance at audit firms lessens audit complex and challenging matters in the audit. The finding that audit firm guidance is associated with fewer cryptocurrency-related CAMs implies these guides have partially equipped auditors to handle the complexities of auditing crypto assets and activities. By codifying procedures, risk assessments, and best practices, the guidance allows auditors to approach cryptocurrencies in a more standardized, less subjective manner. This results in fewer matters rising to the level of CAM disclosure.

Collectively, the findings indicate lack of authoritative guidance plays a role in auditor reactions. The increased fees and maintained conservatism suggest persisting challenges despite some firm guidance. However, the reduced CAMs imply guidance assists in auditing complexity. Without authoritative standards, audit firms appear cautious and invest in audit knowledge with their own accounting guidance for their clients. Auditors pass such increased audit costs to clients by increasing audit fees; eventually, having guidance at the audit firm level could lessen subjectivity, complexity, and difficulty in the audit, resulting in a lower proportion of critical audit matters related to cryptocurrency. These results highlight the difficulty in auditing novel ecosystems like cryptocurrencies and the vital role of evolving guidance to match the pace of technological innovation.

Additionally, the results shown in Table IA.9 suggest auditors charge a volatility premium through higher fees when cryptocurrency riskiness increases during downturns. In contrast, we do not find significant interaction effects for the other auditor responses, such as going concern opinions, audit reporting delay, and CAMs. A potential explanation is that auditors can adjust fees in a faster manner in responding to changing market conditions compared to the other responses.

5.4 Additional analyses

5.4.1 Different estimation based on matching samples

To further validate our findings, we conducted additional analyses using matched samples based on propensity score matching and covariate matching. We first estimated propensity scores for cryptocurrency exposure using key covariates from our models. Firms exposed to cryptocurrency were then matched to non-exposed firms with similar propensity scores using nearest neighbour 1:1 matching without replacement. We also created a matched sample by directly matching key covariates from our models. Tables IA.10 and IA.11 compare firm characteristics between firms exposed and not exposed to cryptocurrency. All p-values are greater than 0.05, indicating that there are no statistically significant differences across covariates between exposed and unexposed clients after matching at the level 5%.

Using these matched samples, we re-estimated our auditor response models. The results, shown in Table IA.12, remain consistent with our main findings in Table 5. Across various model specifications, the coefficient on cryptocurrency exposure remains positive and statistically significant. The persistence of significant effects after matching lends further credence to our conclusions about the relationship between client-level exposure to cryptocurrency and auditor responses.

5.4.2 Alternative measure of client-level exposure to cryptocurrency

Finally, we redefine our cryptocurrency exposure by including an indicator variable that equals to one if keywords related to cryptocurrency (see Table A.1) occur in Item 1 "Business" or Item 1A "Risk factors" of a 10-K filing and zero otherwise. We then re-estimate the audit response models from Equation (3) using this alternative cryptocurrency exposure measure.

The results presented in Table IA.13 are consistent with estimates by continuous measures in Table 3. Specifically, the cryptocurrency exposure indicator variable is positively and

significantly associated with all auditor response variables, including audit fees, going-concern opinions, audit reporting lags, and the proportion of CAMs mentioning cryptocurrency.

For the audit fees model in Columns (1) and (2), the marginal effects of cryptocurrency exposure range from 0.162 to 0.193, implying that exposure increases audit fees by 17.58% to 21.28%.[34] Columns (3) and (4) show that cryptocurrency-exposed clients have audit report lags that are 2.7 to 5.26 days longer. In Columns (5)-(6), the results indicate that firm exposure to cryptocurrency raises the likelihood of receiving going-concern opinions by 4.8% to 6.7%. Although positive, the association between cryptocurrency exposure and the proportion of CAMs related to cryptocurrency is statistically insignificant. Overall, using an alternative binary indicator for cryptocurrency exposure yields consistent results, providing further evidence that exposure is associated with heightened auditor effort and scrutiny.

6 Conclusion

This study develops novel measures of client-level cryptocurrency exposure based on textual analysis of "Item 1 Business" and "Item 1A Risk Factors" sections in 10-K filings. To our knowledge, this represents one of the first attempts to quantify exposure to cryptocurrency - an emerging asset class that transcends traditional client boundaries. We then use these new measures to investigate the relationship between client-level exposure to cryptocurrency and auditor responses. The results demonstrate that greater client cryptocurrency exposure corresponds to increased audit fees, heightened auditor conservatism, and longer audit report lags. While the analysis of critical audit matters mentioning cryptocurrencies is directionally consistent, the results should be interpreted cautiously, given the limited sample size. We corroborate our findings using propensity score matching and covariate matching, yielding similar conclusions.

Importantly, this study provides evidence that the lack of authoritative accounting

[34]The economic magnitudes are calculated as exp(0.162)-1 and exp(0.193)-1 respectively.

guidance on cryptocurrency is a potential mechanism driving auditors' heightened scrutiny of cryptocurrency-exposed clients. The absence of authoritative standards creates uncertainty for auditors regarding the appropriate accounting treatment and disclosure of cryptocurrency activities. Our results suggest auditors respond to this lack of guidance by exerting greater effort and exhibiting conservatism when auditing cryptocurrency-exposed clients. More broadly, these findings highlight how auditors proactively respond to new risk factors that emerge outside formal client boundaries and under conditions of uncertain regulatory guidance.

Finally, we provide preliminary evidence that technological advancements have profoundly impacted the audit profession. This is exemplified by auditors' shifting recruitment strategies in reaction to clients' growing cryptocurrency exposure and underlying blockchain technologies. Further research can build on this study by exploring how auditors adapt their practices to address other emerging technologies and their associated risks.

Appendices

Table A.1: Keywords for searching cryptocurrency discussion

Category	**Keywords**
Top crypto coins ranked by market capitalization with unique meanings	bitcoin
	ethereum
	litecoin
	dogecoin
	usd coin
	binance usd
	altcoin
Underlying technology	blockchain
Cryptocurrency synonyms	crypto asset*
	crypto coin*
	cryptocoin*
	cryptocurrenc*
	crypto currenc*
	crypto mining
	cryptography asset*
	cryptographic asset*
Cryptocurrency characteristics	distributed ledger
	decentralized ledger
Type of funding using cryptocurrencies	initial coin offering

This table lists keywords used to identify discussion in Item 1 and Item 1A related to cryptocurrency. Those keywords and their synonyms will be extracted from current papers related to cryptocurrency and newspaper articles (i.e. Financial Times, Wall Street Journal, etc.). We begin by identifying the top 20 coins based on their market capitalization and keep ones with unique meanings. This list comprises the names of cryptocurrency coins ranked by market capitalization after keeping coins' names with unique meanings, the underlying technology, cryptocurrency synonyms, cryptocurrency characteristics, and type of funding using cryptocurrencies. We also conduct a human audit on a limited sample of Item 1 and Item 1A to verify that we are using the crypto-related words.

Table A.2: Keywords for cryptocurrency business exposure

Topics	Patterns	Example sentence triple	Observations
production	develop*, product*, service*, solution*, client*, customer*, deliver*, offer*	We have recently begun offering derivative products linked to Bitcoin and other cryptocurrencies in certain jurisdictions, and intend to expand the types of products offered, the associated types of cryptocurrencies and the jurisdictions in which the products are offered. The distributed ledger technology underlying cryptocurrencies and other similar financial assets is evolving at a rapid pace and may be vulnerable to cyberattacks or have other inherent weaknesses that are not yet apparent. We may be, or may become, exposed to risks related to cryptocurrencies or other financial products that rely on distributed ledger technology through our facilitation of clients activities involving such financial products linked to distributed ledger technology.	GAIN Capital Holdings Inc. ;December 31, 2017
		These new lines of business pose risks and challenges that could materially impact our business, financial condition and results of operations. Currently, all of the revenue generated from these endeavors has been derived from our technology services agreement with ProximaX that is related to the implementation of PSP into ProximaX proprietary blockchain protocol. However, the success of our new ventures substantially depends upon our ability to expand our client base beyond ProximaX, and our failure to do so would have a material negative impact on our ability to generate revenue and our financial condition.	PeerStream Inc.; December 31, 2018
transaction	payment*, transaction*, wallet*, accept*	We expect that the users of our blockchain based payments solution, when such solution is fully implemented, will be able to make payments by using payment options of their preference fiat m1y, mainstream and alternative cryptocurrencies. The main function of the blockchain based payments solution is to provide the 1 click payment technology solution with minimum transaction costs and maximum comfort for the users. We expect that such function will be complementary to our current platform which supports multiple payment methods internationally.	Net Element, Inc.; December 31, 2017
		Avra plans to charge a percentage of the transaction in the same way as a credit card provider. AvraATM is another technology solution planned by the Company is called AvraATM, which it plans to develop a software to be integrated with kiosks which will allow the kiosk to have the ability to accept payments, effectively converting the existing kiosk into a purchase point (ATM) for bitcoin and other cryptocurrencies. The planned revenue model is 1 where a percentage fee will be charged for the purchase of currency which will vary depending on the expectations of the individual owners of each kiosk ne2rk.	Avra Inc.; January 31, 2015

TABLE A.2 (continued from previous page)

Topics	Patterns	Example sentence triple	Observations
mining	min*, block*, power capacity, block*, pool*, processing power, computer*, equipement*	We believe that our current inventory of miners establishes us among the top public companies in the United States mining cryptocurrency. Government Regulation Government regulation of blockchain and cryptocurrency is being actively considered by the United States federal government via a number of agencies and regulatory bodies, as well as similar entities in other countries. State government regulations also may apply to our activities and other activities in which we participate or may participate in the future.	Marathon Digital Holdings Inc.; December 31, 2020
		As of June 30, 2021, we operated our cryptocurrency mining operations in a hosted facility located in Carthage, New York, and effective September 1, 2021, expanded our mining operations to a second hosted facility located in Kearney, Nebraska. The hosting and power purchase agreements for the 2 facilities require the Company to pay monthly a contractual rate per kilowatt hour of electricity consumed in the Company cryptocurrency mining operations. The Company is aggressively looking to expand its power capacity and is currently negotiating purchase or investment in multiple real estate properties capable of being deployed as data centers for cryptocurrency mining operations.	Integrated Ventures Inc.; June 30, 2021
investments	invest*, acquir*, hold*, divest*, share*, asset*, financ*	Our future strategy is to expand into the infrastructure technology and cybersecurity areas. We will look to acquire companies in these respective areas, focusing on companies that have the ability to utilize blockchain technology in their respective operations. Target Markets, Sales and Marketing Our target market will be primarily in North America, with a concentration in the USA and Canada.	Global Digital Solutions, Inc.; December 31, 2018
		We hold all of our cryptocurrencies in cold storage to reduce the risk of malfeasance, but the risk of loss of our cryptocurrency assets cannot be wholly eliminated. Hackers or malicious actors may launch attacks to steal, compromise or secure cryptocurrencies, such as by attacking the cryptocurrency ne2rk source code, exchange miners, third party platforms, cold and hot storage locations or software, or by other means. We may be in control and possession of 1 of the more substantial holdings of cryptocurrency.	OBITX, Inc.; January 31, 2021

This table exhibits four topics pertaining to activities related to cryptocurrencies: (1) production, (2) transaction, (3) mining, and (4) investments, and provides corresponding sentence triples as examples. To obtain word patterns for each topic, we selected 200 sentence triples mentioning crypto-related keywords from Item 1 in a random manner, then read and manually analyzed them to define the topics and establish a set of seed words related to each. Subsequently, the Latent Dirichlet Allocation (LDA) algorithm was employed to utilize these seeds and automatically classify topics, thus discovering new vocabulary likely to be indicative of the concerned topic from these corpora. The final collection of crypto-related topics and their word patterns comprise the original and newly identified keywords from the algorithm.

Table A.3: Key words for cryptocurrency risk exposure

Topics	Patterns	Example sentence triple	Observations
regulation risks	regula*, laws*, legal*, rule*, tax*, sec, irs, requirement*, compl*, treat*	There is substantial uncertainty regarding legal and regulatory requirements relating to cryptocurrencies or transactions utilizing cryptocurrencies. These uncertainties, as well as potential accounting and tax issues, or other requirements relating to cryptocurrencies could have a material adverse effect on our business.	The Meet Group, Inc.; December 31, 2018
		There is currently no broadly accepted regulatory framework for Bitcoin or other cryptocurrencies, and the regulation of cryptocurrencies is developing and changing rapidly in the United States and other countries around the world. For example, in the United States, it is unclear whether many cryptocurrencies are securities under federal securities laws, and the implications for us if any of our products are linked to cryptocurrencies that are determined to be securities could be significant and adverse. In addition, some market observers have asserted that material price increases in many cryptocurrency markets, such as that for Bitcoin, may indicate the existence of a bubble, and if markets for any cryptocurrencies linked to our products suffer severe declines, our customers could experience significant losses and we could lose their business.	GAIN Capital Holdings, Inc.; December 31, 2018
business operations	business*, operat*, stategy, prospect*, profit*	Such factors could have a material adverse effect on our ability to continue as a going concern or to pursue our new strategy at all, which could have a material adverse effect on our business, prospects or operations and harm investors. We may face risks of Internet disruptions, which could have an adverse effect on the price of digital currencies. A disruption of the Internet may affect the use of digital currencies and subsequently the value of our securities.	Riot Blockchain, Inc.; December 31, 2018
		We entered the bitcoin mining industry through our acquisition of ATL in December 2020. We acquired a second data center in August 2021 and have had a co location agreement with New York based Coinmint in place since July 2021 Bitcoin mining has now become our principal revenue generating business activity. We currently intend to continue to acquire additional facilities, equipment and infrastructure capacity to continue to expand our bitcoin mining operations.	CleanSpark, Inc.; September 30, 2021
cyber attacks	hack*, cyber, cybersecurity, criminal, botnet, malware, theft, attack*	Further, we cannot provide assurance that our wallet will not be hacked or compromised. The bitcoin and blockchain ledger, as well as other cryptocurrencies and blockchain technologies, have been, and may in the future be, subject to security breaches, hacking, or other malicious activities. Any loss of private keys relating to, or hack or other compromise of, digital wallets used to store our customers bitcoins could adversely affect our customers ability to access or sell their bitcoins and could harm customer trust in us and our products, require us to expend significant funds for remediation, and expose us to litigation and other potential liability.	Square, Inc.; December 31, 2020

TABLE A.3 (continued from previous page)

Topics	Patterns	Example sentence triple	Observations
		Moreover, in the past, flaws in the source code for digital assets have been exposed and exploited, including flaws that disabled some functionality for users, exposed users personal information and or resulted in the theft of users digital assets. The cryptography underlying Bitcoin could prove to be flawed or ineffective, or developments in mathematics and or technology, including advances in digital computing, algebraic geometry and quantum computing, could result in such cryptography becoming ineffective. In any of these circumstances, a malicious actor may be able to take the Trust Bitcoin, which would adversely affect the value of the Shares.	Grayscale Bitcoin Trust (BTC) ; December 31, 2020
market risks	volatil*, uncertain*, fluctuat*, stability, accept*, bubble, swing*, switch	If there is a significant decrease in the price of bitcoin, we will experience a more pronounced impact on our financial condition than if we used our cash to purchase a more diverse portfolio of assets. Our bitcoin holdings are less liquid than our existing cash and cash equivalents and may not be able to serve as a source of liquidity for us to the same extent as cash and cash equivalents In September 2020, we adopted bitcoin as our primary treasury reserve asset. Historically, the bitcoin markets have been characterized by more price volatility, less liquidity, and lower trading volumes compared to sovereign currencies markets, as well as relative anonymity, a developing regulatory landscape, susceptibility to market abuse and manipulation, and various other risks inherent in its entirely electronic, virtual form and decentralized network.	MicroStrategy Incorporated; December 31, 2020
		Price volatility undermines any bitcoin role as a medium of exchange, as retailers are much less likely to accept it as a form of payment. Market capitalization for a bitcoin as a medium of exchange and payment method may always be low. The relative lack of acceptance of bitcoins in the retail and commercial marketplace, or a reduction of such use, limits the ability of end users to use them to pay for goods and services.	Troika Media Group, Inc. ; June 30, 2021

TABLE A.3 (continued from previous page)

Topics	Patterns	Example sentence triple	Observations
peers risks	compet*, entrant*, resources	Increased competition may negatively affect our earnings by creating pressure to lower prices or credit standards on our products and services requiring additional investment to improve the quality and delivery of our technology and or reducing our market share, or affecting the willingness of our clients to do business with us. In addition, the widespread adoption of new technologies, including internet banking services, cryptocurrencies and payment systems, could require substantial expenditures to modify or adapt our existing products and services as we grow and develop our internet banking and mobile banking channel strategies in addition to remote connectivity solutions. We might not be successful in developing or introducing new products and services, integrating new products or services into our existing offerings, responding or adapting to changes in consumer behavior, preferences, spending, investing and or saving habits, achieving market acceptance of our products and services, reducing costs in response to pressures to deliver products and services at lower prices or sufficiently developing and maintaining loyal customers.	Seacoast Banking Corporation of Florida; December 31, 2019
		We do not have the resources to compete with larger providers of similar services at this time. The digital currency industry has attracted various high profile and well established operators, some of which have substantially greater liquidity and financial resources than we do. With the limited resources we have available, we may experience great difficulties in expanding and improving our network of computers to remain competitive and with creating a U.S. based digital currency exchange.	Riot Blockchain, Inc.; December 31, 2018

This table exhibits five topics pertaining to risks related to cryptocurrencies: (1) regulation, (2) business operations, (3) cybersecurity attacks, (4) market risks, and (5) peer risks, and provides corresponding sentence triples as examples. To obtain word patterns for each topic, we selected 200 sentence triples mentioning crypto-related keywords from Item 1A in a random manner, then read and manually analyzed them to define the topics and establish a set of seed words related to each. Subsequently, the Latent Dirichlet Allocation (LDA) algorithm was employed to utilize these seeds and automatically classify topics, thus discovering new vocabulary likely to be indicative of the concerned topic from these corpora. The final collection of crypto-related topics and their word patterns comprise the original and newly identified keywords from the algorithm.

