The Value of Auditor Assurance in Cryptocurrency Trading

Jingyi Qian

jyqian@umd.edu

Robert H. Smith School of Business

University of Maryland

July 15, 2024

This paper is based on my dissertation at Emory University. I thank my dissertation committee chair, Ilia Dichev, and my committee members, Clifton Green, Teri Yohn, and Donny Zhao for their invaluable guidance and support. I am grateful for helpful comments from Leo Barcellos, Kyle Broderick, Nerissa Brown, Sean Cao, Qiang Cheng, Jen Choi, William Ciconte, Givoly Dan, Kai Du, Cassandra Estep, Rebecca Hann, Sterling Huang, Michael Kimbrough, Matthew Lyle, Robbie Moon, Jed Neilson, Gaizka Ormazabal, David Reeb, Nick Seybert, Suhas Sridharan, and workshop participants at Emory University, Georgia Institute of Technology, IESE Business School, National University of Singapore, Penn State University, Singapore Management University, the University of Illinois Urbana-Champaign, and the University of Maryland. I also appreciate Nate Andrew (RSM US) and Gregory Johnson (Rubicon Crypto) for providing helpful institutional insight. Financial support from Goizueta Business School and Robert H. Smith School of Business is gratefully acknowledged.

Electronic copy available at: https://ssrn.com/abstract=4536274

The Value of Auditor Assurance in Cryptocurrency Trading

Abstract

This study examines the value of System and Organization Controls 2 (SOC 2) audits to customers. A SOC 2 audit is a voluntary assurance service provided by an independent CPA over a firm's internal controls relevant to information system security. I use cryptocurrency exchanges, a setting where the lack of customer trust can be particularly acute, to examine whether SOC 2 audits increase customer demand. I find a substantial increase in liquidity following the disclosure of initial SOC 2 audit completion: the trading volume of cryptocurrencies listed on audited exchanges increases by more than 60 percent, and the price impact decreases by approximately 40 percent in the three months after SOC 2 audit disclosure. Exploring the channels through which SOC 2 audits provide value to customers, I find that exchanges with high-quality security measures are more likely to initiate SOC 2 audits, and that continued audits ensure that the quality of security measures remains high. Overall, this study provides novel evidence that SOC 2 audits provide value to customers by sending a credible and positive signal of exchange security, and thus significantly increase customer demand.

JEL Classification: M42, G23, G32

Keywords: System and Organization Controls 2 (SOC 2) Audit, Crypto Exchange, Crypto Trading, Security Measures, Customer Trust

Electronic copy available at: https://ssrn.com/abstract=4536274

1. Introduction

Data security has become a central concern in the current digital era. Firms are constantly confronted with heightened cybersecurity challenges, which mostly arise from the generation of big data and the critical need for internet solutions. To deal with these challenges and provide assurance to customers, companies are increasingly adopting System and Organization Controls 2 (hereafter, SOC 2) audits. A SOC 2 audit is a voluntary assurance service provided by an independent CPA regarding a firm's internal controls over information system security (Schoenfeld [2024]). While existing studies primarily focus on traditional financial statement audits (DeFond and Zhang [2014], Minnis [2011], Lisowsky and Minnis [2020]), the evidence on the value and benefits of SOC 2 audits is limited. This paper attempts to fill this gap by examining whether SOC 2 audits increase customer demand.

I explore the setting of cryptocurrency exchanges, which are trading platforms where customers buy and sell cryptocurrencies. The crypto market has grown to over $2 trillion since 2024 and has over 20,000 cryptocurrencies in circulation today. Cryptocurrency exchanges play a key role in this growth and process the vast majority of crypto transactions. SOC 2 audits are particularly crucial for crypto exchanges because data security issues and the associated loss of customer trust are pervasive in crypto market. As one illustration of these issues, when customers trade their digital assets on cryptocurrency exchanges, the exchange takes custody of the digital assets, which can be lost in case of data breaches.[1] More than 40 exchanges have experienced major hacks and data breaches in the past decade, causing massive financial losses for customers. For example, the then largest crypto exchange Mt. Gox lost approximately 850,000 bitcoins worth more than $400 million in 2014—approximately 7 percent of the bitcoins in circulation. Note that,

[1] The blockchain itself cannot be hacked. However, most transactions on crypto exchanges are off the blockchain and are only recorded within the exchange's own system. See detailed explanation in section 2.1.

Electronic copy available at: https://ssrn.com/abstract=4536274

unlike most banks, cryptocurrency exchanges are not insured by governments, so customers have no recourse beyond the exchange in recovering losses from security breaches. As crypto investors learn about the lack of regulation and the related risks of deceptive disclosures from crypto exchanges, they may recognize the benefits of SOC 2 audits.

Because a SOC 2 audit is conducted by an independent CPA to assure the effectiveness of internal controls over information system security, it likely boosts customer trust about exchange security operations. Thus, I predict that SOC 2 audits increase customer demand for trading on the exchange. Specifically, I examine whether trading volume and liquidity increase significantly for cryptocurrencies listed on exchanges after the disclosure of initial SOC 2 audit completion.

I first select a sample of crypto exchanges that have conducted SOC 2 audits (SOC 2 exchanges). Because crypto exchanges differ significantly in the number and kinds of cryptocurrencies offered, I conduct the analyses at the exchange*cryptocurrency pair level (Li et al. [2021]). My treatment sample includes 197 cryptocurrency pairs listed on SOC 2 exchanges. To provide preliminary evidence on the economic significance of SOC 2 audits for trading on the exchange, I analyze the average daily trading volumes of the treatment sample over a 12-month window around the initial SOC 2 audit disclosure. The results reveal that the month immediately following the disclosure experiences the highest trading volume, exceeding the average daily volume of the six-month pre-disclosure period by over 100 percent. The magnitude tapers off after the first month but is still economically meaningful. The average daily volume in the six-month post-disclosure period is 60 percent higher than in the pre-disclosure period. These findings suggest that SOC 2 audits are economically significant events for crypto exchanges, indicating a substantial impact on customer demand.

Electronic copy available at: https://ssrn.com/abstract=4536274

I employ a difference-in-differences research design to rigorously examine whether SOC 2 audits influence customer demand. Specifically, I study whether the trading volume and liquidity of cryptocurrencies listed on SOC 2 exchanges (treatment sample) significantly increase in the three months following the SOC 2 audit disclosure, compared to cryptocurrencies listed on non-SOC 2 exchanges (control sample). To construct a control sample of cryptocurrency pairs of similar characteristics, I search among trading pairs of the same currency type listed on non-SOC 2 exchanges and select (with replacement) the pair with the closest trading volume prior to the audit disclosure. The full sample comprises 392 cryptocurrency pairs traded on 58 crypto exchanges in the three months before and after the SOC 2 audit disclosure. Consistent with the preliminary evidence, I find that the disclosure of initial SOC 2 audit completion is associated with a more than 60 percent increase in the trading volume and approximately a 40 percent decrease in price impact of cryptocurrency pairs listed on SOC 2 exchanges in the three months following the audit disclosure. The findings suggest that SOC 2 audits significantly enhance exchange liquidity. Customers value SOC 2 audits as a reliable assurance of the exchange's high-quality security measures, making them more likely to trade on the exchange as a result (Bonetti and Ormazabal [2023], Du and Wu [2019]). Because crypto exchanges generate a large portion of revenues from trading fees, the significant increase in trading volume yields substantial benefits to audited exchanges in terms of revenue and cash flow. Taking Coinbase as an example, the increase in trading volume corresponds to an increase in monthly revenue of approximately $18 million.