Table A.4: Variable definitions

Variable	Definition
Dependent variables	
AUDITLAG	The number of days between the auditor signature date and fiscal year-end
AUFEES	The audit fees for the current year t (in millions USD)
CAMCRYPTO	The percentage of critical audit matters mentioning cryptocurrency-related keywords in year t
GCO	Indicator variable that equals one if a company receives going-concern audit opinion in year t, and zero otherwise
LNAUFEES	The natural logarithm of total audit fees of a company in year t
LN_JOB_POSTINGS	The natural logarithm of crypto-related job postings plus one in calendar year t of audit office j
N_CAM	The percentage of critical audit matters mentioning cryptocurrency-related keywords in year t
Cryptocurrency exposure	
CRYPTO_BUS_EXPOSURE	The relative frequency with which keywords related to cryptocurrency (see Table A.1) occur in Item 1 "Business" of a 10-K filling. We count the number of such keywords and divide by the total number of words in Item 1 "Busines" in year t. We multiply by 10^4 for ease of interpretation
CRYPTO_RISK_EXPOSURE	The relative frequency with which keywords related to cryptocurrency (see Table A.1) occur in Item 1A "Risk factors" of a 10-K filling. We count the number of such keywords and divide by the total number of words in Item 1A "Risk factors" in year t. We multiply by 10^4 for ease of interpretation
LN_CLIENTS_CRYPTO_RISK_EXPOSURE	The natural logarithm of the number of clients having a positive value of CRYPTO_RISK_EXPOSURE in calendar year t of audit office j plus one
LN_CLIENTS_CRYPTO_EXPOSURE	The natural logarithm of the number of clients having a positive value either of CRYPTO_BUS_EXPOSURE or CRYPTO_RISK_EXPOSURE in calendar year t of audit office j plus one
Cryptocurrency business topic exposure	
CRYPTO_PRODUCTION	The relative frequency with which keywords capture production topic (see Table A.2) in Item 1 "Business" of a 10-K filling. For topic exposure, we count only **topic keywords** appear in the sentence triples around cryptocurency keywords and divide by the total number of words in Item 1 "Business" in year t. We multiply by 10^2 for ease of interpretation
CRYPTO_TRANSACTION	The relative frequency with which keywords capture transaction topic (see Table A.2) in Item 1 "Business" of a 10-K filling. For topic exposure, we count only **topic keywords** appear in the sentence triples around cryptocurrency keywords and divide by the total number of words in Item 1 "Business" in year t. We multiply by 10^2 for ease of interpretation
CRYPTO_MINING	The relative frequency with which keywords capture mining topic (see Table A.2) in Item 1 "Business" of a 10-K filling. For topic exposure, we count only **topic keywords** appear in the sentence triples around cryptocurrency keywords and divide by the total number of words in Item 1 "Business" in year t. We multiply by 10^2 for ease of interpretation

TABLE A.4 (continued from previous page)

Variable	Definition
CRYPTO_INVESTMENTS	The relative frequency with which keywords capture investments topic (see Table A.2) in Item 1 "Business" of a 10-K filling. For topic exposure, we count only **topic keywords** appear in the sentence triples around cryptocurrency keywords and divide by the total number of words in Item 1 "Business" in year t. We multiply by 10^2 for ease of interpretation
Cryptocurrency risk topic exposure	
CRYPTO_CYBER	The relative frequency with which keywords capture cybersecurity risk topic (see Table A.3) in Item 1A "Risk Factors" of a 10-K filling. For topic exposure, we count only **topic keywords** that appear in the sentence triples around cryptocurrency keywords and divide by the total number of words in Item 1A "Risk Factors" in year t. We multiply by 10^2 for ease of interpretation
CRYPTO_REG	The relative frequency with which keywords capture regulation risk topic (see Table A.3) in Item 1A "Risk Factors" of a 10-K filling. For topic exposure, we count only **topic keywords** appear in the sentence triples around cryptocurency keywords and divide by the total number of words in Item 1A "Risk Factors" in year t. We multiply by 10^2 for ease of interpretation
CRYPTO_OPERATION	The relative frequency with which keywords capture business operations risk topic (see Table A.3) in Item 1A "Risk Factors" of a 10-K filling. For topic exposure, we count only **topic keywords** appear in the sentence triples around cryptocurrency keywords and divide by the total number of words in Item 1A "Risk Factors" in year t. We multiply by 10^2 for ease of interpretation
CRYPTO_MARKET	The relative frequency with which keywords capture market risk topic (see Table A.3) in Item 1A "Risk Factors" of a 10-K filling. For topic exposure, we count only **topic keywords** appear in the sentence triples around cryptocurency keywords and divide by the total number of words in Item 1A "Risk Factors" in year t. We multiply by 10^2 for ease of interpretation
CRYPTO_PEERS	The relative frequency with which keywords capture peers risk topic (see Table A.3) in Item 1A "Risk Factors" of a 10-K filling. For topic exposure, we count only **topic keywords** appear in the sentence triples around cryptocurency keywords and divide by the total number of words in Item 1A "Risk Factors" in year t. We multiply by 10^2 for ease of interpretation
Other variables	
CRYPTO_HOLDING	Indicator variable that equals one if a firm holds cryptocurrency on its balance sheet
COIN_DOWN	Indicator variable that equals one if the ratio of changes in bitcoin price from year t to year $t-1$ to price in year $t-1$ is negative. Bitcoin USD (BTC-USD) price quote is collected from Yahoo finance (See https://finance.yahoo.com)
DELOITTE_GUIDANCE	The natural logarithm of pages in guidance for Deloitte's clients which has a fiscal-year end after September 7, 2018 and zero otherwise
EY_GUIDANCE	The natural logarithm of pages in guidance for Ernst & Young's clients, which has a fiscal-year end after August 31, 2018 and zero otherwise

TABLE A.4 (continued from previous page)

Variable	Definition
KPMG_GUIDANCE	The natural logarithm of pages in guidance for KPMG's clients which has a fiscal-year end between November 11, 2018 and April 30, 2019 or after April 30, 2019; and zero otherwise
PWC_GUIDANCE	The natural logarithm of pages in guidance for PwC's clients which has a fiscal-year end between September 9, 2018 and December 31, 2019 or after December 31, 2019; and zero otherwise
Control variables	
BIG4	Indicator variable that equals one if the auditor is a Big4 auditor in year t, and zero otherwise
BTM	Book value of equity divided by market value of equity (CEQ/(PRCC_F*CSHO) in year t
CFO	The ratio of cash flows from operation to total assets in year t (OANCF/AT) in year t
GROWTH	The percentage of changes in sales from the current year to last year $((SALE_t - SALE_{t-1})/SALE_{t-1})$
LEV	The ratio of total debts to total assets in year t $(DLTT+DLC)/AT$
LOSS	Indicator variable that equals one if income before extraordinary items is less than zero in year t, and zero otherwise
BUSSEG	The number of business segments
GEOSEG	The number of geographic segments
RESTRUCT	Indicator variable that equals one if the company is undergoing restructuring, as indicated by the disclosure of restructuring costs (RCA, RCP, RCEPS, RCD) in year t, and zero otherwise
ROA	The ratio of net income to average total assets $(NI_t/(0.5-(AT_t+AT_{t-1})))$
SIZE	The natural logarithm of total assets (AT) in year t

References

Acemoglu, D., Autor, D., Hazell, J. and Restrepo, P. (2020), Ai and jobs: Evidence from online vacancies, Technical report, National Bureau of Economic Research.

Acemoglu, D. and Restrepo, P. (2020), 'Robots and jobs: Evidence from us labor markets', *Journal of Political Economy* **128**(6), 2188–2244.

Anderson, C. M., Fang, V. W., Moon, J. and Shipman, J. E. (2022), 'Accounting for cryptocurrencies', *Available at SSRN 4294133* .

Athey, S., Parashkevov, I., Sarukkai, V. and Xia, J. (2016), 'Bitcoin pricing, adoption, and usage: Theory and evidence'.

Bae, J., Yu Hung, C. and Van Lent, L. (2023), 'Mobilizing Text As Data', *European Accounting Review* pp. 1–22.
URL: *https://www.tandfonline.com/doi/full/10.1080/09638180.2023.2218423*

Barth, M. E. (2022), 'Accounting standards: the 'too difficult' box – the next big accounting issue?', *Accounting and Business Research* **52**(5), 565–577.
URL: *https://www.tandfonline.com/doi/full/10.1080/00014788.2022.2079757*

Bell, T. B., Landsman, W. R. and Shackelford, D. A. (2001), 'Auditors' perceived business risk and audit fees: Analysis and evidence', *Journal of Accounting Research* **39**(1), 35–43.
URL: *http://www.jstor.org/stable/2672944*

Benoit, K., Watanabe, K., Wang, H., Nulty, P., Obeng, A., Müller, S. and Matsuo, A. (2018), 'quanteda: An r package for the quantitative analysis of textual data', *Journal of Open Source Software* **3**(30), 774–774.

Biais, B., Bisiere, C., Bouvard, M., Casamatta, C. and Menkveld, A. J. (2020), 'Equilibrium bitcoin pricing', *Available at SSRN 3261063* .

Bourveau, T., Brendel, J. and Schoenfeld, J. (2023), 'Decentralized finance (DeFi) assurance: Audit adoption and capital markets effects', *Available at SSRN 4457936* .

Burke, J., Hoitash, R., Hoitash, U. and Xiao, S. X. (2022), 'The disclosure and consequences of US critical audit matters', *The Accounting Review* .

Carson, E., Fargher, N. L., Geiger, M. A., Lennox, C. S., Raghunandan, K. and Willekens, M. (2013), 'Audit reporting for going-concern uncertainty: A research synthesis', *Auditing: A Journal of Practice & Theory* **32**(Supplement 1), 353–384.

Cassell, C. A., Drake, M. S. and Dyer, T. A. (2018), 'Auditor litigation risk and the number of institutional investors', *Auditing: A Journal of Practice & Theory* **37**(3), 71–90.

Cheng, A., Davis, Y., Huang, H. H. and Ma, Y. (2022), 'Cryptoassets and auditing: Consequences of new assets', *Available at SSRN 4277644* .

Chod, J., Trichakis, N., Tsoukalas, G., Aspegren, H. and Weber, M. (2020), 'On the financing benefits of supply chain transparency and blockchain adoption', *Management Science* **66**(10), 4378–4396.

Chy, M. and Hope, O.-K. (2021), 'Real effects of auditor conservatism', *Review of Accounting Studies* **26**(2), 730–771.

Cohen, L., Malloy, C. and Nguyen, Q. (2020), 'Lazy prices', *The Journal of Finance* **75**(3), 1371–1415.

Commerford, B. P., Dennis, S. A., Joe, J. R. and Ulla, J. W. (2022), 'Man Versus Machine: Complex Estimates and Auditor Reliance on Artificial Intelligence', *Journal of Accounting Research* **60**(1), 171–201.
URL: *https://onlinelibrary.wiley.com/doi/10.1111/1475-679X.12407*

Cong, L., Li, Y. and Wang, N. (2019), 'Tokenomics: Dynamic adoption and valuation (working paper no. 63)', *Columbia Business School Research Paper* .

DeAngelo, L. E. (1981), 'Auditor size and audit quality', *Journal of accounting and economics* **3**(3), 183–199.

Defond, M. L., Francis, J. R. and Hallman, N. J. (2018), 'Awareness of SEC enforcement and auditor reporting decisions', *Contemporary Accounting Research* **35**(1), 277–313.

DeFond, M. L., Raghunandan, K. and Subramanyam, K. R. (2002), 'Do non–audit service fees impair auditor independence? Evidence from going concern audit opinions', *Journal of accounting research* **40**(4), 1247–1274.

DeFond, M. and Zhang, J. (2014), 'A review of archival auditing research', *Journal of Accounting and Economics* **58**(2-3), 275–326.

Downar, B., Ernstberger, J., Koch, C. and Prott, M. (2021), 'Does practitioner research help auditors to provide higher audit quality and improve their reputation?', *European Accounting Review* **31**(5), 1059–1088.

Duggan, W. (2022), 'The history of bitcoin, the first cryptocurrency', *US News* **August 31**.
URL: *https://money.usnews.com/investing/articles/the-history-of-bitcoin*

Eric Minuskin (2022), 'EY launches second generation of EY blockchain analyzer: Smart contract and token review on Ethereum'. URL: https://www.ey.com/en_sy/news/2022/05/ey-launches-second-generation-of-ey-blockchain-analyzer-smart-contract-and-token-review-on-ethereum. Last accessed on 2022-11-25.

Ernst & Young (2019), 'Blockchain solutions'. https://www.ey.com/en_gl/blockchain-platforms, Last accessed on 2022-10-01.

Fedyk, A., Hodson, J., Khimich, N. and Fedyk, T. (2022), 'Is artificial intelligence improving the audit process?', *Review of Accounting Studies* **27**(3), 938–985.
URL: *https://link.springer.com/10.1007/s11142-022-09697-x*

Florackis, C., Louca, C., Michaely, R. and Weber, M. (2022), 'Cybersecurity Risk', *The Review of Financial Studies* .
URL: *https://doi.org/10.1093/rfs/hhac024*

Foley, S., Karlsen, J. R. and Putniņš, T. J. (2019), 'Sex, drugs, and bitcoin: How much illegal activity is financed through cryptocurrencies?', *The Review of Financial Studies* **32**(5), 1798–1853.

Frey, E., Adams, G. S., Pfeffer, J. and Belmi, P. (2023), 'What we (do not) know about punishment across organizational boundaries', *Journal of Management* **49**(1), 196–236.

Guo, F., Lin, C., Masli, A. and Wilkins, M. S. (2021), 'Auditor responses to shareholder activism', *Contemporary Accounting Research* **38**(1), 63–95.

Hassan, T. A., Hollander, S., van Lent, L., Schwedeler, M. and Tahoun, A. (2023), 'Firm-Level Exposure to Epidemic Diseases: COVID-19, SARS, and H1N1', *The Review of Financial Studies* p. hhad044.
URL: *https://doi.org/10.1093/rfs/hhad044*

Hassan, T. A., Hollander, S., Van Lent, L. and Tahoun, A. (2019), 'Firm-level political risk: Measurement and effects', *The Quarterly Journal of Economics* **134**(4), 2135–2202.

Hay, D. C., Knechel, W. R. and Wong, N. (2006), 'Audit fees: A meta-analysis of the effect of supply and demand attributes', *Contemporary Accounting Research* **23**(1), 141–191.

Hershbein, B. and Kahn, L. B. (2018), 'Do recessions accelerate routine-biased technological change? evidence from vacancy postings', *American Economic Review* **108**(7), 1737–72.

Hester, M. (2022), 'Response to Staff Accounting Bulletin No.121', *SEC* **March 31**.
URL: *https://www.sec.gov/news/statement/peirce-response-sab-121-033122*

Hombach, K. and Sellhorn, T. (2022), 'Does every accounting issue need a solution?', *Accounting and Business Research* **52**(5), 540–561.

Hu, N., Xu, J. and Xue, S. (2022), 'Regulatory risk and auditors' reporting conservatism: Evidence from Chinese comment letters', *Journal of Accounting and Public Policy* **41**(6), 106997.

Jermann, U. J. (2018), 'Bitcoin and cagan's model of hyperinflation', *Available at SSRN 3132050* .

Jiang, W., Tang, Y., Xiao, R. J. and Yao, V. (2021), Surviving the fintech disruption, Technical report, National Bureau of Economic Research.

Kachelmeier, S. J., Rimkus, D., Schmidt, J. J. and Valentine, K. (2020), 'The Forewarning Effect of Critical Audit Matter Disclosures Involving Measurement Uncertainty*', *Contemporary Accounting Research* **37**(4), 2186–2212.
URL: *https://onlinelibrary.wiley.com/doi/10.1111/1911-3846.12583*

Knechel, W. R. (2013), 'Do auditing standards matter?', *Current Issues in Auditing* **7**(2), A1–A16.

Knechel, W. R. (2016), 'Audit quality and regulation', *International Journal of Auditing* **20**(3), 215–223.

Knechel, W. R. (2021), 'The future of assurance in capital markets: Reclaiming the economic imperative of the auditing profession', *Accounting Horizons* **35**(1), 133–151.

Knechel, W. R., Maex, S. and Park, H. J. (2023), 'Decentralized Finance (DeFi) and Cybersecurity Assurance', *Working paper* .

Knechel, W. R. and Payne, J. L. (2001), 'Additional Evidence on Audit Report Lag', *AUDITING: A Journal of Practice & Theory* **20**(1), 137–146.
URL: *https://publications.aaahq.org/ajpt/article/20/1/137/5495/Additional-Evidence-on-Audit-Report-Lag*

KPMG (2020), 'KPMG chain fusion'. URL: https://audit.kpmg.us/kpmg-chain-fusion.html. Last accessed on 2022-11-25.

Law, K. and Shen, M. (2020), 'How Does Artificial Intelligence Shape Audit Firms?'.
URL: *https://papers.ssrn.com/abstract=3718343*

Le, P. (2021), 'Letter to FASB technical director'.
URL: *https://www.microstrategy.com/content/dam/website-assets/collateral/bitcoin-downloads/microstrategy-FASB-ITC-response-letter_09-15-2021.pdf*

Lennox, C. S. and Kausar, A. (2017), 'Estimation risk and auditor conservatism', *Review of Accounting Studies* **22**(1), 185–216.

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.

Liu, Y. and Tsyvinski, A. (2021), 'Risks and returns of cryptocurrency', *The Review of Financial Studies* **34**(6), 2689–2727.

Lu, T. and Sapra, H. (2009), 'Auditor conservatism and investment efficiency', *The Accounting Review* **84**(6), 1933–1958.

Lugo, D. (2022), 'Accounting rules will be developed for crypto assets, FASB says'.
URL: *https://tax.thomsonreuters.com/news/accounting-rules-will-be-developed-for-crypto-assets-fasb-says/*

Luo, M. and Yu, S. (2022), 'Financial reporting for cryptocurrency', *Review of Accounting Studies* pp. 1–34.

Manning, L. (2021), 'FASB flooded with emails as bitcoin community demands change', https://www.nasdaq.com/articles/fasb-flooded-with-emails-as-bitcoin-community-demands-change-2021-10-07.

Minutti-Meza, M. (2021), 'The art of conversation: the expanded audit report', *Accounting and Business Research* **51**(5), 548–581.
URL: *https://www.tandfonline.com/doi/full/10.1080/00014788.2021.1932264*

Nakamoto, S. and Bitcoin, A. (2008), 'A peer-to-peer electronic cash system', *Bitcoin.–URL: https://bitcoin. org/bitcoin. pdf* **4**.

Ng, T. B.-P. and Tan, H.-T. (2003), 'Effects of authoritative guidance availability and audit committee effectiveness on auditors' judgments in an auditor-client negotiation context', *The Accounting Review* **78**(3), 801–818.

Pagnotta, E. and Buraschi, A. (2018), 'An equilibrium valuation of bitcoin and decentralized network assets', *Available at SSRN 3142022* .

PCAOB (2015), 'AU Section 150 - Generally Accepted Auditing Standards — pcaobus.org', https://pcaobus.org/oversight/standards/archived-standards/pre-reorganized-auditing-standards-interpretations/details/AU150. [Accessed 05-Feb-2023].

PCAOB (2020), 'Audits involving cryptoassets information for auditors and audit committees spotlight', https://pcaobus.org/Documents/Audits-Involving-Cryptoassets-Spotlight.pdf.

PWC (2019), 'Supporting the auditing of cryptocurrency'. URL: https://www.pwc.com/gx/en/services/audit-assurance/publications/halo-solution-for-cryptocurrency.html. Last accessed on 2022-10-01.

Santos, F. M. and Eisenhardt, K. M. (2005), 'Organizational boundaries and theories of organization', *Organization science* **16**(5), 491–508.

Sautner, Z., Van Lent, L., Vilkov, G. and Zhang, R. (2023), 'Firm-level climate change exposure', *The Journal of Finance* **78**(3), 1449–1498.

Schilling, L. and Uhlig, H. (2019), 'Some simple bitcoin economics', *Journal of Monetary Economics* **106**, 16–26.

Schipper, K. (2022), 'Why do accounting issues end up in the 'too difficult'box?', *Accounting and Business Research* **52**(5), 482–506.

SEC (2011), 'Securities and Exchange Commission (SEC), How to read a 10-K?', https://www.sec.gov/files/reada10k.pdf. [Accessed 28-Jan-2023].

Simunic, D. A. (1980), 'The pricing of audit services: Theory and evidence', *Journal of accounting research* pp. 161–190.

Sockin, M. and Xiong, W. (2020), A model of cryptocurrencies, Technical report, National Bureau of Economic Research.

Stanley, J. D. (2011), 'Is the audit fee disclosure a leading indicator of clients' business risk?', *Auditing: A Journal of Practice & Theory* **30**(3), 157–179.

Vincent, N. E. and Wilkins, A. M. (2020), 'Challenges when auditing cryptocurrencies', *Current Issues in Auditing* **14**(1), A46–A58.

World Bank Group (2020), 'Smart contract technology and financial inclusion'.

Yermack, D. (2017), 'Corporate governance and blockchains', *Review of Finance* **21**(1), 7–31.

FIGURES AND TABLES

(a) Cryptocurrency Market Capitalization

(b) Bitcoin Market Capitalization

(c) Ethereum Market Capitalization

Figure 1: Cryptocurrency Market Capitalization

Source: COINMARKETCAP.COM

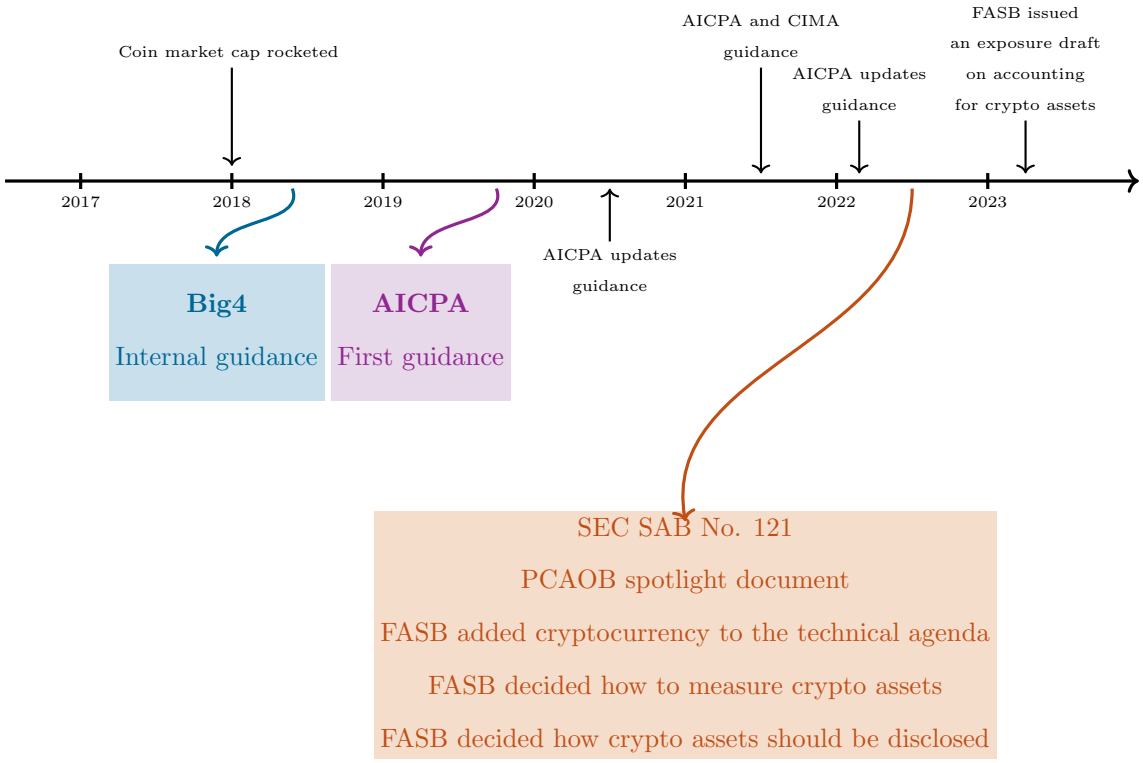
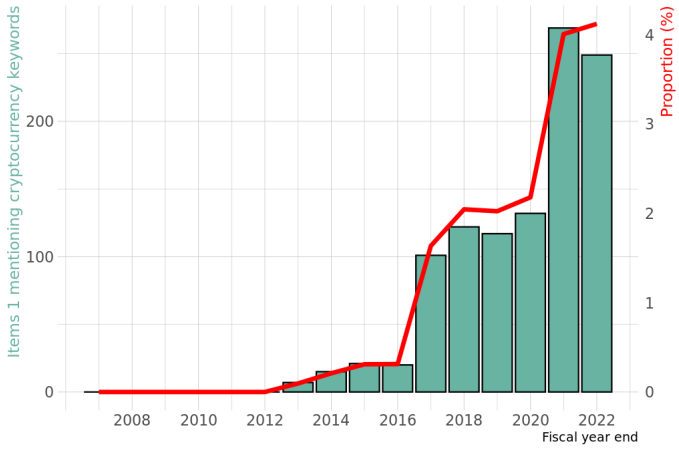


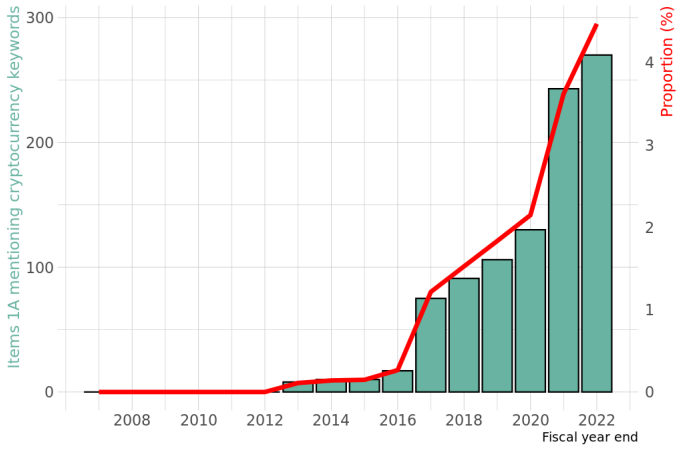
FIGURE 2: TIMELINE OF NON-AUTHORITATIVE GUIDANCE ON ACCOUNTING AND AUDITING FOR CRYPTOCURRENCY

- **December 2019**: The American Institute of Certified Public Accountants (AICPA) first published non-authoritative guidance on accounting for digital assets. The guidance is based on existing professional literature and the experience of members of the AICPA's Digital Assets Working Group and AICPA staff and is specific to U.S. generally accepted auditing standards (GAAP).
- **July 2020**: The AICPA added non-authoritative guidance on auditing digital assets. This practice aid provides auditors with information to consider when accepting or continuing audit engagements that involve digital assets.
- **May 2021**: The AICPA and the Chartered Institute of Management Accountants (CIMA) jointly released guidance for auditing and accounting for the risks of digital assets such as cryptocurrency with the new information on audit risk assessment. It also has a section discussing laws and regulations, along with related-party transactions. It describes the particular challenges and potential procedures that auditors should consider complying with laws and regulations, along with the identification, accounting and disclosure of related parties in an audit of an entity that holds or transacts with digital assets.
- **January 2022**: the AICPA updated its non-authoritative guidance on best practices for accounting for digital assets, the "Accounting for and auditing of digital assets practice aid." The latest edition includes non-authoritative guidance on crypto asset lending and borrowing, derivatives and mining. Some topics include evaluating whether a contract contains a derivative or an embedded derivative, how lenders should account for the crypto assets they have loaned, and how a borrower accounts for crypto assets borrowed.
- **March 2022**: The SEC staff released Staff Accounting Bulletin No. 121 (SAB No. 121), which expresses the staff's views on how an entity that has an obligation to safeguard "crypto-assets" for another party should account for that obligation.

- **May 2022**: The Public Company Accounting Oversight Board (PCAOB) released a document with information for auditors and audit committees about audits involving crypto assets, such as Bitcoin and other digital currencies. The Spotlight document "Audits Involving Cryptoassets - Information for Auditors and Audit Committees" calls 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. The PCAOB's staff has noticed that cryptocurrencies such as Bitcoin have recently started to be recorded and disclosed in the financial statements of companies, broker-dealers and other issuers. When doing inspections of auditors of some smaller issuers, the PCAOB's staff has seen situations where transactions involving crypto assets were material to the financial statements.
- **May 2022**: The Financial Accounting Standards Board (FASB) on May 11, 2022, unanimously voted to add a project to its technical agenda to develop recognition, measurement, presentation, and disclosure guidance for cryptocurrencies, a subset of digital assets. The topic has become sufficiently prevalent to warrant accounting rules that reflect the underlying economics of those types of assets.
- **June 2022**: The AICPA has published a set of questions and answers that explain recently released SEC staff guidance regarding the accounting for entities that have obligations to safeguard crypto assets held for their platform users.
- **August 2022**: The FASB, at its August 31 meeting, decided to narrow the proposed scope of its digital assets project that formally launched in May to focus specifically on cryptocurrencies.
- **October 2022**: The FASB decided to require all entities, public and private, with investments in in-scope crypto assets to measure those assets at fair value, with gains and losses recorded in the current period comprehensive income unless other industry-specific US GAAP applies to those costs.
- **December 14, 2022**: The FASB decided how crypto assets would be presented in the financial statements and what disclosures would be required.
- **February 1, 2023**: The FASB decided to issue an exposure draft of a new crypto asset accounting standard with a 75-day public comment period. In addition, the Board reached decisions about transition, effective dates and refinements to the scope initially established in August 2022.



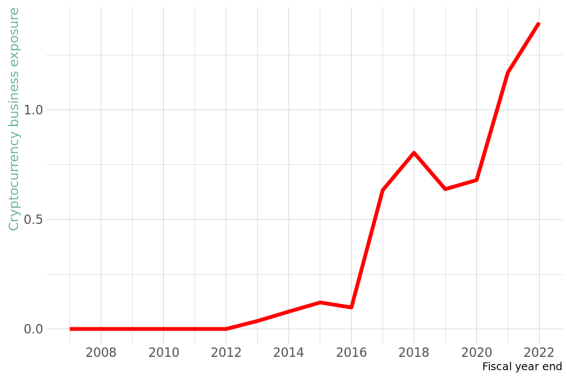
(A) Items 1



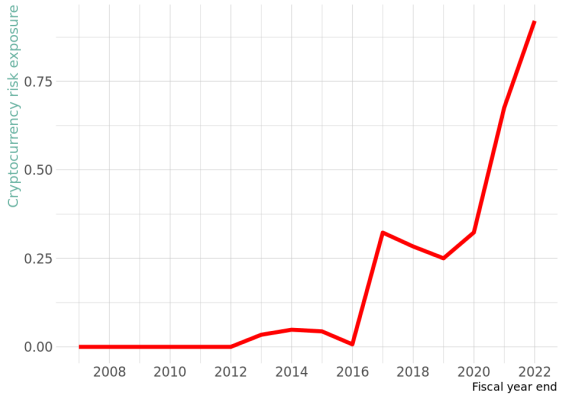
(B) Items 1A

Figure 3: Items 1 and 1A mentioning cryptocurrency keywords by years

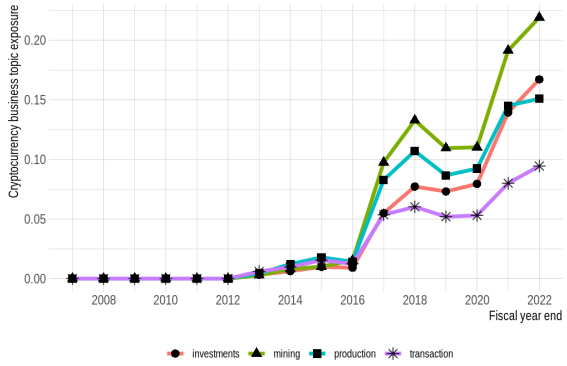
These figures provide the distribution of Items 1 and 1A mentioning cryptocurrency keywords. The bars indicate the number of items, and the red line indicates the proportion of items over the fiscal year 2008 to 2022. See the list of cryptocurrency keywords in Table A.1 and the distribution by years in Table IA.6.



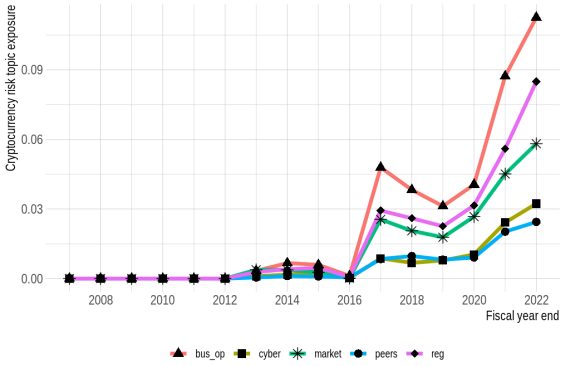
(A) Business exposure



(B) Risk exposure



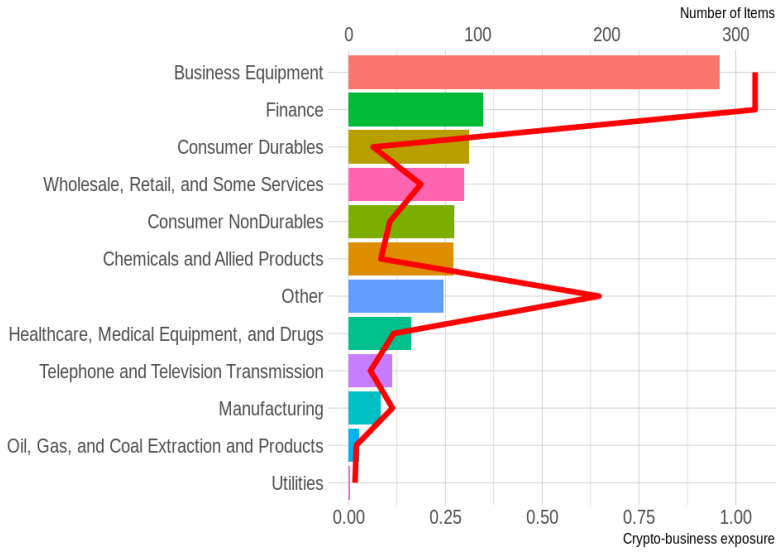
(C) Business topic exposure



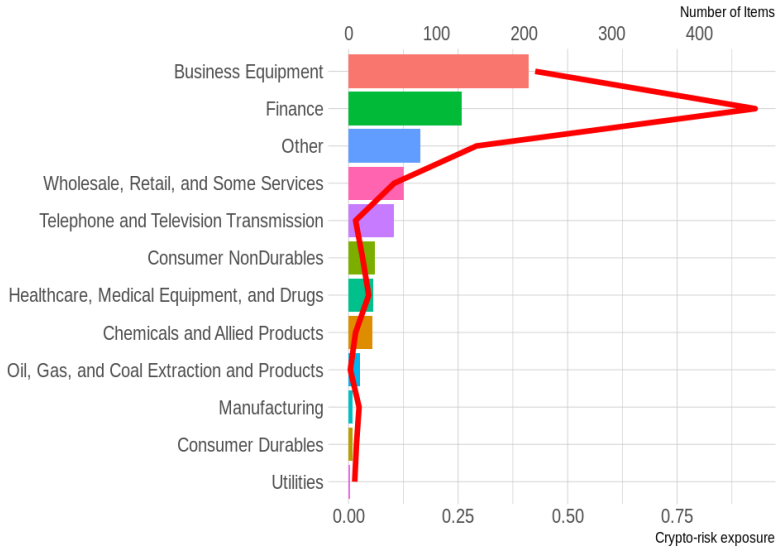
(D) Risk topic exposure

Figure 4: Cryptocurrency exposure by years

These figures plot the yearly average of crypto exposure (*CRYPTO_BUS_EXPOSURE* and *CRYPTO_RISK_EXPOSURE*) and crypto topic exposure from fiscal year 2008 to 2022. Panel A and Panel B depict the trend of crypto exposure over time. In Panel C, four topics related to the cryptocurrency business, as measured by Item 1, are plotted, while Panel D illustrates five topics associated with cryptocurrency risk, measured by Item 1A. See the list of cryptocurrency keywords in Table A.1, the list of business topics in Table A.2, risk topics in Table A.3, and the definition of variables in Table A.4.