The critical assumption in a difference-in-differences design is the parallel trend assumption, which posits that in the absence of SOC 2 audit disclosure, the change in trading volume and liquidity for the treatment sample would not have been different from the control sample. I conduct diagnostic test of this assumption by examining the pre-trends in trading volume and price impact

Electronic copy available at: https://ssrn.com/abstract=4536274

between the treatment and control samples before the SOC 2 audit disclosure. In support of this assumption, I find that the treatment and control trading pairs have similar trends in trading volume and price impact before the disclosure of audit completion. Moreover, the decision to obtain a SOC 2 audit is unlikely to be random. To control for exchange characteristics that might vary with both cryptocurrency trading and the decision to obtain SOC 2 audits, I create a propensity score matched sample based on both exchange and cryptocurrency characteristics. For each exchange-year, I calculate the propensity to conduct SOC 2 audits based on lagged exchange characteristics. For each SOC 2 exchange, I then select (with replacement) 20 non-SOC 2 exchanges with the closest propensity scores. This creates a sample of non-SOC 2 exchanges from which I select my control sample of cryptocurrency pairs. Following the procedure for the main test, I then search within trading pairs of the same currency type listed on the matched control exchanges and select (with replacement) the pair with the closest trading volume before audit disclosure. I rerun the analyses of trading volume and liquidity and find that my results are robust to this matching method.

I also investigate whether the effect of SOC 2 audits varies over time and across different cryptocurrencies. My findings indicate that the impact on trading and liquidity is most pronounced in the first month after SOC 2 audit disclosure and diminishes over the following two months. This pattern aligns with previous research suggesting that cryptocurrency trading is driven by attention (Brown et al. [2015], Liu and Tsyvinski [2021], Sockin and Xiong [2023]). Additionally, I explore the cross-sectional variation in exchange trading and liquidity by comparing cryptocurrencies with high and low trading volumes/market capitalizations. The results show that the improved trading and liquidity are not confined to a specific subset of cryptocurrencies, indicating that SOC 2 audits have a similar effect on all cryptocurrencies listed on SOC 2 audited exchanges.

Electronic copy available at: https://ssrn.com/abstract=4536274

Furthermore, I explore the channels through which SOC 2 audits provide value to customers. One possible channel relates to crypto exchanges' choice to conduct SOC 2 audits, i.e., the "signaling channel" (Kausar et al. [2016]). Prior research suggests that the decision to have voluntary audits is determined by a cost-benefit trade-off (Allee and Yohn [2009], Badertscher et al. [2023], Dedman et al. [2014], Lennox and Pittman [2011], Lisowsky and Minnis [2020]). For exchanges with high-quality security measures, the cost of meeting the SOC 2 criteria (hereafter, indirect cost) is significantly lower. Therefore, I posit that crypto exchanges with better security practices are more likely to initiate SOC 2 audits as a positive signal to customers about the quality of their security. To test this conjecture, I examine factors associated with crypto exchanges' decision to get audited and find that exchanges with high-quality security measures in the past have a significantly higher propensity to do so. Moving from the average security level of non-SOC 2 exchanges to the significantly higher security level of SOC 2 exchanges, the probability of getting SOC 2 audits increases by 7.52 percent.

Another potential channel is that the audit process *itself* improves exchange security operations, i.e., the "real effects" channel (Minnis [2011]). If auditors identify control deficiencies, managers must remediate the deficiencies to obtain SOC 2 compliance. Thus, the audit process itself may increase managers' cybersecurity awareness and improve the security measures. Using a difference-in-differences research design, I do not find strong evidence that crypto exchange security practices change significantly after SOC 2 audits.

Combining the findings from both channels suggests that crypto exchanges opt for SOC 2 audits only when they anticipate the benefits exceed the costs, including audit fees and management effort. A suitable time for exchanges to undergo the audit is as they grow and achieve a high level of security, thus reducing the indirect cost of SOC 2 compliance. Consequently, SOC

Electronic copy available at: https://ssrn.com/abstract=4536274

2 audits provide value for customers by sending a credible and positive signal about exchange security and quality. Additionally, since SOC 2 audits must be conducted periodically, continued audits help exchanges to maintain high security standards.

This study makes three main contributions. First, it provides novel insight into the benefits of SOC 2 audits, which are increasingly adopted but have received limited attention from prior literature (DeFond and Zhang [2014], Minnis [2011], Lisowsky and Minnis [2020], Schoenfeld [2024]). A SOC 2 audit is different from a traditional financial statement audit in that it provides assurance regarding an organization's internal controls over *information system security*, which speaks to the business operations, whereas a financial statement audit provides assurance over *the reliability of financial reporting*. This study enhances our understanding of SOC 2 audits and suggests that they build customer trust and increase customer demand. In addition, I provide evidence of the channels through which SOC 2 audits bring value to customers: SOC 2 audits send a positive signal about exchange security measures, which helps to reduce information asymmetry between exchanges and customers. Moreover, the continued execution of such audits ensures that the quality of the exchange security operations remains high. Overall, this study sheds light on the broader value of auditor assurance outside of financial statement auditing.

Second, this paper contributes to the auditing literature by documenting the role of customers in voluntary audits. Extant research on the voluntary financial reporting of private firms primarily focuses on the demand from capital providers (Allee and Yohn [2009], Barton and Waymire [2004], Lisowsky and Minnis [2020], Minnis [2011]), which have significant influence over whether the firm obtains an audit. Because a crypto exchange has millions of customers, individual customers are unlikely to have sufficient leverage over an exchange's audit decision. However, I

Electronic copy available at: https://ssrn.com/abstract=4536274

provide novel evidence on the role of customers in firms' voluntary SOC 2 audit decisions via their collective demand for the firm's services.

Third, this study explores a severe form of information asymmetry between firms and customers by using cryptocurrency exchanges (Costello [2013]). The setting of crypto exchanges is of inherent interest to accounting researchers. The crypto market has become one of the most important economic sectors in the past decade, and crypto exchanges play a key role in the market by providing access and liquidity to customers. The severe information asymmetry problem stems from several distinct features of the crypto market: the complexity of blockchain technology, customer confusion about exchange operations, the almost complete absence of regulations and customer protection, and the lack of established and credible disclosure channels for crypto exchanges. My study shows that SOC 2 audits help to reduce information frictions by offering trustworthy verification from CPAs, shedding light on the important role that CPAs could play in less regulated emerging markets.

I note two caveats to my study. First, theories on audit as a costly signal (Spence [1973], Jensen and Meckling [1976]) suggest that the value of SOC 2 audits in boosting customer demand likely extends beyond crypto exchanges, although the magnitude of the impact may vary. Due to the severe information asymmetry between crypto exchanges and their customers, the value of SOC 2 audits is likely higher for crypto exchanges compared to other firms. For instance, public companies have a more transparent information environment, so the benefits of SOC 2 audits might be less pronounced for them. Second, to study the question of whether SOC 2 audits provide value to customers, it would be impractical to use a quasi-experimental setting that provides random assignment of SOC 2 audits to crypto exchanges because audits could affect firm value through two channels: the signaling channel (Kausar et al. [2016]) and the real effects channel

Electronic copy available at: https://ssrn.com/abstract=4536274

(Minnis, 2011). Since I document that the choice to have SOC 2 audits is not random but is rather endogenously determined by exchange characteristics (i.e., the signaling channel), there is a lack of as-if random variation in the explanatory variable (SOC 2 audits). In this case, the estimated causal effect from a DiD design will not represent an estimate of the average treatment effect (ATE), which is the expected causal effect on a crypto exchange selected at random from the population. Instead, my findings speak to the value of SOC 2 audits to exchanges that voluntarily perform the audit.[2]

The remainder of the paper proceeds as follows. Section 2 discusses the institutional background of crypto exchanges and SOC 2 audits. Section 3 reviews the prior literature and formalizes my hypothesis. Section 4 discusses the data, sample selection, and descriptive statistics. Section 5 examines the effect of SOC 2 audits on exchange trading and liquidity. Section 6 studies the channels through which SOC 2 audits create value. Section 7 concludes.

2. Institutional Background

2.1 Cryptocurrency exchanges

A blockchain is a decentralized ledger of all transactions across a peer-to-peer network. Transactions are recorded in a block that is linked to previous blocks using cryptography, making the whole system a chain of blocks, which is therefore called "blockchain." Because all peers in the blockchain network could validate transactions, the system does not involve third parties to ensure validity and trust. To incentivize peers to validate transactions, they are rewarded cryptocurrencies, a process known as "mining." A cryptocurrency is a digital currency working as

[2] See Armstrong et al. (2022) for an excellent discussion of the two channels through which audits affect firm value, employing both quasi-experimental and non-experimental methods, and how to interpret the results from these different methods.