(A) Business exposure



(B) Risk exposure

Figure 5: Cryptocurrency exposure by industries

These figures plot the average of *CRYPTO_BUS_EXPOSURE* in Panel A and *CRYPTO_RISK_EXPOSURE* in Panel B. The bars indicate the average cryptocurrency exposures and the red lines indicate the number of Items 1/1A discussing cryptocurrency by sectors. See the list of cryptocurrency keywords in Table A.1 and the definition of variables in Table A.4.

Table 1: Audit procedures and financial statement assertions

Assertions	Audit procedures performed
Existence or occurrence	- Obtained confirmation of the company's digital assets in custody - Evaluated certain internal controls over the digital assets process performed at the custodial locations, related specifically to the generation of the private cryptographic keys, the storing of these keys - Performed a site visitation of the facility where the company's mining hardware is located (observation of the physical and environmental controls and mining equipment inventory) - Evaluated certain internal controls over the digital assets process performed at the custodial locations, related specifically to the generation of the private cryptographic keys, the storing of these keys
Completeness	- Compared the company's record of digital asset transactions to the records on the public blockchain and digital assets in custody - Evaluated the design and tested the operating effectiveness of certain internal controls over the digital assets process, including a control over the comparison of the company's records of digital assets held to the custodial records
Valuation or allocation	- Examined management's processes for determining the amount of impairment expense recognized - Examined supporting sale and cash receipt evidence for cryptocurrency sales, including management's processes for calculating any gains on sales of cryptocurrencies - Assessed the total hash power contributed onto the network by the company against total block rewards and transaction fees issued over the year - Evaluated certain internal controls over the digital assets process performed at the custodial locations, related specifically to the reconciliation of digital assets per the custodial service ledgers to the public blockchain - Tested supporting documentation for the valuation of cryptocurrency awards earned - Evaluated the provisions of the contract between the company and the pool - Developed an independent range of possible valuations for the equity instruments issued based on third-party data and independently developed assumptions of the company's risk-free rate, holding period, and volatility - Reviewed and tested underlying agreements giving rise to the receipt of crypto assets - Agreed the fair values of the crypto assets at the transaction date and year-end date to an independent third-party source - Confirmed that only the cryptocurrencies traded on an active market have been measured at fair value - Performed a post-year-end review to identify transactions that support the realization of the year-end carrying value
Rights and obligations	- Independently and directly confirmed the balance and ownership of digital currency that is in the custody of a third party
Presentation and disclosure	- Examined management's processes for the inclusion of digital currency as a current asset on the balance sheet and accompanying footnote disclosures

This table shows the financial statement assertions according to AS 15 - *Audit evidence* and the extant audit procedures carried out by auditors in engagements involving cryptocurrency. We collected a universal database of CAMs in Audit Analytics covering the period from June 30, 2019 to January 1, 2023 and manually read the content of CAMs crypto-related engagements. Out of a total of 5688 unique clients (19,252 CAMs), there are 24 clients (45 CAMs) mentioned cryptocurrency as a CAM in their audit reports. A limited number of audit engagements in our sample have been subjected to the requirements of CAMs. This is because the regulation requiring auditors to communicate CAMs in their reports was effective recently in 2019.

Table 2: Summary Statistics

Variable	N	Mean	Std. Dev.	Min	Pctl. 25	Pctl. 75	Max
LNAUFEES	33000	-0.118	1.423	-3.507	-1.122	0.866	3.105
AUFEES	33000	2.183	3.537	0.030	0.326	2.378	22.314
GCO	33000	0.0831	0.276	0.000	0.000	0.000	1.000
AUDITLAG	33000	66.385	19.019	34.000	55.000	75.000	156.000
N_CAM	7718	1.438	0.662	1	1.000	2.000	6
CAMCRYPTO	7718	0.00136	0.0356	0.000	0.000	0.000	1.000
CRYPTO_BUS_EXPOSURE	33000	0.234	6.314	0.000	0.000	0.000	441.640
CRYPTO_RISK_EXPOSURE	33000	0.170	4.094	0.000	0.000	0.000	220.557
CRYPTO_PRODUCTION	33000	0.0272	0.525	0.000	0.000	0.000	26.190
CRYPTO_TRANSACTION	33000	0.0171	0.547	0.000	0.000	0.000	40.698
CRYPTO_MINING	33000	0.0377	0.992	0.000	0.000	0.000	65.854
CRYPTO_INVESTMENTS	33000	0.025	0.583	0.000	0.000	0.000	35.135
CRYPTO_CYBER	33000	0.00502	0.127	0.000	0.000	0.000	8.096
CRYPTO_REG	33000	0.0153	0.333	0.000	0.000	0.000	16.754
CRYPTO_OPERATION	33000	0.0223	0.556	0.000	0.000	0.000	31.390
CRYPTO_MARKET	33000	0.0127	0.279	0.000	0.000	0.000	14.236
CRYPTO_PEERS	33000	0.00568	0.111	0.000	0.000	0.000	6.338
SIZE	33000	6.483	2.582	-1.011	4.945	8.230	11.830
LEV	33000	0.329	0.503	0.000	0.0554	0.429	4.001
CFO	33000	-0.0349	0.369	-2.424	-0.000062	0.103	0.365
ROA	33000	-0.148	0.651	-4.754	-0.062	0.056	0.360
BUSSEG	33000	0.213	0.836	-0.791	-0.0338	0.195	6.125
GEOSEG	33000	0.418	1.039	-6.903	0.171	0.757	4.288
GROWTH	33000	0.363	0.481	0	0.000	1.000	1
BTM	33000	0.282	0.450	0	0.000	1.000	1
LOSS	33000	215.364	772.125	-679.465	-7.160	111.912	5158.950
RESTRUCT	33000	404.697	1202.140	-220.687	-0.00225	235.619	8156.554
BIG4	33000	0.597	0.491	0.000	0.000	1.000	1.000
N_CLIENTS_CRYPTO_BUS_EXPOSURE	6621	0.0483	0.280	0.000	0.000	0.000	6.000
N_CLIENTS_CRYPTO_RISK_EXPOSURE	6621	0.0739	0.377	0.000	0.000	0.000	7.000
LN_CLIENTS_CRYPTO_BUS_EXPOSURE	6621	0.0301	0.157	0.000	0.000	0.000	1.946
LN_CLIENTS_CRYPTO_RISK_EXPOSURE	6621	0.044	0.195	0.000	0.000	0.000	2.079
N_JOB_POSTINGS	6621	0.845	4.345	0.000	0.000	0.000	96.000
LN_JOB_POSTINGS	6621	0.191	0.605	0.000	0.000	0.000	4.575

This table reports the summary statistics of cryptocurrency exposure variables from Item 1 "Business" ($CRYPTO\_BUS\_EXPOSURE$) and Item 1A "Risk Factors" ($CRYPTO\_RISK\_EXPOSURE$) of 10-K fillings, cryptocurrency topic exposure variables, and auditor responses variables. All variables are described in Table A.4. All financial variables are winsorized at 1% and 99% levels, except cryptocurrency exposure variables and the percentage of critical audit matters mentioning cryptocurrency-related keywords ($CAMCRYPTO$).

Table 3: Correlation table of cryptocurrency exposure variables

	A	B	C	D	E	F	G	H	I	J	K
A: CRYPTO_BUS_EXPOSURE		**0.89**	**0.82**	**0.86**	**0.94**	**0.86**	**0.76**	**0.80**	**0.92**	**0.85**	**0.73**
B: CRYPTO_RISK_EXPOSURE	**0.34**		**0.77**	**0.76**	**0.87**	**0.82**	**0.90**	**0.91**	**0.97**	**0.94**	**0.74**
C: CRYPTO_PRODUCTION	**0.96**	**0.36**		**0.73**	**0.86**	**0.86**	**0.72**	**0.78**	**0.78**	**0.79**	**0.74**
D: CRYPTO_TRANSACTION	**0.68**	**0.31**	**0.68**		**0.88**	**0.86**	**0.58**	**0.79**	**0.77**	**0.73**	**0.59**
E: CRYPTO_MINING	**0.89**	**0.32**	**0.88**	**0.60**		**0.91**	**0.74**	**0.84**	**0.89**	**0.83**	**0.77**
F: CRYPTO_INVESTMENTS	**0.86**	**0.37**	**0.84**	**0.69**	**0.78**		**0.75**	**0.87**	**0.79**	**0.79**	**0.66**
G: CRYPTO_CYBER	**0.42**	**0.50**	**0.45**	**0.46**	**0.37**	**0.48**		**0.82**	**0.85**	**0.84**	**0.64**
H: CRYPTO_REG	**0.40**	**0.72**	**0.41**	**0.37**	**0.37**	**0.44**	**0.57**		**0.86**	**0.87**	**0.63**
I: CRYPTO_OPERATION	**0.39**	**0.86**	**0.40**	**0.35**	**0.36**	**0.42**	**0.55**	**0.70**		**0.93**	**0.77**
J: CRYPTO_MARKET	**0.39**	**0.63**	**0.41**	**0.40**	**0.36**	**0.42**	**0.57**	**0.60**	**0.61**		**0.77**
K: CRYPTO_PEERS	**0.29**	**0.77**	**0.31**	**0.30**	**0.29**	**0.32**	**0.46**	**0.58**	**0.74**	**0.49**	

This table reports Pearson correlations above and Spearman correlations below the diagonal of cryptocurrency exposure and cryptocurrency topic exposure variables. The number of observations is 33,000. Correlations with significance levels below 5% appear in bold print. Refer to Table A.4 for variable definitions.

Table 4: Correlation table of variables in audit fees, going-concern, audit reporting lag models

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
A: LNAUFEES		**-0.03**	**-0.02**	**0.82**	**-0.12**	**0.37**	**0.37**	**-0.11**	**0.06**	**-0.28**	**0.40**	**0.30**	**0.34**	**-0.38**	**0.73**	**-0.61**
B: CRYPTO_BUS_EXPOSURE	-0.01		**0.89**	**-0.04**	0.01	**-0.04**	**-0.05**	**0.04**	-0.01	**0.04**	**-0.01**	-0.01	**-0.02**	**0.05**	**-0.03**	**0.04**
C: CRYPTO_RISK_EXPOSURE	**0.05**	**0.34**		**-0.03**	-0.00	**-0.03**	**-0.04**	**0.04**	-0.00	**0.04**	**-0.01**	-0.00	**-0.01**	**0.04**	**-0.03**	**0.04**
D: SIZE	**0.79**	**-0.02**	**0.07**		**-0.23**	**0.52**	**0.52**	**-0.13**	**0.21**	**-0.48**	**0.25**	**0.28**	**0.19**	**-0.52**	**0.58**	**-0.66**
E: LEV	**0.24**	-0.01	**-0.04**	**0.20**		**-0.47**	**-0.54**	**0.02**	**-0.47**	**0.18**	**-0.01**	**-0.04**	**-0.09**	**0.42**	**-0.06**	**0.21**
F: CFO	**0.37**	**-0.04**	**-0.02**	**0.34**	**0.03**		**0.83**	**-0.13**	**0.25**	**-0.42**	**0.13**	**0.13**	**0.17**	**-0.59**	**0.25**	**-0.39**
G: ROA	**0.33**	**-0.04**	-0.00	**0.41**	**-0.06**	**0.72**		**-0.15**	**0.31**	**-0.43**	**0.12**	**0.13**	**0.15**	**-0.61**	**0.25**	**-0.40**
H: GROWTH	-0.00	0.01	**0.02**	0.01	**-0.03**	**0.03**	**0.10**		**-0.04**	**0.12**	**-0.10**	**-0.06**	**-0.10**	**0.12**	**-0.06**	**0.10**
I: BTM	**-0.04**	**-0.03**	-0.00	**0.18**	**-0.26**	**-0.07**	**0.03**	**-0.13**		**-0.14**	-0.00	**0.06**	**0.02**	**-0.32**	**0.01**	**-0.15**
J: LOSS	**-0.27**	**0.03**	**-0.02**	**-0.48**	**0.07**	**-0.52**	**-0.83**	**-0.08**	**-0.18**		**-0.02**	**-0.15**	**-0.08**	**0.36**	**-0.19**	**0.35**
K: RESTRUCT	**0.41**	-0.01	**-0.02**	**0.24**	**0.13**	**0.17**	**0.09**	**-0.15**	**-0.02**	**-0.02**		**0.12**	**0.30**	**-0.12**	**0.27**	**-0.23**
L: BUSSEG	**0.26**	**0.01**	**0.03**	**0.23**	**0.06**	**0.13**	**0.14**	**-0.04**	**0.08**	**-0.14**	**0.13**		**0.09**	**-0.12**	**0.16**	**-0.15**
M: GEOSEG	**0.42**	-0.01	0.01	**0.23**	**-0.02**	**0.25**	**0.21**	**-0.05**	**-0.03**	**-0.12**	**0.34**	**0.08**		**-0.15**	**0.20**	**-0.21**
N: GCO	**-0.34**	**0.06**	-0.00	**-0.41**	**0.17**	**-0.37**	**-0.40**	**-0.05**	**-0.28**	**0.36**	**-0.12**	**-0.12**	**-0.21**		**-0.28**	**0.46**
O: BIG4	**0.74**	**-0.03**	0.00	**0.58**	**0.17**	**0.31**	**0.26**	-0.00	**-0.08**	**-0.19**	**0.27**	**0.14**	**0.25**	**-0.28**		**-0.54**
P: AUDITLAG	**-0.66**	**0.03**	**-0.02**	**-0.68**	**-0.11**	**-0.42**	**-0.42**	**-0.02**	**0.04**	**0.35**	**-0.25**	**-0.14**	**-0.28**	**0.38**	**-0.58**	

This table reports Pearson correlations above and Spearman correlations below the diagonal of key variables in Equation (3) where the dependent variables are the natural logarithm of audit fees, an indicator of receiving going-concern opinions, the number of days from the end of a client's financial year and the auditor signature date. The number of observations is 33,000. Correlations with significance levels below 5% appear in bold print. Refer to Table A.4 for variable definitions. All financial variables are winsorized at 1% and 99% level, except cryptocurrency exposure variables and the percentage of critical audit matters mentioning cryptocurrency-related keywords ($CAMCRYPTO$).

Table 5: Cryptocurrency exposure and auditor responses

	LNAUFEES		AUDITLAG		GCO		CAMCRYPTO	
	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
CRYPTO_BUS_EXPOSURE	0.010**		0.205***		0.006***		0.028***	
	(2.915)		(5.412)		(15.368)		(34.523)	
CRYPTO_RISK_EXPOSURE		0.011**		0.227***		0.004***		0.028***
		(2.250)		(3.327)		(6.735)		(13.984)
SIZE	0.420***	0.420***	-3.805***	-3.806***	-0.026***	-0.026***	0.000	0.000
	(15.414)	(15.412)	(-13.538)	(-13.529)	(-6.277)	(-6.292)	(-0.568)	(-1.337)
LEV	0.056	0.056	1.458	1.465	0.044***	0.044***	0.001**	0.001***
	(1.200)	(1.203)	(1.530)	(1.539)	(5.979)	(6.014)	(2.454)	(3.263)
CFO	-0.154*	-0.153*	-0.453	-0.447	-0.145***	-0.145***	0.007	0.009
	(-1.828)	(-1.824)	(-0.211)	(-0.209)	(-7.845)	(-7.831)	(1.075)	(1.196)
ROA	-0.016	-0.016	-0.986	-0.985	-0.093***	-0.093***	-0.006	-0.008
	(-1.638)	(-1.629)	(-1.695)	(-1.698)	(-7.073)	(-7.064)	(-0.981)	(-1.116)
GROWTH	-0.010	-0.010	0.356	0.356	0.005**	0.006**	0.000	0.000
	(-0.595)	(-0.596)	(1.347)	(1.344)	(2.533)	(2.517)	(-0.713)	(0.728)
BTM	-0.055***	-0.055***	-0.307	-0.306	-0.032***	-0.032***	0.001*	0.001**
	(-7.785)	(-7.784)	(-1.234)	(-1.231)	(-5.645)	(-5.642)	(2.192)	(2.370)
LOSS	0.194***	0.194***	3.669***	3.664***	0.027**	0.027**	-0.001	-0.002
	(4.227)	(4.229)	(5.051)	(5.037)	(2.593)	(2.579)	(-1.190)	(-1.150)
RESTRUCT	0.223***	0.223***	-0.416	-0.413	0.000	0.000	0.000	0.000
	(8.658)	(8.658)	(-1.412)	(-1.401)	(0.007)	(0.014)	(-0.698)	(1.589)
BUSSEG	0.071***	0.071***	0.641***	0.641***	0.005*	0.005*	0.000	0.000
	(3.282)	(3.282)	(3.973)	(3.969)	(2.008)	(2.008)	(-1.177)	(-1.285)
GEOSEG	0.054***	0.054***	-0.128	-0.129	-0.001	-0.001	0.000	0.000
	(4.149)	(4.148)	(-1.111)	(-1.113)	(-0.873)	(-0.897)	(-1.214)	(-1.471)
BIG4	0.718***	0.718***	-7.757***	-7.753***	-0.011	-0.011	-0.001	0.000
	(4.999)	(4.999)	(-8.887)	(-8.883)	(-1.306)	(-1.303)	(-1.107)	(-0.226)
Adjusted R^2	0.84933	0.84933	0.48981	0.48984	0.44052	0.44033	0.62026	0.63520
Observations	33,000	33,000	33,000	33,000	33,000	33,000	7,718	7,718
Year fixed effects	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Industry fixed effects	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

This table reports the results from linear probability models relating auditor responses to the firm's exposure to cryptocurrency as shown in Equation (3):

$$\text{Auditor responses}_{it} = \beta_0 + \beta_1 * \text{Crypto exposure}_{it} + \beta * Z + \epsilon_{it}$$

The outcome variable is either (i) the natural logarithm of audit fees in year t ($LNAUFEES_{it}$), (ii) the number of days between a client's fiscal year-end and auditor signature date ($AUDITLAG$), (iii) an indicator variable that equals one if the auditor issues a going-concern opinion to the client in year t and zero otherwise (GCO_{it}), (iv) the percentage of critical audit matters mentioning cryptocurrency-related keywords ($CAMCRYPTO$). *Crypto exposure*$_{it}$ is our variable of interest and is defined as how frequently the cryptocurrency-related keywords appear in Item 1 "Business" ($CRYPTO\_BUS\_EXPOSURE$) and Item 1A "Risk Factors" ($CRYPTO\_RISK\_EXPOSURE$) in year t. Table A.1 defines all cryptocurrency-related keywords in detail. All financial variables are winsorized at 1% and 99% levels, except cryptocurrency exposure variables and the percentage of critical audit matters mentioning cryptocurrency-related keywords ($CAMCRYPTO$). We standardize cryptocurrency exposure variables to have standard deviations equal to one. All variables are described in Table A.4. Standard errors are clustered by Fama-French 12 industries. ***, ** and * indicate significance at the 1%, 5% and 10% levels in a two-tailed test.