Electronic copy available at: https://ssrn.com/abstract=4536274

a medium of exchange (Anderson et al. [2022]). With the development of blockchain technology comes the demand for cryptocurrencies. As of February 2022, more than 10,000 cryptocurrencies exist, and the total cryptocurrency market capitalization is around $1.8 trillion, roughly 8 percent of the US GDP in 2021.

Cryptocurrency exchanges are platforms on which people buy and sell cryptocurrencies against fiat currencies or other digital assets. Crypto exchanges serve as a vital intermediary between buyers and sellers and greatly facilitate trade in the crypto market.[3] [4] They generate revenue from several sources, including brokering trades, market making, and custody services. Trading fees are typically a percentage of the trade value and depend on the size of the trade, the trader's monthly volume, and whether it is a maker or taker order.[5] Even though trading fee schedules vary across crypto exchanges, typically maker orders are charged lower fees than taker orders and high-volume trades are charged lower fees to incentivize the provision of liquidity. When traders deposit (withdraw) their assets to (from) crypto exchanges, fees apply as well. These transaction fees constitute a major part of crypto exchanges' total revenue.[6] For example, Coinbase's transaction revenue accounts for 96 percent of total net revenue in 2020 and 93 percent

[3] This paper focuses specifically on centralized crypto exchanges (CEX). Another type of crypto exchange is the decentralized exchange (DEX), a peer-to-peer platform on which transactions occur directly on blockchains. Centralized exchanges play the dominant role in the crypto market, with the trading volume more than 10 times higher than that of decentralized exchanges in 2021.

[4] A common misconception is that blockchains eliminate the need for intermediaries in the financial market. It is true that within the blockchain ecosystem third-party intermediaries are unnecessary because everyone can validate on-chain transactions—for example, sending bitcoins in the bitcoin blockchain network. However, if the blockchain system needs to interact with other parties (e.g., using bitcoins to buy other services/products/currencies that are not in the bitcoin network) intermediaries are still needed because the services/products/currencies provided are off the blockchain.

[5] Crypto exchanges utilize a maker-taker fee model. Traders can place either a market order or a limit order to a crypto exchange's order book to interact with other traders. A market order is an order which allows traders to buy or sell cryptocurrency instantly at the market price. Doing so takes liquidity from the exchange and is therefore called a "taker order". A limit order is an order which allows traders to set a specific price at which they intend to buy or sell cryptocurrency, which provides liquidity to the exchange and is therefore called a "maker order".

[6] For smaller and newer crypto exchanges, transaction fees may constitute a smaller proportion of total revenue because they have lower trading volume and thus generate revenue from other sources, such as listing fees of crypto coins and tokens.

Electronic copy available at: https://ssrn.com/abstract=4536274

in 2021 (Coinbase [2021]). Besides the role of brokering trades between buyers and sellers, some crypto exchanges serve as market makers and charge a spread between the market price and the quoted price. Crypto exchanges also provide digital wallet services, which safeguard clients' assets and charge subscription and service fees. Appendix A uses Coinbase as an example to illustrate crypto exchanges' revenue sources and fee schedules.

An important feature of centralized crypto exchanges is that they are custodians of customers' assets. Even though blockchain technologies enable secure and immutable transactions on the blockchain, trading on centralized crypto exchanges is not as secure as one might think. To see how trading on centralized exchanges involves the blockchain network, when customers deposit (withdraw) their digital coins to the exchange (their own digital wallets), transactions are broadcasted and recorded on the blockchain. However, most transactions that take place on the exchange are not recorded on the blockchain at all, but rather within the exchange's own system. For instance, if user A buys bitcoins from user B, their account balances on the exchange will be changed, but the exchange will still be holding the bitcoins for user A unless he or she withdraws. In other words, centralized crypto exchanges take control of customers' digital assets and customers are left only with a claim for the value of the assets.

Because centralized crypto exchanges store and protect large amounts of sensitive customer information, including digital assets' private keys and user identity, they are especially susceptible to cyberattacks and data breaches, which can generate huge losses for customers.[7] Over 40 exchanges have been hacked in the past 10 years, including popular ones like Binance and Bithumb. In one of the most recent hacks in 2022, Binance lost 2 million BNB tokens, which were worth

[7] Private keys prove ownership of cryptocurrency and allow owners to transfer cryptocurrency to others. So, safeguarding digital assets is essentially safeguarding private keys. If hackers infiltrate exchange systems and obtain clients' private keys, they can use private keys to transfer digital assets to themselves, allowing the hackers to steal cryptocurrencies from crypto exchanges.

Electronic copy available at: https://ssrn.com/abstract=4536274

$570 million at that time. Even worse, consumer protection has been very limited in the crypto market. Governments have not insured any crypto exchanges, so they have no obligation to step in and recover losses from hacks. Therefore, the lack of customer trust in data security has become a serious issue for crypto exchanges.

To address customer concerns, crypto exchanges need credible channels to disclose security information to the market. However, they do not have established channels to disclose in the absence of regulatory mandates.[8] Although exchanges could voluntarily disclose their security measures, this option could easily result in cheap talk. For example, QuadrigaCX, which was the largest crypto exchange in Canada by late 2018, was not registered with any securities regulator. It was run entirely by Gerald Cotten, the CEO of QuadrigaCX, so it lacked a proper system of internal controls. Even though QuadrigaCX disclosed to its customers on Reddit that it used "the tried and tested method of storing 99% coins in cold storage," it turns out that the statement was untrue and misleading.[9] Over the years, Cotten misappropriated customers' assets and ran a Ponzi scheme to cover losses. Because he was the only one controlling clients' private keys, after his mysterious death in 2019, around C$215 million was lost for 76,000 clients (Ontario Securities Commission [2022]). In summary, lack of customer trust in data security is particularly acute for crypto exchanges, generating demands for credible third-party assurance like SOC 2 audits.

2.2 System and Organization Controls 2 (SOC 2) Audits

[8] Some countries require crypto exchanges to register as money service businesses (MSBs) and obtain exchange licenses, while others do not (Tang and Zhang [2021]). In the United States, crypto exchanges are required to register as MSBs with Financial Crimes Enforcement Network (FinCEN) and obtain money transmitter licensing in each state, primarily for combatting money laundering and terrorist financing. However, the rules imposed on either MSBs or money transmitters are not as strict as the rules for broker-dealers, so investor and consumer protection have been very limited.

[9] A cold storage (wallet) is a physical device that keeps cryptocurrencies completely offline and is therefore less likely to be hacked.

Electronic copy available at: https://ssrn.com/abstract=4536274

SOC 2 audits fall under the Statement on Standards for Attestation Engagements (SSAE) No. 18, which was released by the American Institute of Certified Public Accountants (AICPA) in 2016 (AICPA [2016]). According to the AICPA definition, a SOC 2 report is "a report on controls at a service organization relevant to security, availability, processing integrity, confidentiality, or privacy" (AICPA [2022]).[10] In essence, SOC 2 audits focus on the security of an organization's information system.[11] The goal of a SOC 2 audit is to help service organizations build trust and confidence with their customers. Although SOC 2 audits are not required by law, the increasing trend of third-party outsourcing, like payroll processing and customer relationship management (CRM), has fueled the need for SOC 2 audits.

A SOC 2 audit is based on five Trust Service Criteria (TSCs): security, availability, processing integrity, confidentiality, and privacy. These criteria do not specify prescriptive controls that organizations should have. Instead, they stipulate high-level objectives and require auditors to collect evidence on the specific controls in place to meet those criteria. See Appendix B for the AICPA definitions of the criteria. Among the five criteria, security is the baseline criterion and is required for every SOC 2 audit. It focuses on controls relevant to whether the information system could be compromised by unauthorized access. Because crypto exchanges manage large amounts of customer assets, they are particularly vulnerable to hackers' attacks, making the security of data and information systems their top priority. The other four criteria are optional, but some might also apply to crypto exchanges. For example, the availability criterion asks if the exchange has disaster recovery and business continuity plans. As cyberattacks could easily drive exchanges into bankruptcy, having insurance funds is a good practice against losses.

[10] A service organization is a firm that provides a service to its customers.
[11] An organization should define the scope of its information system, which could be the entire organization, a business unit, or a product line.

Electronic copy available at: https://ssrn.com/abstract=4536274

The privacy criterion asks if the exchange has controls to protect users' personal information. Crypto exchanges collect sensitive personal information like Social Security Numbers (SSN). As such, customers want assurances that their personal information is managed and protected properly. In practice, crypto exchanges have latitude in choosing which criteria to include in their SOC 2 audits depending on their business environments—but the security principle is a must.

SOC 2 audits are performed by CPAs. To do so, CPA firms increasingly hire IT auditors with expertise in information security and information technology (Bauer et al. [2019], Schoenfeld [2024]).[12] They also offer education programs to equip auditors with the necessary skills.[13] Like financial statement audits, SOC 2 audits must be conducted periodically.[14] During the audit, auditors collect evidence and perform tests to make sure the controls in place meet the Trust Service Criteria. For example, a firm should maintain control over logical access to its information system.[15] To do so, the firm could require two-factor authentication when users log in to the network from remote locations. To make sure the control objective is met, auditors could interview the system manager, inspect the authentication configuration protocol, and attempt to log in from a remote location themselves. If auditors identify material control gaps, the firm must remediate the gaps to achieve SOC 2 compliance.

The cost of a SOC 2 audit varies widely depending on multiple factors, including the complexity of the information system, the number of Trust Services Criteria included, the size of

[12] IT auditors usually hold university degree in management information system or accounting and qualifications related to IT security, such as Certified Information Systems Auditor (CISA), Certified Information Systems Security Professional (CISSP), or Certified in Risk and Information Systems Control (CRISC).
[13] For instance, Ernst & Young provides a tech MBA to educate employees on technology, including artificial intelligence (AI), blockchain and robotic process automation (RPA).
[14] There are two types of SOC 2 audits: Type 1 and Type 2. A Type 1 audit examines whether the *design* of internal controls is effective as of a point-in-time, whereas a Type 2 audit covers whether the *design and operation* of controls are effective over a period of time, usually six months or one year. Typically, a Type 1 audit is the starting point for a Type 2 audit.
[15] Logical access refers to interactions with hardware through remote access.

Electronic copy available at: https://ssrn.com/abstract=4536274

the organization, the number of locations, and so forth. The audit fee (direct cost) is typically between $100K to $250K per year but could go up to millions of dollars for large firms with complex information systems. But perhaps more importantly, the indirect cost of meeting SOC 2 compliance is much more substantial. Firms need to dedicate ample time and resources to the audit, including preparation for the audit, walkthroughs with auditors, providing audit evidence, and remediation of control gaps. Some firms even hire dedicated personnel to take charge of the audit.

The final output of the audit is a SOC 2 report. Typically, a SOC 2 report includes management assertion, auditor's opinion, description of the service system relevant to the Trust Service Criteria, and description of tests of controls and results of tests.[16] According to the AICPA, SOC 2 reports cannot be publicly distributed and can only be shared with intended users, such as customers, auditors, and regulators. When crypto exchanges have completed SOC 2 audits for the first time, they typically post blogs on their websites, Twitter, or Medium.com. They also list SOC 2 certifications on the home page. See Appendix D for Gemini's SOC 2 audit disclosures.

3. Literature Review and Hypothesis Development

Prior research has examined firms' voluntary financial audits in the absence of regulatory requirements. The literature suggests that firms' voluntary audits are driven by the need to mitigate agency problems and optimize contracts with outside stakeholders, and the incentive increases with the severity of the agency costs (Armstrong et al. [2010], Bushman and Smith [2001], Watts [1977], Jensen and Meckling [1976]). In addition, the literature provides evidence of the forces that create demand for audited financial statements, including firm size, growth opportunities, ownership dispersion, and the use of external debt and trade credit (Allee and Yohn [2009],

[16] The types of SOC 2 audit opinions include a qualified, unqualified, disclaimer or adverse opinion.

Electronic copy available at: https://ssrn.com/abstract=4536274

Badertscher et al. [2023], Barton and Waymire [2004], Dedman et al. [2014], Lisowsky and Minnis [2020]).

The extant literature also examines the benefits from voluntary financial reporting and audits. Allee and Yohn [2009] use a sample of privately held small firms from the National Survey of Small Business Finances (NSSBF) and find that firms with audited financial statements enjoy greater access to credit, and firms with accrual-based financial statements receive a lower cost of credit. Using a sample of larger private firms, Minnis [2011] documents that voluntary audits of financial statements significantly reduce firms' cost of debt and provide more useful information to lenders. Kausar et al. [2016] use the setting of U.K. private firms where the choice to voluntarily obtain audits became available to external financiers after 2004. They find that the choice to undergo an audit reveals information to financiers, thereby reducing financing constraints. These studies show that the demand for financial statements comes from lenders and that voluntary financial reporting reduces firms' cost of debt. Other studies document the effect of equity investors' demand. Focusing on the regime before mandatory financial reporting, Barton and Waymire [2004] provide evidence that managers voluntarily presented high-quality financial reporting to reduce the agency and information cost between managers and investors, and investors experienced significantly smaller losses during the 1929 market crash. Overall, the prior literature on voluntary audits primarily examines the benefit of financial statement audits to capital providers.

In contrast to traditional financial statement audits, SOC 2 audits provide benefits to *customers*. Therefore, I examine the value and benefits of SOC 2 audits to customers. This examination is important because, despite the increasing adoption and importance, research on the value of SOC 2 audits is rather limited. Navarro and Sutton [2021] use experiments to study the effect of voluntary cybersecurity risk management (CyRM) on investors' judgments and decisions,

Electronic copy available at: https://ssrn.com/abstract=4536274

but they do not directly focus on SOC 2 audits. Most closely related to my study is Schoenfeld [2024], which examines the benefits and costs of SOC audits for the S&P 500 firms. It finds that 29 percent of the sample firms have received SOC audits and provides characteristics of firms conducting SOC audits, including industry, firm size, and exposure to technology. While Schoenfeld [2024] examines a whole suite of SOC audits and does not distinguish between different types of audits within the SOC framework, my study focuses exclusively on SOC 2 audits.[17] Moreover, Schoenfeld [2024] examines the S&P 500 firms, which are big and established firms with transparent information environments, whereas I study cryptocurrency exchanges, most of which are privately held and suffer from severe information problems. Overall, while these studies provide important insight into SOC 2 audits, the benefits and value afforded to customers remain somewhat opaque, I aim to fill this gap using crypto exchanges' SOC 2 compliance.

Conducting SOC 2 audits likely reduces the information asymmetry between crypto exchanges and customers. For outside stakeholders like customers, it is difficult to verify and examine the quality of exchange security measures. Because a SOC 2 audit is conducted by an independent CPA, it provides trustworthy third-party assurance of exchange security operations (Bonetti and Ormazabal [2023], Bourveau et al. [2024]). Moreover, SOC 2 audits require substantial time and resources and must be conducted periodically, likely sending a positive message about the management's efforts toward security and the quality of security measures.[18]

[17] Within the SOC reporting framework, SSAE18 provides guidelines for a variety of attestation for service organizations, including SOC 1, SOC 2, and SOC 3. A SOC 1 audit focuses on internal controls relevant to *user entities' financial reporting*. For example, a payroll processing company's internal controls could directly affect its user entities' financial statements; therefore, the user entities and their auditors would be interested in knowing relevant internal controls at the payroll processing company. A SOC 3 report is a public distribution version of a SOC 2 report.

[18] Conversations with a crypto investment advisory firm suggest that institutional customers consider crypto exchanges' SOC 2 audits as a strong signal about the efforts devoted to security and compliance. Some institutional customers are not willing to partner with crypto exchanges that haven't completed SOC 2 audits. Also see Appendix C for anecdotal evidence of customer reactions to Crypto.com SOC 2 audit disclosure, including the comments on Reddit and the price surge of Crypto.com exchange native token CRO.