Table 6: Cryptocurrency business exposure and auditor responses

	LNAUFEES				AUDITLAG			
	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
Panel A								
CRYPTO_PRODUCTION	0.012				0.315***			
	(1.711)				(6.592)			
CRYPTO_TRANSACTION		0.011***				0.093**		
		(3.667)				(2.483)		
CRYPTO_MINING			0.010**				0.223***	
			(2.365)				(5.747)	
CRYPTO_INVESTMENTS				0.012				0.181***
				(1.711)				(4.159)
Adjusted R^2	0.84935	0.84933	0.84933	0.84934	0.48997	0.48972	0.48983	0.48978
Observations	33,000	33,000	33,000	33,000	33,000	33,000	33,000	33,000
Panel B								
	GCO				CAMCRYPTO			
	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
CRYPTO_PRODUCTION	0.007***				0.023***			
	(5.069)				(4.829)			
CRYPTO_TRANSACTION		0.006***				0.024***		
		(8.169)				(26.752)		
CRYPTO_MINING			0.005***				0.027***	
			(8.999)				(14.908)	
CRYPTO_INVESTMENTS				0.006***				0.026***
				(7.224)				(8.909)
Adjusted R^2	0.44080	0.44058	0.44049	0.44058	0.41839	0.46997	0.57031	0.52255
Observations	33,000	33,000	33,000	33,000	7,718	7,718	7,718	7,718
Control variables	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Year fixed effects	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Industry fixed effects	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

This table reports the results from linear probability models relating auditor responses to the firm's topic exposure to cryptocurrency. The outcome variable is either (i) the natural logarithm of audit fees in year t ($LNAUFEES_{it}$), (ii) the number of days between a client's fiscal year-end and auditor signature date ($AUDITLAG$), (iii) an indicator variable that equals one if the auditor issues a going-concern opinion to the client in year t and zero otherwise (GCO_{it}), (iv) the percentage of critical audit matters mentioning cryptocurrency-related keywords ($CAMCRYPTO$). Our variables of interest are four topics of cryptocurrency business exposure in year t. Table A.1 defines all cryptocurrency-related keywords in detail. All financial variables are winsorized at 1% and 99% levels, except cryptocurrency exposure variables and the percentage of critical audit matters mentioning cryptocurrency-related keywords ($CAMCRYPTO$). We standardize cryptocurrency exposure variables to have standard deviations equal to one. All variables are described in Table A.4. Standard errors are clustered by Fama-French 12 industries. ***, ** and * indicate significance at the 1%, 5% and 10% levels in a two-tailed test.

Table 7: Cryptocurrency risk exposure and auditor responses

	LNAUFEES					AUDITLAG				
	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)
Panel A										
CRYPTO_CYBER	0.009					0.239***				
	(1.485)					(3.194)				
CRYPTO_REG		0.012*					0.221**			
		(1.847)					(2.384)			
CRYPTO_OPERATION			0.012**					0.206***		
			(2.772)					(3.537)		
CRYPTO_MARKET				0.012*					0.225***	
				(1.912)					(3.260)	
CRYPTO_PEERS					0.011					0.160***
					(1.499)					(7.154)
Adjusted R^2	0.84932	0.84934	0.84935	0.84935	0.84934	0.48985	0.48983	0.48981	0.48983	0.48976
Observations	33,000	33,000	33,000	33,000	33,000	33,000	33,000	33,000	33,000	33,000
Panel B										
	GCO					CAMCRYPTO				
	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)
CRYPTO_CYBER	0.002***					0.026***				
	(3.476)					(7.168)				
CRYPTO_REG		0.004***					0.027***			
		(4.547)					(6.446)			
CRYPTO_OPERATION			0.004***					0.027***		
			(5.707)					(11.072)		
CRYPTO_MARKET				0.004***					0.028***	
				(3.953)					(11.278)	
CRYPTO_PEERS					0.006***					0.022***
					(4.515)					(7.431)
Adjusted R^2	0.44017	0.44035	0.44028	0.44028	0.44055	0.52044	0.57024	0.59383	0.63282	0.39025
Observations	33,000	33,000	33,000	33,000	33,000	7,718	7,718	7,718	7,718	7,718
Control variables	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Year fixed effects	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Industry fixed effects	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

This table reports the results from linear probability models relating auditor responses to the firm's topic exposure to cryptocurrency. The outcome variable is either (i) the natural logarithm of audit fees in year t ($LNAUFEES_{it}$), (ii) the number of days between a client's fiscal year-end and auditor signature date ($AUDITLAG$), (iii) an indicator variable that equals one if the auditor issues a going-concern opinion to the client in year t and zero otherwise (GCO_{it}), (iv) the percentage of critical audit matters mentioning cryptocurrency-related keywords ($CAMCRYPTO$). Our variables of interest are five topics of cryptocurrency risk exposure in year t. Table A.1 defines all cryptocurrency-related keywords in detail. All financial variables are winsorized at 1% and 99% levels, except cryptocurrency exposure variables and the percentage of critical audit matters mentioning cryptocurrency-related keywords ($CAMCRYPTO$). We standardize cryptocurrency exposure variables to have standard deviations equal to one. All variables are described in Table A.4. Standard errors are clustered by Fama-French 12 industries. ***, ** and * indicate significance at the 1%, 5% and 10% levels in a two-tailed test.

Table 8: Number of cryptocurrency-exposed clients and audit office hiring efforts

	LN_JOB_POSTINGS	
	(1)	(2)
LN_CLIENTS_CRYPTO_BUS_EXPOSURE	0.194*	
	(1.934)	
LN_CLIENTS_CRYPTO_RISK_EXPOSURE		0.203**
		(2.171)
M_SIZE	-0.020	-0.023
	(-1.250)	(-1.395)
M_LEV	0.005	0.004
	(0.226)	(0.190)
M_CFO	0.025	0.024
	(0.936)	(0.915)
M_ROA	-0.032**	-0.029**
	(-2.378)	(-2.182)
M_BUSSEG	0.006	0.008
	(0.345)	(0.430)
M_GEOSEG	-0.008	-0.009
	(-0.680)	(-0.715)
M_GROWTH	0.021***	0.021***
	(3.117)	(3.136)
M_BTM	-0.005	-0.006
	(-0.485)	(-0.532)
M_LOSS	0.056**	0.059**
	(2.096)	(2.192)
M_RESTRUCT	-0.044	-0.045
	(-1.194)	(-1.216)
M_SOX404	0.016	0.015
	(0.467)	(0.454)
M_GCO	0.014	0.009
	(0.409)	(0.263)
M_AUDITLAG	-0.001*	-0.001*
	(-1.687)	(-1.719)
Adjusted R^2	0.00569	0.00729
Observations	6,593	6,593
Calendar year fixed effects	Yes	Yes
Audit office fixed effects	Yes	Yes

This table reports the results from linear probability models relating an auditor's crypto-related job postings to the extent of its clients' exposure to cryptocurrency. The outcome variable is the natural logarithm of crypto-related job postings in calendar year t of audit office j ($LN\_JOB\_POSTINGS_{jt}$) plus 1. The variable of interest is the natural logarithm of clients having a positive value to either $CRYPTO\_BUS\_EXPOSURE$, $CRYPTO\_RISK\_EXPOSURE$ plus 1. We also include controls for the average (mean) traits of an office's client portfolio (M_X_{jt}). All financial variables are winsorized at 1% and 99% levels. All variables are described in Table A.4. Standard errors are clustered by the audit office. ***, ** and * indicate significance at the 1%, 5% and 10% levels in a two-tailed test.

Table 9: Effect of changes in guidance on accounting for cryptocurrencies

	LNAUFEES		AUDITLAG		GCO		CAMCRYPTO	
	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
CRYPTO_BUS_EXPOSURE	0.009***		0.215***		0.006***		0.028***	
	(3.639)		(5.563)		(17.113)		(39.723)	
CRYPTO_BUS_EXPOSURE × EY_GUIDANCE	0.066***		0.456***		0.001		-0.008***	
	(3.903)		(3.173)		(0.672)		(-28.043)	
CRYPTO_BUS_EXPOSURE × PWC_GUIDANCE	0.040		0.060		0.010***		-0.009***	
	(1.000)		(0.085)		(4.246)		(-56.643)	
CRYPTO_BUS_EXPOSURE × DELOITTE_GUIDANCE	0.052		-1.488		0.019		-0.010***	
	(0.991)		(-0.446)		(0.943)		(-18.361)	
CRYPTO_BUS_EXPOSURE × KPMG_GUIDANCE	0.003		-0.179***		-0.002***		-0.001	
	(0.733)		(-6.023)		(-4.172)		(-1.165)	
CRYPTO_RISK_EXPOSURE		0.010**		0.237***		0.004***		0.030***
		(2.532)		(4.087)		(7.511)		(16.080)
CRYPTO_RISK_EXPOSURE × EY_GUIDANCE		0.073**		0.656		0.004		-0.009***
		(2.461)		(1.656)		(1.226)		(-15.671)
CRYPTO_RISK_EXPOSURE × PWC_GUIDANCE		0.046		0.498***		0.024***		-0.009***
		(0.571)		(4.504)		(7.578)		(-19.828)
CRYPTO_RISK_EXPOSURE × DELOITTE_GUIDANCE		0.001		0.149		0.002***		-0.011***
		(0.101)		(0.471)		(3.209)		(-13.791)
CRYPTO_RISK_EXPOSURE × KPMG_GUIDANCE		0.002		-0.142***		-0.002***		-0.003***
		(0.576)		(-3.790)		(-5.437)		(-5.163)
EY_GUIDANCE	-0.012**	-0.011**	-0.666***	-0.658***	-0.004	-0.004	0.000***	0.000
	(-2.705)	(-2.662)	(-5.013)	(-4.930)	(-1.576)	(-1.573)	(-5.854)	(-1.151)
PWC_GUIDANCE	0.027**	0.027**	-0.357*	-0.347*	0.001	0.001	0.000***	0.000
	(2.454)	(2.306)	(-1.911)	(-1.976)	(0.463)	(0.592)	(-6.781)	(-1.286)
DELOITTE_GUIDANCE	-0.037***	-0.038***	-0.779***	-0.724***	-0.003	-0.004	0.000***	0.000
	(-3.596)	(-3.843)	(-4.685)	(-3.158)	(-1.066)	(-1.360)	(-4.325)	(-0.358)
KPMG_GUIDANCE	-0.035***	-0.035***	-0.099	-0.097	0.000	0.000	0.000	0.000
	(-4.631)	(-4.635)	(-0.840)	(-0.826)	(-0.162)	(-0.167)	(-0.473)	(0.217)
Adjusted R^2	0.85002	0.85003	0.49047	0.49051	0.44058	0.44048	0.62238	0.65015
Observations	33,000	33,000	33,000	33,000	33,000	33,000	7,718	7,718
Year fixed effects	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Industry fixed effects	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

This table reports the results from linear probability models relating auditor responses to the firm's exposure to cryptocurrency. The outcome variable is either (i) the natural logarithm of audit fees in year t ($LNAUFEES_{it}$), (ii) the number of days between a client's fiscal year-end and auditor signature date ($AUDITLAG$), (iii) an indicator variable that equals one if the auditor issues a going-concern opinion to the client in year t and zero otherwise (GCO_{it}), (iv) the percentage of critical audit matters mentioning cryptocurrency-related keywords ($CAMCRYPTO$). $CRYPTO\_BUS\_EXPOSURE$ and $CRYPTO\_RISK\_EXPOSURE$ are defined as how frequently the cryptocurrency-related keywords appear in Item 1 "Business" and Item 1A "Risk Factors" in year t, respectively. Table A.1 defines all cryptocurrency-related keywords in detail. All financial variables are winsorized at 1% and 99% levels, except cryptocurrency exposure variables and the percentage of critical audit matters mentioning cryptocurrency-related keywords ($CAMCRYPTO$). We standardize cryptocurrency exposure variables to have standard deviations equal to one. All variables are described in Table A.4. Standard errors are clustered by Fama-French 12 industries. ***, ** and * indicate significance at the 1%, 5% and 10% levels in a two-tailed test.

Internet Appendix

A MicroStrategy Inc., Case Study

1. **Excerpts from the Critical audit matters of MicroStrategy Inc., for the fiscal year ended December 31, 2020**

> *Evaluation of audit evidence pertaining to the existence and control of digital assets*
>
> As discussed in Notes 2(g) and 5 to the consolidated financial statements, the Company accounts for its digital assets as indefinite-lived intangible assets. The digital assets are recorded at cost, net of any impairment losses incurred since acquisition. As of December 31, 2020, the Company has $1.054 billion of digital assets, net of $70.7 million of impairment.
>
> We identified the evaluation of audit evidence pertaining to the existence of the digital assets and whether the Company controls the digital assets as a critical audit matter. Subjective auditor judgment was involved in determining the nature and extent of evidence required to assess the existence of the digital assets and whether the Company controls the digital assets, as control over the digital assets is provided through private cryptographic keys stored using third-party custodial services at multiple locations that are geographically dispersed. In addition, professionals with specialized skills and knowledge in blockchain technology were needed to assist in the evaluation of the sufficiency of certain audit procedures.
>
> The following are the primary procedures we performed to address this critical audit matter. We evaluated the design and tested the operating effectiveness of certain internal controls over the digital assets process, including a control over the comparison of the Company's records of digital assets held to the custodial records. We involved professionals with specialized skills and knowledge in blockchain technology, who assisted in evaluating certain internal controls over the digital assets process performed at the custodial locations, related specifically to the generation of the private cryptographic keys and the storing of these keys. We obtained confirmation of the Company's digital assets in custody as of December 31, 2020 and compared the total digital assets confirmed to the Company's record of digital asset holdings. We also compared the Company's record of digital asset holdings to the records on the public blockchain using a software audit tool. We applied auditor judgment in determining the nature and extent of audit evidence required, especially related to assessing the existence of the digital assets and whether the Company controls the digital assets. We evaluated the sufficiency and appropriateness of audit evidence obtained by assessing the results of procedures performed over the digital assets.
>
> /s/ KPMG LLP
>
> We have served as the Company's auditor since 2013.
>
> McLean, Virginia
> February 12, 2021

FIGURE IA.1: EXAMPLE OF CRITICAL AUDIT MATTERS FROM MICROSTRATEGY INC. 10-KS IN 2020

Source:

https://www.sec.gov/Archives/edgar/data/1050446/000156459021005783/mstr-10k_20201231.htm

2. **Presentation of cryptocurrency on a financial statement**

Item 1.	Business

Overview

MicroStrategy® pursues two corporate strategies in the operation of its business. One strategy is to grow our enterprise analytics software business and the other strategy is to acquire and hold bitcoin.

.....

We also pursue a business strategy of acquiring bitcoin when our cash, cash equivalents and short-term investments exceed current working capital requirements, and we may from time to time, subject to market conditions, issue debt or equity securities in capital raising transactions with the objective of using the proceeds to purchase bitcoin. We view our bitcoin holdings as long-term holdings and we do not plan to engage in regular trading of bitcoin or to hedge or otherwise enter into derivative contracts with respect to our bitcoin holdings, though we may sell bitcoin in future periods as needed to generate cash for treasury management and other general corporate purposes.

…...

We believe that bitcoin is attractive because it can serve as a store of value, supported by a robust and public open source architecture, that is untethered to sovereign monetary policy and can therefore serve as a hedge against inflation. We also believe that bitcoin offers additional opportunity for appreciation in value with increasing adoption due to its limited supply. In addition, we believe that our bitcoin strategy is complementary to our analytics software and services business, as we believe that our bitcoin and related activities in support of the bitcoin network enhance awareness of our brand and can provide opportunities to secure new customers for our analytics offerings. We are also exploring opportunities to apply bitcoin related technologies such as blockchain analytics into our software offerings.

…...