Electronic copy available at: https://ssrn.com/abstract=4536274

Thus, a SOC 2 audit may boost customer trust and confidence and attract more customers to the platform, likely improving exchange trading volume and liquidity. Summarizing, my main hypothesis is as follows:

Hypothesis: *Trading volume and liquidity of listed cryptocurrencies increase significantly after crypto exchanges disclose initial SOC 2 audit completion.*

Note that the prediction is subject to some caveats. If customers do not fully understand the importance of exchange security, they might not appreciate the value of SOC 2 audits. Moreover, if exchanges' SOC 2 audit disclosures attract limited attention from customers, I might fail to observe an increase in trading volume and liquidity on audited exchanges.

4. Data, Variables, and Descriptive Statistics

4.1 Data and sample

I first search and compile a list of crypto exchanges that have conducted SOC 2 audits as of February 2022 and the announcement dates of audit completion disclosures. Table 1 lists the sample of SOC 2 exchanges and a summary of the information disclosed.[19] Gemini is the first crypto exchange to obtain SOC 2 Type 1 audit, in January 2019, followed by Gemini and Coinbase's completion of SOC 2 Type 2 audits in 2020, and ItBit and Crypto.com's completion in 2021. To eliminate the impact of potentially confounding events, I review each exchange's news and press webpage to ensure there were no significant events occurring around the time of the

[19] Even though Bittrex completed a SOC 2 audit in 2021, it is excluded from my sample because of the data measurement error. The Bittrex exchange has 2 trading platforms: Bittrex and Bittrex Global. Bittrex is a US exchange serving US customers, while Bittrex Global is a European exchange serving non-US customers. The platform that completed SOC 2 audit is Bittrex, rather than Bittrex Global. However, since both platforms share a liquidity pool, their trading data are aggregated and there is no way to segregate the trading data between them. All trading pairs listed on Bittrex except BADGER-USD are listed on Bittrex Global as well, so I cannot find a sample of trading pairs that are listed only on Bittrex. Hence, Bittrex's trading data contain too much measurement error and cannot fairly represent the sole trading volume of the Bittrex platform that completed SOC 2 audits.

Electronic copy available at: https://ssrn.com/abstract=4536274

audit completion disclosure. As SOC 2 audits must be conducted on a regular basis, I confirm that each SOC 2 exchange continues to receive SOC 2 audits in later years by either directly contacting the exchange or searching its website. The scope of the audit can be either the exchange trading platform or the asset custody, which holds and protects customers' assets. The most common Trust Services Criteria applied include security, availability, and confidentiality, of which security is the required criterion. All audits have been conducted by well-established auditing firms, including Deloitte, Ernst & Young, and Grant Thornton.

<Insert Table 1 here>

Like foreign exchanges, crypto exchanges offer exchange rates for cryptocurrency pairs. For instance, the exchange rate for the BTC/USD pair on Coinbase, for which BTC is the base currency and USD is the quote currency, tells how many US dollars are needed to buy one bitcoin on Coinbase.[20] As crypto exchanges vary greatly in terms of the number and types of trading pairs offered, I follow the prior literature and choose the unit of analysis at the exchange*currency pair level (Li et al. [2021]).

I obtain cryptocurrency pair daily Open/High/Low/Close/Volume (hereafter, OHLCV) data for cryptocurrency pairs traded on all centralized exchanges from CryptoCompare. For each exchange*trading pair, the data provide daily open, high, low, close, and trading volume in both base currency and quote currency. CryptoCompare data is of high quality (Alexander and Dakos [2020]) and is widely used by practitioners and researchers (Borri and Shakhnov [2021], Makarov and Schoar [2020], Augustin et al. [2021]).[21] In addition, I download the data for Crypto.com from

[20] See the definition of base currency and how to read crypto trading pairs in the links below.
https://www.gemini.com/cryptopedia/glossary#base-currency
https://www.coindesk.com/learn/what-are-crypto-trading-pairs/

[21] To verify CryptoCompare data accuracy, I construct OHLCV data for some exchanges using transaction data downloaded directly from exchanges' API. In all cases, the self-constructed OHLCV data are the same as the data from CryptoCompare.

Electronic copy available at: https://ssrn.com/abstract=4536274

its own API because CryptoCompare only provides the data for Crypto.com as of December 2021, which is after Crypto.com's audit completion.

As the price and volume data are expressed in units of quote currencies and cryptocurrency pairs have different quote currencies, I convert the OHLCV data into USD to make the data comparable across different pairs. Hence, I obtain daily spot exchange rates between fiat currencies and USD from Datastream and exchange rates between cryptocurrencies and USD from CryptoCompare. For each cryptocurrency pair traded on exchange j on day t, I convert the OHLCV data into USD based on the daily spot exchange rate between the quote currency (either fiat or crypto) and USD.

My treatment sample includes cryptocurrency pairs listed on SOC 2 exchanges in the three months before and after audit disclosure. Detailed sample selection procedures are presented in Table 1 Panel B. There are 197 cryptocurrency pairs listed on Gemini, Coinbase, ItBit, and Crypto.com.

To construct a control sample of cryptocurrency pairs traded on non-SOC 2 exchanges, I conduct matching based on the characteristics of cryptocurrency pairs. Specifically, for each trading pair listed on SOC 2 exchanges, I search within trading pairs of the same currency type listed on non-SOC 2 exchanges and select (with replacement) the pair with the closest trading volume in the three months before audit disclosure by using mahanalobis matching (Blankspoor [2019], Lester [2019], Michels [2017]). For example, for the BTC-USD pair listed on Gemini, I search within all BTC-USD pairs on non-SOC 2 exchanges and select the pair with the closest trading volume in the three months before Gemini's audit disclosure. Matching on currency type, time, and trading volume helps to control for characteristics of cryptocurrency pairs and common shocks in the crypto market. To further ensure good matches, I drop pairs with mahanalobis

Electronic copy available at: https://ssrn.com/abstract=4536274

distance scores greater than the 99th percentile of the score distribution. My control sample includes 195 currency pairs listed on 56 non-SOC 2 exchanges.

Following prior studies (Augustin et al. [2021], Borri and Shakhnov [2021]), I only keep observations with positive OHLCV values. To minimize the effect of potential data errors and extreme values, I exclude the top and bottom one percent of the data and drop observations with daily log returns (in absolute value) greater than 200 percent.

4.2 *Variable definitions and descriptive statistics*

I compute two measures to empirically gauge whether SOC 2 audit completion attracts more customers to the exchange. First, I define *Trading Volume* as the natural logarithm of the average daily trading volume in USD of cryptocurrency pair i listed on exchange j in month t.

$$Trading\ Volume_{ijt} = ln\ (\frac{1}{T}\sum_{\tau=1}^{T} \$Vol_{ij\tau}) \qquad (1)$$

Where $\$Vol_{ij\tau}$ is the daily trading volume in USD of currency pair i on exchange j at day τ, and T is the number of trading days for pair i on exchange j in month t.

Second, I calculate the *Amihud Ratio* as the proxy for price impact, that is, the price movement associated with one dollar of trading volume. Thus, the lower the *Amihud Ratio*, the lower the price impact. If SOC 2 audits improve cryptocurrency pairs' liquidity, we should observe a lower *Amihud Ratio* after audit disclosure. *Amihud Ratio* is defined as the natural logarithm of the average of daily absolute returns divided by daily trading volume in USD for cryptocurrency pair i on exchange j in month t (Amihud [2002]). The formal expression is

$$Amihud\ Ratio_{ijt} = ln\ (\frac{1}{T}\sum_{\tau=1}^{T} \frac{|ret_{ij\tau}|}{\$Vol_{ij\tau}}) \qquad (2)$$

Where $ret_{ij\tau}$ is the daily return of currency pair i on exchange j at day τ. Both the *Trading Volume* and *Amihud Ratio* are log-transformed because they are highly skewed.