Our Bitcoin Holdings

At December 31, 2020, we carried $1.054 billion of digital assets on our balance sheet, consisting of the approximately 70,469 bitcoins and reflecting $70.7 million in cumulative impairment losses attributable to bitcoin trading price fluctuations, and held $59.7 million in cash and cash equivalents, compared to no digital assets and $456.7 million in cash and cash equivalents at December 31, 2019, reflecting the shift in our liquid asset holdings following the adoption of our new Treasury Reserve Policy. As of February 8, 2021, we held approximately 71,079 bitcoins that were acquired at an aggregate purchase price of $1.145 billion and an average purchase price of approximately $16,109 per bitcoin, inclusive of fees and expenses. We expect to purchase additional bitcoin in future periods, though we may also sell bitcoin in future periods as needed to generate Cash Assets for treasury management purposes.

FIGURE IA.2: EXAMPLE OF BITCOIN-RELATED BUSINESSES FROM MICROSTRATEGY INC. 10-KS IN 2020

Source: https://sec.report/Document/0001564590-21-005783/#ITEM_1__BUSINESS

	Years Ended December 31,	
	2020	2019
Reconciliation of non-GAAP net income:		
Net (loss) income	$ (7,524)	$ 34,355
Share-based compensation expense	11,153	10,209
Digital asset impairment losses	70,698	0
Gain from Domain Name Sale	0	(29,829)
Interest expense arising from amortization of debt discount and issuance costs	1,543	0
Income tax effects (1)	(25,841)	7,450
Non-GAAP net income	$ 50,029	$ 22,185
Reconciliation of non-GAAP diluted earnings per share:		
Diluted (loss) earnings per share	$ (0.78)	$ 3.33
Share-based compensation expense (per diluted share)	1.15	0.99
Digital asset impairment losses (per diluted share)	7.31	0.00
Gain from Domain Name Sale (per diluted share)	0.00	(2.89)
Interest expense arising from amortization of debt discount and issuance costs (per diluted share)	0.16	0.00
Income tax effects (per diluted share)	(2.67)	0.72
Non-GAAP diluted earnings per share	$ 5.17	$ 2.15

FIGURE IA.3: EXAMPLE OF NON-GAAP NET INCOME FROM MICROSTRATEGY INC. 10-KS IN 2020

Source:

https://www.sec.gov/Archives/edgar/data/1050446/000156459021005783/mstr-10k_20201231.htm

B Identifying cryptocurrency topic exposure

To streamline the analysis process, we extract sentence triples surrounding cryptocurrency keywords to ensure the necessary context to infer the topics of cryptocurrency. More specially, we collect 17,127 sentence triples in Item 1 and 8,229 in Item 1A. After excluding duplicated discussions, we get 13,996 sentence triples in Item 1 and 6,696 in Item 1A, respectively.[35]

Step 1: Selecting cryptocurrency topics. To determine topics that clients discuss when mentioning cryptocurrency keywords, we manually read a large number of randomly selected sentence triples to identify broad topics that are economically meaningful and cover as many sentence triples as possible. The topic should be clearly defined to minimize classification ambiguity in order to guide the machine for automated reading, and classification follows next. We read a training sample of 200 random sentence triples and define four main topics of business activities in Item 1: *(1) production, (2) transaction, (3) mining, (4) investments* and five risk topics in Item 1A: *(1) regulation, (2) business operations, (3) cybersecurity attacks, (4) market risks, and (5) peer risks.*[36]

[35]Duplicates are driven by sentence triples mentioning more than one keyword in its middle sentence.

[36]We initially define five topics; however, because the number of sentence triples of topic M&A is small

Step 2: Developing keywords list of each topic: After defining topics of cryptocurrency business and risk, we develop a list of keywords for each topic. To this end, we develop an interactive procedure that relies on both human reading and machine learning of seeded LDA (Latent Dirichlet Allocation) to identify keywords for each topic.[37]

In each round, while labelling each sentence triple to one of the predefined topics, we manually keep track of typical and meaningfully relevant keywords. Those keywords are the seeds to guide the LDA classification later. Seed words must be unambiguous keywords that readers could quickly agree to represent the topic since a human can reliably know some of the vocabularies used to discuss a given matter ahead of time (Bae, Yu Hung and Van Lent, 2023). Then, the algorithm uses the seed words to explore new keywords that are also likely indicative of the topic of interest. One of the advantages of this method is that humans only need to specify a short list of initial keywords associated with each topic and, therefore, are less susceptible to human error. We then compare (1) topics classified by our selected keywords and (2) topics predicted by the machine and cease the loop until we have fewer than 10 false cases (both positives and negatives). The resulting set of cryptocurrency-related topics and their keywords include the initially human-defined and newly identified keywords from the algorithm, and we make the final decision in selecting which words are chosen for the next step to calculate cryptocurrency topic exposure. If not, we adjust the seed words until the predictive performance meets the required threshold.

More specifically, we start with a training set of 200 random sentence triples from 13,996 of Item 1 of 10-K filings and 200 of Item 1A of 10-K filings to read and select seed words for each crypto-related risks topic. It should be noted that classifying topics even by human reading is a difficult task.[38] We are unambiguously able to assign 133/200 (142/200) sentence triples to one of the predefined topics based on our judgments in Item 1 (Item 1A). There are some common issues in the rest of the training set, including (1) the given sentence triple does not fit any predefined topic and (2) the given sentence triple could relate to multiple topics. Therefore, to generate the keyword lists as clearly as possible, we rely on the set of 133 (142) classifiable sentence triples in Item 1 (Item 1A). We repeat the procedure and cease the iteration after reaching eight false negatives and positives in-sample. The set to test out-of-sample fit includes 30 random sentence triples from the whole population after removing the training set. We stop and save the keywords if this audit produces fewer than five false negatives and positives. Finally, we save validated keywords from conducting the topic classification

(7/200), we remove that label and re-classify those corpora as the closest one of the remaining four topics.

[37]We use seeded LDA package and guidance following Benoit, Watanabe, Wang, Nulty, Obeng, Müller and Matsuo (2018), see more details at `https://tutorials.quanteda.io/machine-learning/topicmodel/`. This methodology allows us to guide the topic discovery process by providing sets of seed words that are representative of the corpus.

[38]Hassan et al. (2023) can clearly classify 437/600 triple sentences in the training sample.

for the whole population in the next step. Our keywords are shown in Tables A.2 and A.3, confirming that our keywords are meaningful and intuitively capture the topics of interest.

Step 3: Classifying sentence triples and topic exposure. After having the topic-specific keywords and classifying all sentence triples, we then calculate the score of topic exposure at each item as the following equation:

$$\text{Crypto Topic Exposure}_{it}^{T} = \frac{1}{S_{it}} \sum_{s=1}^{S_{it}} (1[s \in C^{T}]) * 10^{2} \tag{6}$$

where S_{it} is the total number of sentence triples in Item 1 or Item 1A, $1[\cdot]$ is the indicator function, and C^{T} is the set of final keywords associated with one of the topic categories T shown in Table A.2 and Table A.3.

C Additional Tables

Table IA.1: Keywords are common but irrelevant to cryptocurrency

Keywords	Example sentence triple	Observations
crypto	There were no end use contracts terminated for the year ended April 30, 2021 FEI Zyfer Segment FEI Zyfer designs, develops and manufactures products which provide Precision Navigation and Timing (PNT), primarily incorporating Global Navigation Satellite System(s) technology. FEI Zyfer products make use of both in the clear civil and **crypto** secured military signals for GPS. FEI Zyfer products are integrated into radar systems, airborne SIGINT COMINT platforms, information ne2rks, test equipment, military command and control terminals, and satellite ground stations.	Frequency Electronics Inc; April 30, 2021
	The Company plans to file for loan forgiveness of the second tranche of PPP funding during fiscal year ending March 31, 2022 The COVID 19 outbreak and the uncertainty of economic conditions relating thereto negatively impacted the Company results of operations, cash flows and financial position in the past fiscal year but the Company expects improved results for FY 2022 Based on the operational and financial plans that management has developed, the Company expects to be able to meet its obligations as they become due over the next twelve months. Mode 5 Identification Friend or Foe (IFF) Products T 47 M5 Dual **Crypto** Test Set This new test set has been well received in the market, especially in the international market. It is designed as a KIV 77 KIV78 Mode 5 upgrade for the approximately 2,000 AN APM 480A and T 47 series Mode 4 IFF test sets that the Company has sold both domestically and internationally.	Tel-Instrument Electronics Corp.; March 31, 2021
cryptographic	In common usage, public private key pair cryptography is highly complex and difficult to maintain. The proper management of cryptographic keys and the process of **cryptographically** signing messages are crucial to establishing effective security practices. The Catenis product line vastly simplifies this process, allowing clients to securely leverage the benefits and power of the blockchain.	Q2 Holdings Inc.; December 31, 2018
	This phenomenon is known as a Flash Crash and regulators have imposed some regulations to slow down or suspend trading when a market drops more than a fixed percentage in a short period of time. Encryption The U.S. government has historically tightly regulated the export of **cryptographic** technologies under the Arms Export Control Act and the associated International Traffic in Arms regulations (ITAR) as a form of munition. The logic behind the export restrictions is that the ability to secure information has great value to the military and intelligence agencies, and the US Government does not want those technologies sold or distributed to foreign adversaries.	Quantum Computing Inc.; December 31, 2020
cryptography	A significant barrier to online commerce, portal, social ne2rking and enterprise software is the secure exchange of valuable and confidential information over public ne2rks. We rely on encryption and authentication technology, such as Open SSL, public key cryptography, encryption algorithms RC2 and MD5, digital certificates and HTTPS, to provide the security and authentication necessary to affect the secure exchange of confidential information. Advances in computer capabilities, new 12 discoveries in the field of **cryptography**, new hacking methods, security holes in 3rd party comp1nts (such as operating system bugs) or other events or developments could cause a breach of the above measures that we use to protect customer data and identity.	BroadVision Inc.; December 31, 2018

TABLE IA.1 (continued from previous page)

Keywords	Example sentence triple	Observations
	We take a number of measures to ensure the security of our hardware and software systems and customer information. Advances in computer capabilities, new discoveries in the field of **cryptography** or other developments may result in the technology used by us to protect data being breached or compromised. In the past, banks and other financial service providers have been the subject of sophisticated and highly targeted attacks on their information technology.	Atlanticus Holdings Corporation; December 31, 2018
digital assets	This leads to member acquisition and revenue growth, allowing us to invest more into our content library and enabling the growth cycle to continue. By investing in our in house studios, **digital asset** management system and digital delivery platforms, we can produce and distribute new digital content at low incremental costs. With our end to end production capabilities and unique, exclusive relationships with thought leaders in our areas of focus, we believe we can develop content much more efficiently than our competitors.	Gaia Inc; December 31, 2019
	We intend our proposed CFM solutions will include Web Content Management , which we believe will provide software for authoring, maintaining, and administering websites designed to offer a visitor experience that integrates content from internal and external sources. **Digital Asset** Management , which we believe will provide a set of content management services for browsing, searching, viewing, assembling, and delivering rich media content such as images, audio and video. Customer Communications Management Software , which we believe will make it possible for organizations to process and deliver highly personalized documents in paper or electronic format rather than a 1 message fits all approach.	Beyond Commerce Inc.; December 31, 2021

This table provides examples of sentence triples presented with typical excerpts of non-cryptocurrency topics. We perform a human audit on a limited sample of Item 1 and Item 1A on 10-K fillings to read manually sentence triples surrounding keywords to make sure that our proposed keywords capture well disclosures on cryptocurrency and eliminate misidentified keywords because crypto-related discussion with some common keywords might capture other topics rather than cryptocurrency. For instance, we decide not to use some words even though they are often used in academic journals or newspaper articles, such as crypto, cryptographic, cryptography, digital currency, digital currencies, and digital assets. This is because those above-mentioned keywords per se could refer the secure information and communication techniques or anything that is stored digitally like images, video, word documents, PDFs, graphics, and design files.

Table IA.2: Sample of job descriptions

Auditor name	City	Job title	Excerpt from job descriptions
Deloitte	Memphis, TN	Deloitte Risk & Financial Advisory Associate Software Engine	The position provides excellent opportunity to: + Work as a subject matter resource for supporting client engagement teams in assessing risk of digital asset ecosystems including, but not limited to misappropriation of assets, accuracy and completeness of blockchain data, technical, compliance, and governance risks + Identify strategic risks and opportunities in the digital asset ecosystem based on industry insights, latest academic research, exchange with colleagues + Educate clients and internal teams on digital assets + Prepare technical documentation and diagrams for digital assets and contribute to developing auditing guidance with a focus on topical areas: private key management, smart contract platforms, multi-signature arrangements, privacy coins, protocol governance, byzantine fault tolerance, proof-of-work, and proof-of-stake consensus models + Facilitate use of technology-based tools or methodologies to analyze, design, and/or implement products and services + Analyze, design, code, and test digital asset related software components with an eye for building functional, performance, scalable, production software [...]
KPMG	Atlanta, GA	Manager, Digital Asset Specialis	KPMG is currently seeking a Manager, Digital Asset Specialist to join our Audit Technology Organization (Delivery - Asset Management Solutions team). This is a remote work opportunity organization. Responsibilities: + Serve as a digital asset subject matter expert, for the US audit practice in both internal and external facing roles + Develop and provide support for the advancement of data and technology solutions to support the execution of audits of digital assets and blockchain/Web3 companies + Support research efforts into new trends in digital assets, blockchain technologies and Web3 as well as the impact on the audit and our clients + Work with software development team to expand capabilities in our digital asset tools, manage the product roadmap, document new feature requirements and support subsequent releases + Collaborate with our third-party data providers to support new digital assets/blockchains through vendor APIs; perform data quality reviews over vendor data for assets + Facilitate business development activities related to blockchain/web3 companies. Qualifications: + Minimum five years of recent experience in delivering audit or advisory engagements in a client-facing capacity + Bachelor's degree from an accredited college/university or equivalent work experience; CPA qualification preferred + Experience in audit or risk assurance areas such as internal audit, IT controls testing, IT advisory or data analytics + Specific experience working with clients on digital asset related projects or personal interest in digital assets preferred [...]

Table IA.2 (continued from previous page)

Auditor name	City	Job title	Excerpt from job descriptions
EY	San Francisco, CA	Financial Services Audit - Blockchain Developer - Senior	You will be a part of the US Blockchain Assurance team, an innovative and collaborative group of software developers, auditors and technology consultants who are dedicated to developing the deep technical understanding, methodology and tools required to enable a variety of Assurance services to companies that hold and transact in digital assets. You will have the opportunity to research the latest public blockchains, smart contracts and digital assets, as well as serve the clients that drive this exciting and disruptive industry forward. To provide Assurance services including audits, audit-readiness, forensic investigations and related due diligence, we must have a technical understanding of the wide variety of public blockchains, smart contracts and the digital assets native to these platforms, along with the relevant risks and controls involved. We also must develop the tools and methodology to assess our clients' activities in this sector [...]
PwC	Florham Park, NJ	Digital Assets - Regulatory Risk & Compliance, Manager	As part of the team, youll help our clients enhance their organisational structure, analyse current operations and technology in order to create cost effective compliant operations that support performance objectives and sustainable value for our client. Job Requirements and Preferences : Basic Qualifications : Minimum Degree Required : Bachelor Degree Required Fields of Study : Business Administration/Management, Economics, Engineering, Operations Management/Research, Finance, Accounting, Computer and Information Science Minimum Years of Experience : 5 year(s) with 3 or more years of experience in cryptocurrency and/or digital assets. Preferred Qualifications : Degree Preferred : Master of Business Administration Additional Educational Preferences : Degrees in Science or Engineering may be considered. Preferred Knowledge/Skills : Demonstrates extensive abilities and/or a proven record of success as a team leader working with business stakeholders and understanding their business needs including: Having a general industry understanding of front, middle and back office processes associated with cryptocurrency and related FinTech industries such as banking, lending and payments; Having deep knowledge of the digital assets ecosystem, including crypto, stablecoins and NFTs (either financial products or non-financial products like gaming); Having personal experience in trading crypto/digital assets; Having a track record of delivering crypto services to organizations in the ecosystem (this could be new entrants like crypto exchanges or traditional institutions adopting digital assets); and, Having service delivery experience includes, but is not limited to due diligence, transaction support, governance, internal controls, risk management, regulatory compliance, financial crimes (e.g. AML, Sanctions) product strategy and platform implementation

Table IA.2 (continued from previous page)

Auditor name	City	Job title	Excerpt from job descriptions
Grant Thornton	Philadelphia, PA	Forensic Technology Senior Associate (Full-Stack Developer)	Grant Thornton is looking for a junior software engineer to join its Forensic Technology Services (FTS) practice. The FTS practice focuses on blockchain and cryptocurrency investigations and analysis, cybersecurity incident response, Web3 and NFT technologies, and forensic data analysis. FTS delivers these services to clients using a variety of technologies including SQL, Python, Docker, and MongoDB. This position provides challenging work involving quantitative analysis of structured, semi-structured, and unstructured data using various programming techniques. The responsibilities would range from initial data scoping and ETL through the development of analytical solutions. The project work varies by engagement but includes fraud detection, blockchain analytics, digital asset tracing, historical modeling, outlier analysis, and data visualizations [...]
RSM	New York, NY	Blockchain Sr Associate	The Blockchain Senior Associate is primarily responsible for supporting and teaming with various leaders in Innovation in order to help the firm achieve its innovation objectives. This individual will lead opportunities and have the responsibility of designing and developing applications in different Blockchain platforms including but not limited to Hyper ledger, Ethereum, Bitcoin and other distributed computing environments to deliver solutions to line of business partners. This individual will lead blockchain initiatives as assigned and act as innovation liaison for key stakeholders, internal leaders, subject matter experts and external parties. This Blockchain Senior Associate will act with a sense of urgency and collaborate with internal stakeholders to identify and remove roadblocks that impede time to value on client engagements. This individual will research, design and/or develop blockchain technology including frameworks, distributed ledger protocols and consensus mechanisms. REQUIRED: Knowledge of blockchain, digital asset and cryptocurrency technologies Understanding of the RSM Tax, Audit and/or Consulting lines of business PREFERRED Be able to balance multiple competing priorities [...]