Electronic copy available at: https://ssrn.com/abstract=4536274

The full sample (treatment and control) includes 392 cryptocurrency pairs traded on 58 crypto exchanges in the three months before and after the disclosure of SOC 2 audit completion. Descriptive statistics of the full sample are reported in Table 2 Panel A. Since cryptocurrencies are traded 24 hours a day, 7 days a week, the maximum number of daily observations per month is 31. Cryptocurrency pairs' average daily trading volume varies from $2,075 to $141 million, indicating a large variation in trading volume and liquidity across currency pairs. In Panels B and C, I compare the difference between the treatment and control samples before and after audit disclosure, respectively. Panel B shows that the treatment and control samples are not statistically different in terms of *Trading Volume* and *Amihud Ratio*. In Panel C, the average *Trading Volume* (*Amihud Ratio*) of the treatment sample is significantly higher (lower) than that of the control sample, providing preliminary evidence that completing a SOC 2 audit is associated with greater trading volume and liquidity.

<Insert Table 2 here>

5. The Effect of SOC 2 Audits on Exchange Trading and Liquidity

In this section, I first provide some preliminary evidence of the significant impact of SOC 2 audits on exchange trading and then present more rigorous analyses by using a difference-in-differences research design.

5.1 Preliminary evidence

To provide preliminary evidence on whether SOC 2 audits increase customer demand for trading on audited exchanges and, if so, the extent of such increase, I compare the magnitudes of treatment cryptocurrency pairs' trading volumes in the six months before and after SOC 2 audit disclosure. Specifically, I take treatment pairs' average daily trading volumes for each month and

Electronic copy available at: https://ssrn.com/abstract=4536274

calculate an average of all pairs' average daily trading volumes. I plot the 12 monthly averages in Figure 1. Most markedly, the first month after audit disclosure has the highest average daily trading volume of $7.6 million over the 12 months, and the magnitude is significantly higher than the volumes in the pre-disclosure period at around $3 million to $4 million. After the first month, the average daily trading volumes decrease slightly to around $5 million to $6 million, but the magnitudes are still significantly higher than those before the audit disclosure. The average daily trading volumes in the six months after audit disclosure are on average 60 percent higher than those before the disclosure. Overall, the patterns in Figure 1 show that SOC 2 audits are economically significant events for crypto exchanges.

<Insert Figure 1 here>

Even though this test provides evidence of the economic significance of SOC 2 audits, cryptocurrency trading is also affected by other factors besides SOC 2 audits, including cryptocurrency characteristics and the general crypto market conditions. To control for the effect of these factors, I conduct the main analyses using a difference-in-differences research design, which is detailed in the next section.

5.2 Research Design of the main analyses

I use a difference-in-differences research design that compares the change in trading and liquidity of cryptocurrency pairs listed on SOC 2 exchanges in the three months before and after the disclosure of initial audit completion to that of non-SOC 2 exchanges (Amiram et al. [2017], Armstrong et al. [2012], Chordia et al. [2018], Schipper and Thompson [1983]). Specifically, I employ a stacked difference-in-differences design that creates a panel of treatment and control samples for each event and forms the final sample by stacking all panel samples together (Gormley and Matsa [2011]). Compared to the generalized difference-in-differences design (Bertrand and

Electronic copy available at: https://ssrn.com/abstract=4536274

Mullainathan [2003]), the stacked design allows me to limit my sample period to three months before and after audit disclosure, better alleviating the effect of potentially confounding events in a longer window. The unit of analysis is at the exchange*trading pair*year-month level, such as BTC-USD listed on Gemini in January 2020, for example. I use the following model to test whether the disclosure of SOC 2 audits completion is associated with improved trading and liquidity:

$$Liquidity\ measure_{ijt} = \beta_0 + \beta_1 * SOC2_{jt} + \zeta_{ij} + \eta_t + \epsilon_{ijt} \qquad (3)$$

Where $Liquidity\ measure_{ijt}$ is either $Trading\ Volume_{ijt}$, or $Amihud\ Ratio_{ijt}$ of cryptocurrency pair i on exchange j at month t. $SOC2_{jt}$ is an indicator variable that equals one for all trading pairs on SOC 2 exchanges in the three months following audit disclosure and zero otherwise. I include exchange*cryptocurrency pair (e.g., BTC/USD pair on Coinbase, for which BTC is the base currency and USD is the quote currency) fixed effects ζ_{ij} to control for time-invariant characteristics of each cryptocurrency pair traded on an exchange. To account for time-varying shocks to the crypto market, I add year-month fixed effects η_t. In the most robust specification, I include both base currency*year-month (e.g., BTC*2020m1) fixed effects and quote currency*year-month (USD*2020m1) fixed effects to control for time-varying factors that could affect the trading of the base and quote currency. In all analyses, standard errors are two-way clustered at the exchange and base currency level to account for both time-series and cross-sectional correlations between cryptocurrency pairs on the same exchange (exchange level) and both time-series and cross-sectional correlations of the same cryptocurrency across different exchanges (base currency level).[22]

[22] The full sample includes 58 exchanges and 97 base currencies. Given that there are only four treated exchanges, I also perform robustness tests using the wild bootstrap method (Conley et al. [2018], Roodman et al. [2019]) and

Electronic copy available at: https://ssrn.com/abstract=4536274

5.3 Main results

Table 3 reports the regression results. Panel A presents the impact of SOC 2 audits on the trading volume of cryptocurrencies listed on SOC 2 exchanges. The adjusted R-squared ranges from 0.897 to 0.931, suggesting a good fit of the model. The coefficients on *SOC2* are significantly positive at the one percent level in all specifications. The economic magnitude of the findings is significant and meaningful as well. In column 3, the coefficient on *SOC2* suggests an average of 66 percent (exp(0.506)-1) increase in trading volume for cryptocurrency pairs listed on SOC 2 exchanges in the three months following audit disclosure, providing strong evidence that SOC 2 audits attract more customers to the platform. Given that transaction fees constitute a significant portion of exchange revenues, the large increase in trading volume substantially improves exchange revenue and cash flow, suggesting that SOC 2 audits provide huge benefits to audited exchanges. Taking Coinbase as an example, the increase in trading volume corresponds to an increase in monthly revenue of $18 million.[23]

<Insert Table 3 here>

Table 3 Panel B shows the results of the effect of SOC 2 audits on cryptocurrency pairs' price impact. Consistent with my prediction, the coefficients on *SOC2* are significantly negative at the one percent level in all models. In terms of the economic magnitude, the *Amihud Ratio* decreases by 42 percent (exp(-0.546)-1) for cryptocurrency pairs listed on SOC 2 exchanges in the three months after audit disclosure, suggesting a substantial decrease in price impact and improvement in the market quality after SOC 2 audits.

bootstrapped standard errors (Cameron et al. [2008], Gow et al. [2010]). Across all specifications, the results remain robust.

[23] The estimate is based on the calculation: Increase in monthly revenue = Coinbase average monthly trading volume in the three months before audit disclosure × 0.66 × the average fee in 2020. The average fee in 2020 is roughly 0.57 percent, which is the ratio of transaction revenue to trading volume from Coinbase 2021 10-K report.

Electronic copy available at: https://ssrn.com/abstract=4536274

Taken together, I find that the trading volume of cryptocurrencies listed on SOC 2 exchanges increases by more than 60 percent, and the price impact decreases by roughly 40 percent in the three months after audit disclosure.[24] The findings provide strong evidence that SOC 2 compliance successfully draws in customers to the platform. Thus, SOC 2 audits effectively send a positive message about exchange security and reduce information asymmetry between exchanges and customers.