This table shows a sample of actual job descriptions of crypto-related job postings of auditors in the posted year of 2022. We started with a list of audit firms in Audit Opinion in Audit Analytics from the calendar year 2010. We manually matched the employers' names in Lightcast with the names of auditors in Audit Analytics and retrieved any job postings that mention crypto-related keywords in Table A.1. To minimize false positives, we retain only those jobs by audit offices with the same name and the same city in both Lightcast and Audit Analytics. We then use the list of crypto-related keywords in Table A.1 to identify job postings (job descriptions) that match these specific keywords.

Table IA.3: Snippets of Top Cryptocurrency Business Exposure Observations

CIK - Company	**Report period**	**Crypto-Business exposure**	**Example sentence triple**
1050446 - MICROSTRATEGY Inc	31-Dec-22	450.78	Business Overview MicroStrategy pursues two corporate strategies in the operation of its business. ***One strategy is to acquire and hold bitcoin and the other strategy is to grow our enterprise analytics software business***. We believe that undertaking these two, interdependent corporate strategies serves as a key differentiator for our business, as our bitcoin acquisition strategy has raised our profile with potential software customers while our enterprise analytics software business has provided stable cash flows that allow us to acquire and hold bitcoin for the long-term.
1001601 - MGT CAPITAL INVESTMENTS, INC.	31-Dec-20	441.64	Some of these companies are our suppliers. We compete to attract, engage, and retain personnel, educated and skilled in the Blockchain and cryptocurrency mining space. We compete with vertically integrated companies such as Bitfury Group Limited and Bitmain Technologies LTD that engage in both the ***design and distribution of mining machines***, as well as ***cryptocurrency mining***.
1437750 - T-REX Acquisition Corp.	30-Jun-22	369.46	***Through our operating subsidiary, Raptor Mining LLC ("Raptor Mining"), we are engaged in the cryptocurrency mining***, which is the process of receiving cryptocurrency rewards for securing particular distributed ledger platforms. Our first cryptocurrency mining operation is located in Tampa, Florida, and the first distributed ledger platform that we are securing is Bitcoin. "Bitcoin" refers to the entire decentralized distributed ledger technology founded, upon information and belief, by a person using the pseudonym Satoshi Nakamoto and maintained by thousands of volunteers globally since January 2009.
827876 - CLEANSPARK, INC.	30-Sep-22	346.73	Bitcoin mining has now become our principal revenue generating business activity. ***We currently intend to continue to acquire additional facilities, equipment and infrastructure capacity to continue to expand our bitcoin mining operations.*** In August 2022, we completed the acquisition of certain real property located in Wilkes County, Georgia, and approximately 3,400 S19 and S19j Pro series bitcoin miners capable of providing computing power of approximately 341,000 terahash per second.

Table IA.3 (continued from previous page)

CIK - Company	Report period	Crypto-Business exposure	Example sentence triple
1436229 - BTCS Inc.	31-Dec-16	312.83	OUR BUSINESS Subject to additional financing, the Company plans to create a portfolio of digital assets including bitcoin and other "protocol tokens" to provide investors a diversified pure-play exposure to the bitcoin and blockchain industries. The Company intends to acquire digital assets through: open market purchases, participating in initial digital asset offerings (often referred to as initial coin offerings). Additionally, the Company may acquire digital assets by resuming its transaction verification services business through outsourced data centers and earning rewards in digital assets by securing their respective blockchains.
1520118 - INTEGRATED VENTURES, INC.	30-Jun-18	297.74	Participation in such pools is essential for our mining business. Our Cryptocurrency Operations In our digital currency mining operations, the following models of miners are owned and deployed by the Company: Antminer S9, Antminer L3, Antminer A3, Antminer E3, Antminer X3, Innosillicon A4, PandaMiner Pro and Bitworks. We utilize and rely on cryptocurrency pools to mine cryptocurrencies and generate a mixed selection of digital cryptocurrencies, including BTC, LTC, ETH, and ETN.
1436229 - BITCOIN SHOP INC.	31-Dec-14	296.74	BUSINESS INTRODUCTION During February 2014 ***we entered the business of hosting an online ecommerce marketplace where consumers can purchase merchandise using digital currencies, including bitcoin*** and are building a diversified company with operations in the digital currency ecosystem. In January 2015 we began a rebranding campaign using our BTCS.COM domain (shorthand for Blockchain Technology Consumer Solutions) to better reflect our broadened strategy. We released our new website which included broader information on our strategy, access to our ecommerce site, and launching an invite only beta version of our multi-sig secure storage solution (digital wallet).

This table lists the top observations from our face validation for the top 50 highest scores of cryptocurrency business exposure. For firms with more than one observation, we present the highest one. We calculate the scores of Crypto Exposure in Item 1 at the client level from 2008 to 2022. We measure client-level exposure to cryptocurrency business by the equation:

$$\text{Crypto Exposure}_{it} = \frac{1}{B_{it}} \sum_{b=1}^{B_{it}} (1[b \in C]) * 10^4 \tag{7}$$

where $b = 0, 1, ..., B_{it}$ are the words in Item 1 or Item 1A of firm i in year t, B_{it} is the total number of words in Item 1 or Item 1A, $1[\cdot]$ is the indicator function and C is the set of crypto-related words in Table A.1.

Table IA.4: Snippets of Top Cryptocurrency Risk Exposured Observations

CIK - Company	Report period	Crypto-Risk exposure	Example sentence triple
1723788 - Bitwise 10 Crypto Index Fund	31-Dec-22	268.16	Risks Related to Crypto Assets The Blockchains on which ownership of Portfolio Crypto Assets are recorded and the Portfolio Crypto Assets themselves may be the target of malicious cyberattacks or may contain exploitable flaws in their underlying code, which may result in security breaches, the loss or theft of Portfolio Crypto Assets or the decline in value of Portfolio Crypto Assets. The Portfolio Crypto Assets rely on Blockchains for records of ownership. As a result, the Portfolio Crypto Assets are subject to a number of reliability and security risks attendant to Blockchain and distributed ledger technology, including malicious attacks seeking to identify and exploit weaknesses in the software.
1001601 - MGT CAPITAL INVESTMENTS, INC.	31-Dec-22	225.81	If the market for Bitcoin does not grow as we expect, our business, operating results, and financial condition could be adversely affected. Certain features of Bitcoin's Blockchain, such as "forking" in which one type of Bitcoin could turn into many due to source code variation, or Halving which reduces the rewards for mining efforts by 50% every 210,000 blocks that are solved, pose the risk of adversely affecting our ability to generate revenue. Our operating results have and will significantly fluctuate due to the highly volatile nature of Bitcoin, and if the price of Bitcoin declines, including potentially due to political, economic, or other forces beyond our control, it would materially adversely affect our business.
1580485 - Nodechain, Inc.	31-Dec-17	216.09	Although the Company does not participate in ICOs, its clients and customers may participate in ICOs and these actions may be a prelude to further action which chills widespread acceptance of blockchain and cryptocurrency adoption and have a material adverse effect on the ability of the Company to continue as a going concern or to pursue this segment at all, which would have a material adverse effect on the business, prospects or operations of the Company. Governments may in the future take regulatory actions that prohibit or severely restrict the right to acquire, own, hold, sell, use or trade cryptocurrencies or to exchange cryptocurrencies for fiat currency. Similar actions by governments or regulatory bodies (such as an exchange on which the Company's securities are listed, quoted or traded) could result in restriction of the acquisition, ownership, holding, selling, use or trading in the Company's securities.

Table IA.4 (continued from previous page)

CIK - Company	Report period	Crypto-Risk exposure	Example sentence triple
1767057 - Osprey Bitcoin Trust	31-Dec-21	215.62	Risk Factors Related to the Bitcoin Markets The value of the Units relates directly to the value of Bitcoins, the value of which may be highly volatile and subject to fluctuations due to a number of factors. Due to the unregulated nature and lack of transparency surrounding the operations of Bitcoin exchanges, they may experience fraud, security failures or operational problems, which may adversely affect the value of Bitcoin and, consequently, the value of the Units. Competition from the emergence or growth of other digital assets or methods of investing in Bitcoin could have a negative impact on the price of Bitcoin and adversely affect the value of the Units.
1588489 - Grayscale Bitcoin Trust (BTC)	31-Dec-19	203.45	For instance, the Custodian may not agree to provide access to the IR Virtual Currency. In addition, the Sponsor may determine that there is no safe or practical way to custody the IR Virtual Currency, or that trying to do so may pose an unacceptable risk to the Trust's holdings in Bitcoin, or that the costs of taking possession and/or maintaining ownership of the IR Virtual Currency exceed the benefits of owning the IR Virtual Currency. Additionally, laws, regulation or other factors may prevent Shareholders from benefiting from the Incidental Right or IR Virtual Currency even if there is a safe and practical way to custody and secure the IR Virtual Currency.
1167419 - Riot Blockchain, Inc.	31-Dec-19	202.82	If we are unable to expand and remain competitive, our business could be negatively affected which would have an adverse effect on the trading price of our securities, which would harm investors in our Company. Facebook's development of a cryptocurrency may adversely affect the value of bitcoin and other cryptocurrencies. In May 2019, Facebook announced its plans for a cryptocurrency called Libra, which faced significant government intervention.
1578731 - HashingSpace Corp	31-Aug-15	183.99	Our loss of access to our private keys or our experience of a data loss relating to our bitcoins could have a material adverse effect on our business. Bitcoins are controllable only by the possessor of both the unique public key and private key relating to the local or online digital wallet in which the bitcoins are held. We are required by the operation of the bitcoin network to publish the public key relating to a digital wallet in use by us when it first verifies a spending transaction from that digital wallet and disseminates such information into the bitcoin network.

This table lists the top observations from our face validation for the top 50 highest scores of cryptocurrency risk exposure. For firms with more than one observation, we present

the highest one. We calculate the scores of Crypto Exposure in Item 1 at the client level from 2008 to 2022. We measure client-level exposure to cryptocurrency risk by the equation:

$$\text{Crypto Exposure}_{it} = \frac{1}{B_{it}} \sum_{b=1}^{B_{it}} (1[b \in C]) * 10^4 \tag{8}$$

where $b = 0, 1, ..., B_{it}$ are the words in Item 1 or Item 1A of firm i in year t, B_{it} is the total number of words in Item 1 or Item 1A, $1[\cdot]$ is the indicator function and C is the set of crypto-related words in Table A.1.

Table IA.5: Captured Cryptocurrency keywords and frequencies

Item 1		Item 1A	
keywords	frequency	keywords	frequency
bitcoin	6,906	bitcoin	13,347
blockchain	5,752	blockchain	4,668
cryptocurrency	2,846	cryptocurrency	4,480
cryptocurrencies	1,392	cryptocurrencies	4,167
ethereum	387	ethereum	1,710
distributed ledger	277	crypto assets	1,495
crypto assets	254	crypto asset	855
crypto asset	171	distributed ledger	434
litecoin	111	cryptocurrency-related	186
crypto currency	84	litecoin	145
crypto mining	56	crypto mining	105
initial coin offering	38	distributed ledgers	91
cryptocurrency-related	35	initial coin offering	58
crypto currencies	25	altcoin	36
distributed ledgers	19	crypto currencies	32
decentralized ledger	17	dogecoin	19
dogecoin	11	crypto currency	17
cryptocurrency-based	11	cryptocurrency's	16
altcoin	6	cryptocurrency-based	16
usd coin	5	crypto asset's	14
cryptocurrency-focused	5	crypto asset-related	7
crypto coins	3	usd coin	5
cryptographic asset	3	decentralized ledger	2
cryptographic assets	3	cryptographic assets	1
cryptocoin	2	cryptographic asset	1
cryptocurrencies-bitcoin	2	crypto assets-	1
cryptocurrency's	2	crypto assetholder	1
cryptocurrency-mining	2	crypto assets's	1
cryptocurrency-specific	1		
crypto coin	1		
cryptocurrency-to-cryptocurrency	1		
crypto currency-related	1		
crypto asset-related	1		
cryptocurrency-linked	1		

This table reports validated cryptocurrency keywords and frequencies captured in all Items 1 and Item 1A. Keywords are provided in Table A.1.

Table IA.6: Time Series variation of Cryptocurrency Exposure

Panel A - Distribution of $CRYPTO\_BUS\_EXPOSURE$ by year

Fyear	Mean	Median	Standard deviation	Exposure > 0	Exposure = 0	N
2007	0.0000	0.0000	0.0000	0	875	875
2008	0.0000	0.0000	0.0000	0	8894	8894
2009	0.0000	0.0000	0.0000	0	8746	8746
2010	0.0000	0.0000	0.0000	0	8341	8341
2011	0.0000	0.0000	0.0000	0	7939	7939
2012	0.0000	0.0000	0.0000	0	7541	7541
2013	0.0362	0.0000	1.6497	7	7352	7359
2014	0.0789	0.0000	3.7566	15	7167	7182
2015	0.1205	0.0000	4.9584	21	6767	6788
2016	0.0977	0.0000	4.2362	20	6401	6421
2017	0.6316	0.0000	9.3336	101	6085	6186
2018	0.8079	0.0000	10.8429	124	5854	5978
2019	0.6361	0.0000	9.5339	117	5681	5798
2020	0.6780	0.0000	9.9201	132	5935	6067
2021	1.1686	0.0000	12.4652	269	6453	6722
2022	1.3957	0.0000	15.8788	249	5801	6050

Panel B - Distribution of $CRYPTO\_RISK\_EXPOSURE$ by year

Fyear	Mean	Median	Standard deviation	Exposure > 0	Exposure = 0	N
2007	0.0000	0.0000	0.0000	0	875	875
2008	0.0000	0.0000	0.0000	0	8894	8894
2009	0.0000	0.0000	0.0000	0	8746	8746
2010	0.0000	0.0000	0.0000	0	8341	8341
2011	0.0000	0.0000	0.0000	0	7939	7939
2012	0.0000	0.0000	0.0000	0	7541	7541
2013	0.0340	0.0000	1.8758	8	7351	7359
2014	0.0482	0.0000	2.6078	10	7172	7182
2015	0.0436	0.0000	2.4164	10	6778	6788
2016	0.0071	0.0000	0.2603	17	6404	6421
2017	0.3220	0.0000	6.3486	75	6111	6186
2018	0.2843	0.0000	5.3135	92	5886	5978
2019	0.2494	0.0000	5.3417	106	5692	5798
2020	0.3225	0.0000	5.6175	130	5937	6067
2021	0.6750	0.0000	8.7241	243	6479	6722
2022	0.9193	0.0000	10.1706	270	5780	6050

This table reports the distribution of clients' cryptocurrency exposure over time. Statistics (mean, median, and SD) are reported at the client-year level across time. We also provide the number of observations with positive scores (Exposure > 0), zeros (Exposure = 0), and the total number of observations (N) in each year. We collect all 10-Ks from the EDGAR database and extract all Items 1 and Items 1A. We keep only observations of Items 1 containing at least 30 words and 3 sentences.

Table IA.7: Industry distribution of cryptocurrency exposure

Panel A - Distribution of *CRYPTO_BUS_EXPOSURE* by industry

Rank	Fama-French 12 industries	Mean	Median	Standard deviation	Exposure > 0	Exposure = 0	N
1	Business Equipment	0.9579	0.0000	13.0375	316	13,437	
2	Finance	0.3456	0.0000	7.2763	315	26,557	
3	Consumer Durables	0.3103	0.0000	4.9522	19	2,256	
4	Wholesale, Retail, and Some Services	0.2983	0.0000	7.2199	56	8,387	
5	Chemicals and Allied Products	0.2790	0.0000	4.6484	26	2,555	
6	Consumer NonDurables	0.2723	0.0000	4.8292	32	4,291	
7	Other	0.2434	0.0000	5.0889	194	18,052	
8	Healthcare, Medical Equipment, and Drugs	0.1612	0.0000	5.7169	35	13,076	
9	Telephone and Television Transmission	0.1131	0.0000	1.7491	17	2,331	
10	Manufacturing	0.0830	0.0000	1.6874	34	6,855	
11	Oil, Gas, and Coal Extraction and Products	0.0277	0.0000	1.5846	6	4,696	
12	Utilities	0.0041	0.0000	0.1363	5	3,339	

Panel B- Distribution of *CRYPTO_RISK_EXPOSURE* by industry

Rank	Fama-French 12 industries	Mean	Median	Standard deviation	Exposure > 0	Exposure = 0	N
1	Business Equipment	0.4111	0.0000	6.8235	214	13,539	13,753
2	Finance	0.2558	0.0000	5.5232	464	26,408	26,872
3	Other	0.1625	0.0000	4.2705	146	18,100	18,246
4	Wholesale, Retail, and Some Services	0.1247	0.0000	3.0241	52	8,391	8,443
5	Telephone and Television Transmission	0.1026	0.0000	2.8032	8	2,340	2,348
6	Consumer NonDurables	0.0599	0.0000	1.6598	16	4,307	4,323
7	Healthcare, Medical Equipment, and Drugs	0.0553	0.0000	2.9978	23	13,088	13,111
8	Chemicals and Allied Products	0.0539	0.0000	1.1315	8	2,573	2,581
9	Oil, Gas, and Coal Extraction and Products	0.0254	0.0000	1.3692	2	4,700	4,702
10	Manufacturing	0.0100	0.0000	0.5445	12	6,877	6,889
11	Consumer Durables	0.0087	0.0000	0.2567	9	2,266	2,275
12	Utilities	0.0035	0.0000	0.0954	7	3,337	3,344

This table reports the distribution of clients' cryptocurrency exposure for Fama & French 12 industries. Statistics (mean, median, and SD) are reported at the client-year level across different industries. We rank sectors by the average values of the cryptocurrency exposure measures. We also provide the number of observations with positive scores (Exposure > 0), zeros (Exposure = 0), and the total number of observations (N) in each industry.

Table IA.8: Cryptocurrency-related Big4's accounting guidance

Auditor name	Guidance or financial alert name	Released date (or month)	# Pages
PricewaterhouseCoopers LLP	Cryptographic assets and related transactions: accounting considerations under IFRS	1-Sep-18	26
PricewaterhouseCoopers LLP	Cryptographic assets and related transactions: accounting considerations under IFRS	1-Dec-19	23
PricewaterhouseCoopers LLP	Crypto assets	1-Aug-21	31
PricewaterhouseCoopers LLP	Crypto assets	1-Feb-23	41
Ernst & Young LLP	IFRS (#) Accounting for crypto-assets	1-Aug-18	24
Ernst & Young LLP	Applying IFRS Accounting by holders of crypto-assets – Updated September 2019	1-Sep-19	29
Ernst & Young LLP	Applying IFRS Accounting by holders of crypto assets	1-Oct-21	35
Ernst & Young LLP	Accounting for digital assets, including crypto assets	30-Jun-22	19
Deloitte & Touche LLP	Classification of Cryptocurrency Holdings	9-Jul-18	4
Deloitte & Touche LLP	Corporates investing in crypto	21-Jan-21	15
KPMG LLP	Institutionalization of cryptoassets	1-Nov-18	42
KPMG LLP	Cryptoassets – Accounting and tax	1-Apr-19	4
KPMG LLP	Institutionalization of cryptoassets	1-Nov-20	42
KPMG LLP	Principal market, unit of account and income statement presentation	1-Jan-22	7
KPMG LLP	Constituents to FASB: Crypto asset accounting guidance urgently needed	1-Jan-22	9
KPMG LLP	Accounting for crypto assets - Executive Summary	1-Mar-22	11
KPMG LLP	Evaluating custody of digital assets	1-Mar-22	7
KPMG LLP	Hot topics: Accounting for staking rewards	1-Aug-22	8

This table presents a comprehensive list of guidance and financial alerts pertaining to the accounting for cryptocurrency. The information has been collected from the websites of the Big4 accounting firms.

Table IA.9: Effect of underlying riskiness of client business

	LNAUFEES		AUDITLAG		GCO		CAMCRYPTO	
	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
CRYPTO_BUS_EXPOSURE	0.0091**		0.1812***		0.0053***		0.0283***	
	(2.4765)		(7.5063)		(10.3004)		(83.0143)	
CRYPTO_BUS_EXPOSURE × COIN_DOWN	0.0083***		0.0149		0.0009		-0.0020	
	(5.1078)		(0.1752)		(0.4645)		(-0.6191)	
CRYPTO_RISK_EXPOSURE		0.0082		0.2021***		0.0037***		0.0284***
		(1.5310)		(3.8100)		(4.9113)		(25.7442)
CRYPTO_RISK_EXPOSURE × COIN_DOWN		0.0143***		0.0316		0.0020		-0.0006
		(8.6878)		(0.3164)		(1.0467)		(-0.0599)
COIN_DOWN	0.0540***	0.0538***	-0.1636	-0.1653	0.0101**	0.0101**	-0.0008	-0.0008
	(13.2080)	(13.3319)	(-1.2413)	(-1.2547)	(3.0498)	(3.0524)	(-1.5841)	(-1.2925)
Adjusted R^2	0.85062	0.85065	0.50038	0.50042	0.43405	0.43383	0.62078	0.63522
Observations	25,590	25,590	25,590	25,590	25,590	25,590	7,718	7,718
Industry fixed effects	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

This table reports the results from linear probability models relating auditor responses to the firm's exposure to cryptocurrency. The outcome variable is either (i) the natural logarithm of audit fees in year t ($LNAUFEES_{it}$), (ii) the number of days between a client's fiscal year-end and auditor signature date ($AUDITLAG$), (iii) an indicator variable that equals one if the auditor issues a going-concern opinion to the client in year t and zero otherwise (GCO_{it}), (iv) the percentage of critical audit matters mentioning cryptocurrency-related keywords ($CAMCRYPTO$). $CRYPTO\_BUS\_EXPOSURE$ and $CRYPTO\_RISK\_EXPOSURE$ are defined as how frequently the cryptocurrency-related keywords appear in Item 1 "Business" and Item 1A "Risk Factors" in year t, respectively. $COIN\_DOWN$ is an indicator variable that equals one if the ratio of changes in bitcoin price from year t to year $t-1$ to price in year $t-1$ is negative. Table A.1 defines all cryptocurrency-related keywords in detail. All financial variables are winsorized at 1% and 99% levels, except cryptocurrency exposure variables and the percentage of critical audit matters mentioning cryptocurrency-related keywords ($CAMCRYPTO$). We standardize cryptocurrency exposure variables to have standard deviations equal to one. All variables are described in Table A.4. Standard errors are clustered by Fama-French 12 industries. ***, ** and * indicate significance at the 1%, 5% and 10% levels in a two-tailed test.

Table IA.10: Firm characteristics (matching by covariates)

Panel A: Sample of audit fees and going-concern opinions regressions

	Exposure = 0			**Exposure > 0**			T-test		
Variables	N	Mean	Sd	N	Mean	Sd	Diff	T-statistic	Adjusted p-value
BIG4	320	0.447	0.498	320	0.438	0.497	0.009	0.238	0.972
BTM	320	0.230	1.143	320	0.233	1.069	-0.003	-0.035	0.972
CFO	320	-0.181	0.559	320	-0.212	0.572	0.031	0.701	0.972
LEV	320	0.378	0.744	320	0.391	0.773	-0.013	-0.224	0.972
SIZE	320	5.857	3.397	320	5.812	3.602	0.045	0.163	0.972
LOSS	320	0.519	0.500	320	0.516	0.501	0.003	0.079	0.972
BUSSEG	320	1.688	1.037	320	1.850	1.300	-0.163	-1.749	0.890
GEOSEG	320	1.813	1.680	320	1.834	1.879	-0.022	-0.155	0.972
RESTRUCT	320	0.234	0.424	320	0.241	0.428	-0.006	-0.185	0.972
ROA	320	-0.411	1.055	320	-0.495	1.125	0.084	0.977	0.972
GROWTH	320	0.305	1.065	320	0.416	1.324	-0.111	-1.172	0.972

Panel B: Sample of critical audit matters regression

	Exposure = 0			**Exposure > 0**			T-test		
Variables	N	Mean	Sd	N	Mean	Sd	Diff	T-statistic	Adjusted p-value
BIG4	134	0.612	0.489	134	0.5896	0.4938	0.022	0.373	1.000
BTM	134	0.419	0.544	134	0.3617	0.5963	0.057	0.820	1.000
CFO	134	-0.027	0.237	134	-0.0264	0.2483	0.000	-0.008	1.000
LEV	134	0.283	0.299	134	0.2584	0.2533	0.024	0.720	1.000
SIZE	134	7.361	2.899	134	7.4139	3.0754	-0.053	-0.144	1.000
LOSS	134	0.351	0.479	134	0.3657	0.4834	-0.015	-0.254	1.000
BUSSEG	134	1.746	1.038	134	1.9925	1.3122	-0.246	-1.704	0.987
GEOSEG	134	2.022	1.553	134	2.1791	1.8470	-0.157	-0.752	1.000
RESTRUCT	134	0.261	0.441	134	0.2612	0.4409	0.000	0.000	1.000
ROA	134	-0.106	0.364	134	-0.1143	0.3897	0.009	0.185	1.000
GROWTH	134	0.247	0.703	134	0.2539	0.8019	-0.007	-0.078	1.000

This table shows the characteristics of clients exposed to cryptocurrency and clients not exposed to cryptocurrency when using matching on covariates. All financial variables are winsorized at 1% and 99% levels. All variables are described in Table A.4.

Table IA.11: Firm characteristics (matching by propensity matching score)

Panel A: Sample of audit fees and going-concern opinions regressions

	Exposure = 0			**Exposure > 0**			T-test		
Variables	N	Mean	Sd	N	Mean	Sd	Diff	T-statistic	Adjusted p-value
BIG4	320	0.422	0.495	320	0.438	0.497	-0.016	-0.399	0.759
BTM	320	0.349	1.078	320	0.233	1.069	0.117	1.375	0.627
CFO	320	-0.186	0.604	320	-0.212	0.572	0.026	0.559	0.759
LEV	320	0.345	0.622	320	0.391	0.773	-0.047	-0.843	0.627
SIZE	320	6.137	3.016	320	5.812	3.602	0.326	1.240	0.627
LOSS	320	0.472	0.500	320	0.516	0.501	-0.044	-1.106	0.627
BUSSEG	320	1.800	1.368	320	1.850	1.300	-0.050	-0.474	0.759
GEOSEG	320	2.134	2.538	320	1.834	1.879	0.300	1.699	0.627
RESTRUCT	320	0.272	0.446	320	0.241	0.428	0.031	0.905	0.627
ROA	320	-0.417	1.107	320	-0.495	1.125	0.079	0.890	0.627
GROWTH	320	0.388	1.099	320	0.416	1.324	-0.028	-0.296	0.768

Panel B: Sample of critical audit matters regression

	Exposure = 0			**Exposure > 0**			T-test		
Variables	N	Mean	Sd	N	Mean	Sd	Diff	T-statistic	Adjusted p-value
BIG4	134	0.537	0.500	134	0.590	0.494	-0.052	-0.860	0.928
BTM	134	0.325	0.660	134	0.362	0.596	-0.037	-0.478	0.928
CFO	134	-0.010	0.235	134	-0.026	0.248	0.017	0.560	0.928
LEV	134	0.297	0.340	134	0.258	0.253	0.039	1.057	0.928
SIZE	134	7.449	2.811	134	7.414	3.075	0.035	0.096	0.928
LOSS	134	0.336	0.474	134	0.366	0.483	-0.030	-0.510	0.928
BUSSEG	134	2.007	1.395	134	1.993	1.312	0.015	0.090	0.928
GEOSEG	134	2.493	2.635	134	2.179	1.847	0.313	1.128	0.928
RESTRUCT	134	0.246	0.432	134	0.261	0.441	-0.015	-0.280	0.928
ROA	134	-0.082	0.343	134	-0.114	0.390	0.032	0.719	0.928
GROWTH	134	0.217	0.630	134	0.254	0.802	-0.037	-0.418	0.928

This table shows the characteristics of clients exposed to cryptocurrency and clients not exposed to cryptocurrency when using matching on covariates. All financial variables are winsorized at 1% and 99% levels. All variables are described in Table A.4.

Table IA.12: Client-level exposure to cryptocurrency and auditor responses (matching sample)

	LNAUFEES		AUDITLAG		GCO		CAMCRYPTO	
	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
Panel A: Matching on covariates								
CRYPTO_BUS_EXPOSURE	0.011***		0.100**		0.004***		0.027***	
	(4.711)		(3.069)		(15.688)		(78.512)	
CRYPTO_RISK_EXPOSURE		0.010***		0.126**		0.003***		0.028***
		(4.955)		(2.764)		(5.058)		(18.644)
Adjusted R^2	0.89920	0.89868	0.56057	0.56103	0.49198	0.48926	0.59174	0.62608
Panel B: Propensity score matching								
CRYPTO_BUS_EXPOSURE	0.011***		-0.043		0.003***		0.027***	
	(4.597)		(-1.270)		(15.890)		(66.872)	
CRYPTO_RISK_EXPOSURE		0.011***		-0.006		0.002***		0.028***
		(4.307)		(-0.093)		(4.015)		(21.716)
Adjusted R^2	0.89469	0.89442	0.54371	0.54358	0.51632	0.51371	0.58791	0.62289
Observations	640	640	640	640	640	640	268	268
Control variables	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Year fixed effects	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Industry fixed effects	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

This table reports the results from linear probability models relating auditor responses to the firm's exposure to cryptocurrency as shown in Equation (3) for a matching sample of firms in the same industry-year:

$$\text{Auditor responses}_{it} = \beta_0 + \beta_1 * \text{Crypto exposure}_{it} + \beta * Z + \epsilon_{it}$$

The outcome variable is either (i) the natural logarithm of audit fees in year t ($LNAUFEES_{it}$), (ii) the number of days between a client's fiscal year-end and auditor signature date ($AUDITLAG$), (iii) an indicator variable that equals one if the auditor issues a going-concern opinion to the client in year t and zero otherwise (GCO_{it}), (iv) the percentage of critical audit matters mentioning cryptocurrency-related keywords ($CAMCRYPTO$). $CRYPTO\_BUS\_EXPOSURE$ and $CRYPTO\_RISK\_EXPOSURE$ are defined as how frequently the cryptocurrency-related keywords appear in Item 1 "Business" and Item 1A "Risk Factors" in year t, respectively. Table A.1 defines all cryptocurrency-related keywords in detail. All financial variables are winsorized at 1% and 99% levels, except cryptocurrency exposure variables and the percentage of critical audit matters mentioning cryptocurrency-related keywords ($CAMCRYPTO$). We standardize cryptocurrency exposure variables to have standard deviations equal to one. All variables are described in Table A.4. Standard errors are clustered by Fama-French 12 industries. ***, ** and * indicate significance at the 1%, 5% and 10% levels in a two-tailed test.

Table IA.13: Client-level exposure to cryptocurrency and auditor response (with a dummy variable of cryptocurrency exposure)

	LNAUFEES		AUDITLAG		GCO		CAMCRYPTO	
	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
CRYPTO_BUS_DUM	0.193*		5.260**		0.067***		0.077	
	(1.930)		(2.839)		(4.801)		(1.500)	
CRYPTO_RISK_DUM		0.162***		2.712***		0.048**		0.038
		(6.326)		(4.368)		(3.014)		(1.153)
SIZE	0.420***	0.419***	-3.807***	-3.817***	-0.026***	-0.026***	0.000	-0.001
	(15.383)	(15.212)	(-13.544)	(-13.712)	(-6.304)	(-6.399)	(-1.167)	(-1.177)
LEV	0.057	0.058	1.482	1.491	0.044***	0.044***	0.000	0.000
	(1.201)	(1.215)	(1.561)	(1.581)	(5.903)	(5.999)	(-0.262)	(1.641)
CFO	-0.152	-0.152*	-0.415	-0.434	-0.145***	-0.145***	0.014	0.013
	(-1.792)	(-1.803)	(-0.195)	(-0.203)	(-7.702)	(-7.834)	(0.987)	(1.115)
ROA	-0.015	-0.015	-0.962	-0.972	-0.093***	-0.093***	-0.012	-0.013
	(-1.482)	(-1.464)	(-1.657)	(-1.666)	(-7.008)	(-7.073)	(-1.070)	(-1.083)
GROWTH	-0.010	-0.010	0.355	0.361	0.006**	0.006**	0.002	0.002
	(-0.593)	(-0.580)	(1.369)	(1.356)	(2.533)	(2.496)	(1.039)	(1.023)
BTM	-0.054***	-0.054***	-0.299	-0.295	-0.032***	-0.032***	0.002	0.002
	(-7.804)	(-7.876)	(-1.200)	(-1.181)	(-5.618)	(-5.598)	(1.418)	(1.104)
LOSS	0.194***	0.194***	3.661***	3.670***	0.027**	0.027**	0.000	0.000
	(4.252)	(4.211)	(5.050)	(5.061)	(2.605)	(2.600)	(-0.061)	(-0.136)
RESTRUCT	0.223***	0.224***	-0.412	-0.402	0.000	0.000	0.000	0.000
	(8.838)	(8.777)	(-1.343)	(-1.344)	(0.012)	(0.044)	(0.011)	(0.305)
BUSSEG	0.070***	0.071***	0.632***	0.638***	0.005*	0.005*	0.000	0.000
	(3.278)	(3.290)	(3.970)	(3.949)	(1.967)	(1.981)	(-0.411)	(-0.051)
GEOSEG	0.054***	0.054***	-0.130	-0.130	-0.001	-0.001	-0.001	-0.001
	(4.169)	(4.176)	(-1.124)	(-1.129)	(-0.904)	(-0.917)	(-1.452)	(-1.332)
BIG4	0.718***	0.719***	-7.744***	-7.745***	-0.011	-0.011	-0.002	-0.002
	(4.998)	(4.983)	(-8.785)	(-8.934)	(-1.303)	(-1.267)	(-1.257)	(-0.923)
Adjusted R^2	0.84945	0.84947	0.49043	0.48999	0.44068	0.44054	0.08663	0.04669
Observations	33,000	33,000	33,000	33,000	33,000	33,000	7,718	7,718
Year fixed effects	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Industry fixed effects	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

This table reports the results from linear probability models relating auditor responses to the firm's exposure to cryptocurrency as shown in Equation (3). The outcome variable is either (i) the natural logarithm of audit fees in year t ($LNAUFEES_{it}$), (ii) the number of days between a client's fiscal year-end and auditor signature date ($AUDITLAG$), (iii) an indicator variable that equals one if the auditor issues a going-concern opinion to the client in year t and zero otherwise (GCO_{it}), (iv) the percentage of critical audit matters mentioning cryptocurrency-related keywords ($CAMCRYPTO$). *Crypto exposure*$_{it}$ is our variable of interest and is defined as an indicator equals one if the frequency of the cryptocurrency-related keywords appears in Item 1 "Business" ($CRYPTO\_BUS\_EXPOSURE$) and Item 1A "Risk Factors" ($CRYPTO\_RISK\_EXPOSURE$) in year t is positive, and zero otherwise. Table A.1 defines all cryptocurrency-related keywords in detail. All financial variables are winsorized at 1% and 99% levels, except cryptocurrency exposure variables and the percentage of critical audit matters mentioning cryptocurrency-related keywords ($CAMCRYPTO$). We standardize cryptocurrency exposure variables to have standard deviations equal to one. All variables are described in Table A.4. Standard errors are clustered by Fama-French 12 industries. ***, ** and * indicate significance at the 1%, 5% and 10% levels in a two-tailed test.