5.4 Parallel trends assumption and dynamic effects of SOC 2 audits

A key premise of the difference-in-differences methodology is the parallel trends assumption. Specifically, it requires that absent SOC 2 audits, the change in trading and liquidity for cryptocurrency pairs on SOC 2 exchanges would not have been different from the change for pairs on non-SOC 2 exchanges. Even though one cannot directly test whether the trends in trading and liquidity would be the same for treatment and control sample in the absence of SOC 2 audits (i.e., counterfactuals), I provide diagnostic tests of the assumption by examining whether the treatment and control samples have similar trends in trading and liquidity before the disclosure of SOC 2 audits (Armstrong et al. [2022]). The underlying assumption is that the pre-trends likely provide information about the counterfactuals that we do not observe. If the pre-trends between treatment and control sample are not parallel, then the trends are likely to diverge in the absence of SOC 2 audits. To do so, I replace the indicator variable *SOC2* in model (3) with indicator variables for each month except the last month before audit disclosure, which serves as the regression baseline. The model is specified below:

[24] I also construct measures of bid-ask spreads using the OHLCV data but fail to find strong evidence that bid-ask spreads change significantly after audit disclosure. There are two possible reasons. First, bid-ask spreads are low for some cryptocurrencies, so the change of bid-ask spreads does not have enough power to be detected. Second, measures of bid-ask spreads calculated from the price data are not accurate and contain too much measure error.

Electronic copy available at: https://ssrn.com/abstract=4536274

$$Liquidity\ measure_{ijt} = \beta_0 + \beta_1 * SOC2\_Pre3_{jt} + \beta_2 * SOC2\_Pre2_{jt} + \beta_3 * SOC2\_Post1_{jt} + \beta_4 * SOC2\_Post2_{jt} + \beta_5 * SOC2\_Post3_{jt} + \zeta_{ij} + \eta_t + \epsilon_{ijt} \qquad (4)$$

The estimated coefficients represent the difference in trading and liquidity between the treatment and control sample at each month relative to the difference in the last month before audit disclosure. If the coefficients on *SOC2_Pre3* and *SOC2_Pre2* are not statistically different from zero, the pre-trends between treatment and control sample are parallel, likely suggesting that the parallel trend assumption holds. I report the results in Table 4. The outcome variable is *Trading Volume* in column (1) and *Amihud Ratio* in column (2). In both columns, the coefficients on *SOC2_Pre3* and *SOC2_Pre2* are statistically insignificant. The results suggest that the treatment and control samples have similar trends of trading and liquidity in the three months before audit disclosure, providing support for the identification strategy.

<Insert Table 4 here>

Moreover, the coefficients on *SOC2_Post1*, *SOC2_Post2*, and *SOC2_Post3* show whether the effect of SOC 2 audits varies by time. In column (1), the coefficient on *SOC2_Post1* indicates an average of 70 percent increase in trading volume in the first month after disclosure. The magnitude tapers off in the next two months to around 50 percent. In column (2), *Amihud Ratio* decreases by 50 percent in the first month after audit disclosure, and the effect diminishes to roughly 40 percent in the following two months.[25] To better illustrate the patterns, I plot the estimated coefficients in Figure 2. The results suggest that trading on crypto exchanges seems to be attention-oriented (Liu and Tsyvinski [2021], Sockin and Xiong [2023]). When crypto exchanges initially disclose their SOC 2 audit completion, the disclosures attract customer

[25] In untabulated tests, I further explore the effect of SOC 2 audits in a longer window. The magnitudes of increases in *Trading volume* and decreases in *Amihud ratio* drop to around 30 percent to 40 percent in the fourth to sixth months.

Electronic copy available at: https://ssrn.com/abstract=4536274

attention and bring new customers to the platform. However, the effect of SOC 2 audits diminishes slightly as customer attention decreases over time.

<Insert Figure 2 here>

5.5 Results using the propensity score matched exchange sample

Since the choice to voluntarily obtain a SOC 2 audit could be driven by exchange characteristics (e.g., existing security practices, customer base), which might be correlated with exchange trading and liquidity, I conduct additional tests to further control for potential bias from exchange characteristics by using a propensity score matched exchange sample.

Specifically, I calculate the propensity to conduct a SOC 2 audit for each exchange in each year using model (5), which is discussed in detail in section 6.1. Then for each SOC 2 exchange, I find 20 non-SOC 2 exchanges with the closest propensity scores of having SOC 2 audits in the event year. I form the control sample of cryptocurrency pairs on non-SOC 2 exchanges by matching on both exchange propensity scores and cryptocurrency pair characteristics. Specifically, for each cryptocurrency pair listed on SOC 2 exchanges (treatment sample), I search within trading pairs of the same currency type listed on the 20 matched exchanges and select with replacement the pair with the closest trading volume before audit disclosure. In other words, the matching procedure is the same as the procedure in the main analysis except that now the control pair is selected within the propensity score matched exchanges.

I rerun the regression model specified in model (3) and report the results in Table 5. Panels A and B show the results of *Trading Volume* and *Amihud Ratio*, respectively. Consistent with previous results, the coefficients on *SOC2* are significantly positive at the one percent level for *Trading Volume*, and the coefficients on *SOC2* are all significantly negative at the one percent level for *Amihud Ratio*. The economic magnitudes seem larger than the results in Table 3, likely

Electronic copy available at: https://ssrn.com/abstract=4536274

the result of a different matching sample. Overall, the tests help to address the concern that omitted factors like crypto exchange characteristics might affect both the decision of SOC 2 audits and exchange trading. The findings provide further support for prior results that the trading volume increases significantly and the price impact decreases significantly in the three months following SOC 2 audit disclosure.

<Insert Table 5 here>

5.6 Cross-sectional analyses

Finally, I explore cross-sectional variations in exchange trading and liquidity across cryptocurrency characteristics, including trading volume and market capitalization. The motivation is that cryptocurrencies with certain characteristics might be more heavily affected by exchange security and thus SOC 2 audits. Because cryptocurrencies are widely accepted as investment assets (Baur et al. [2018]), cryptocurrencies with large trading volume and market capitalization may face higher risks of being stolen by cybercriminals. Hence, the increase in customer demand for trading those cryptocurrencies might be more pronounced after SOC 2 audit disclosure. On the contrary, SOC 2 audits provide assurance over the overall information system that likely benefits the security of all cryptocurrencies listed, so the increases in customer demand may not differ across cryptocurrencies. To test my conjectures, I construct two indicator variables, *HighVol* and *HighMktCap*, and designate cryptocurrency pairs as high trading volume/market cap if they are above the median.

<Insert Table 6 here>

The results are presented in Table 6. In Panel A, I include the interaction of *SOC2* and *HighVol*. The coefficients on *SOC2* demonstrate the association between SOC 2 audits and the outcome variable (*Trading Volume/Amihud Ratio*) for cryptocurrencies with low trading volume,

Electronic copy available at: https://ssrn.com/abstract=4536274

and the coefficients on *SOC2*HighVol* show the incremental effects of SOC 2 audits on the outcome variable for the high-volume cryptocurrencies compared with the low-volume ones. I find that the coefficients on *SOC2* are significantly positive for *Trading Volume* and significantly negative for *Amihud Ratio*, which means that SOC 2 audits significantly improve trading and liquidity for low-volume cryptocurrencies. Moreover, the insignificant coefficients on *SOC2*HighVol* suggest a lack of significant differences between the high-and low-trading volume groups, meaning trading and liquidity also improve substantially for high-volume cryptocurrencies. In Panel B, I include the interaction of *SOC2* and *HighMktCap*. Similar to the results in Panel A, I do not find noticeable differences between low-and high-market cap cryptocurrencies, indicating that the economic impacts of SOC 2 audits are similar for both groups. Overall, the increased customer demand for trading on audited exchanges is not driven by cryptocurrencies with certain characteristics, suggesting that SOC 2 audits positively influence all cryptocurrency pairs listed on the audited exchange.

6. Channels through which SOC 2 Audits Provide Value

In this section, I explore how do SOC 2 audits bring value to customers. There are two possible channels. First, exchanges with high-quality security operations are more likely to initiate SOC 2 audits (the "signaling channel"). Therefore, a SOC 2 audit may serve as a credible signal of high-level security measures provided by independent third parties (Kausar et al. [2016], Bonetti and Ormazabal [2023]). Even though exchanges voluntarily disclose their security measures, unverified disclosures could be false.[26] Accordingly, SOC 2 audits allow exchanges to effectively signal and differentiate from competitors and thus positively influence customer perception of

[26] See the example of QuadrigaCX's false disclosures on page 10.

Electronic copy available at: https://ssrn.com/abstract=4536274

exchange security (Spence [1973], Jensen and Meckling [1976]). Second, the audit process *itself* may improve exchange security measures (the "real effects channel"). In other words, a SOC 2 audit could have real consequences on exchange security. One reason is that if control issues are identified, managers need to remediate the issues to meet the SOC 2 criteria (Feng et al. [2015], Kravet et al. [2018]). Along the audit process, management might also raise cybersecurity awareness and devote more resources to security measures. Empirically, I test the signaling channel by studying factors associated with exchanges' decision to conduct SOC 2 audits and test the real effects channel by examining the effect of SOC 2 audits on exchange security measures.

6.1 The Signaling Channel

To investigate the conjecture that exchanges with better security measures are more likely to obtain SOC 2 audits to convey information to customers, I examine the factors influencing exchanges' decisions to engage in SOC 2 audits. Empirically, I construct several measures of crypto exchange characteristics that likely predict SOC 2 audit engagements, including exchange age, security measures, customer base, and trading volume. Below, I discuss the data sources and variable construction.

Security measures: I obtain data on crypto exchange security measures from CryptoCompare. CryptoCompare evaluates crypto exchange security operations over multiple metrics and assigns scores for each metric, with more important metrics receiving higher weights. The team manually collects and updates the data twice a year starting from 2019 Q3 for all exchanges covered by CryptoCompare.

I construct *Security measures* by aggregating scores from the following metrics: SSL rating, the use of a cold wallet, the percentage of funds in cold wallets, geographical distribution of keys,

Electronic copy available at: https://ssrn.com/abstract=4536274

two-factor authentication (2FA), and custody provider.[27] *Security measures* is on a scale of 1 to 14, with higher values indicating better security measures. See the detailed methodology in Appendix F. Conceptually, *Security measures* captures the quality of exchange operations related to data and information system security. For example, a higher cold storage ratio means that the exchange puts a higher proportion of digital assets stored in offline cold wallets, so the assets are less likely to be stolen and thus considered more secure. Moreover, 2FA is a widely recognized security standard to protect customer account security, so the lack of 2FA may suggest that the exchange has bad security measures. I predict that exchanges with better security practices have a higher propensity to have SOC 2 audits.

US web traffic: Because the aim of SOC 2 audits is to boost customer trust and confidence, customer base is a critical factor to consider in deciding whether to get SOC 2 audits. Since SOC 2 audits fall under the AICPA framework, it is more highly recognized by customers in the United States. Thus, exchanges with more US customers are more likely to conduct SOC 2 audits.

Since crypto exchanges do not disclose the number of customers by geographical region, I use web traffic data to proxy for exchange customer base. I manually collect exchange web traffic data from Semrush. Specifically, I search for the percentage of web traffic originating in the US from 2019 to 2022 for each exchange*year.

Hacked before: Although hacking and data breaches are generally low-probability events in most industries, they happen quite often in the crypto market. On the one hand, being hacked may raise management awareness of cybersecurity and increase the chance of conducting SOC 2 audits.

[27] SSL rating shows the quality of websites' SSL (Secure Sockets Layer) protocol by using the grading system from Qualys SSL Labs. Geographical distribution of keys indicates whether an exchange implements geographical distribution of cryptocurrency private keys. 2FA represents whether an exchange offers 2 Factor Authentication for individual account security. Custody provider shows whether an exchange makes use of a custody provider to store their cryptocurrencies.

Electronic copy available at: https://ssrn.com/abstract=4536274

On the other hand, being hacked might indicate poor security measures, suggesting that the exchange may have a lower probability to conduct SOC 2 audits. For each exchange in my sample, I search for whether it has been hacked from 2019 to 2022. *Hacked before* is an indicator variable which equals one if exchange j has been hacked in the past as of year t-1.

Exchange age: More established exchanges have higher trading volume and brand awareness, so they are more likely to get SOC 2 audits because the benefits afforded in terms of revenues and cash flows are higher. I search for the years exchanges were founded and calculate the number of years since the exchange was established.

Exchange volume: I use exchange trading volume as a proxy for exchange size and predict that larger exchanges are more likely to conduct SOC 2 audits. For each exchange, I first aggregate the monthly trading volume of all cryptocurrency pairs listed. Next, I calculate the natural logarithm of the average monthly volume for each exchange*year.

Table 7 Panel A reports descriptive statistics of the exchange sample. The sample includes 321 exchange*year observations of 145 exchanges from 2020 to 2022 (an average of 2.21 years per exchange). *Security measures* range from 3 to 13.94, indicating a wide variation in the quality of security operations. The exchanges that have received the highest score include Coinbase, ItBit, and Binance. Moreover, there is large variation in web traffic originating in the US, ranging from 0 percent to 92 percent. Since most crypto exchanges operate in multiple countries and regions (Makarov and Schoar [2020]), it is not surprising that only 24 exchanges have more than 50 percent of the web traffic originating in the US. Twelve hacks and data breaches occurred in my sample, which accounts for approximately four percent of all observations. Exchange age varies in the range of two to 11 years, with the oldest crypto exchanges, like Kraken and Bitstamp, founded in 2011. Approximately 45 percent of my sample exchanges were founded in 2017 and 2018,

Electronic copy available at: https://ssrn.com/abstract=4536274

following the 2017 crypto market boom. Finally, crypto exchanges differ significantly in terms of trading volume. The maximum average monthly trading volume is $151 billion, while the minimum is only $20 thousand. Overall, crypto exchanges vary considerably in multiple dimensions, including security measures, customer base, age, and trading volume.

<Insert Table 7 here>

Table 7 Panel B compares characteristics between SOC 2 exchanges and non-SOC 2 exchanges. Most notably, SOC 2 exchanges have significantly higher *Security measures* than non-SOC 2 exchanges, suggesting that audited exchanges have much better security practices. The mean *Security measures* for SOC 2 exchanges is 12.06 out of 14, whereas the mean for non-SOC 2 exchanges is only 7.76. Further, audited exchanges have an average of 46 percent of web traffic originating in the US, which is significantly higher than that of non-audited exchanges (9 percent). Moreover, SOC 2 exchanges are hacked more often than non-SOC 2 exchanges. Lastly, on average SOC 2 exchanges are older and have higher trading volumes than non-SOC 2 exchanges, providing preliminary evidence that older and larger exchanges could benefit more from SOC 2 audits and thus have higher incentives to do so.

I use the logistic regression model to predict exchanges' decision to have SOC 2 audits. The sample includes all exchange*year observations from 2020 to 2022. The model is specified below:

$$Prob(SOC2)_{jt} = \gamma_0 + \gamma_1 * Security\ measures_{jt-1} + \gamma_2 * US\ web\ traffic_{jt-1} + \gamma_3 * Hacked\ before_{jt} + \gamma_4 * Exchange\ age_{jt-1} + \gamma_5 * Exchange\ volume_{jt-1} + \eta_t + \varepsilon_{jt} \qquad (5)$$

Where *SOC2* equals one for exchanges in the years of conducting SOC 2 audits, and 0 otherwise. η_t denotes year fixed effects.

I report the regression results in Table 8. Most importantly, the quality of exchange security measures is a strong predictor of the decision to conduct SOC 2 audits. In column (1), the coefficient on lagged *Security measures* is significantly positive at the one percent level,

Electronic copy available at: https://ssrn.com/abstract=4536274

confirming my conjecture that exchanges with better security measures have a higher propensity to get SOC 2 audits. The results are robust to including other exchange characteristics in column (2). The economic magnitude is meaningful as well. Moving from the average *Security measures* of non-SOC 2 exchanges (7.76) to the average *Security measures* of SOC 2 exchanges (12.06), the probability of getting SOC 2 audits increases by 7.52 percent. Moving to other exchange characteristics in column (2), I find that customer base is another key driver in engaging in SOC 2 audits. In addition, exchanges that have been hacked in the past are more likely to get audited, probably due to the heightened cybersecurity awareness resulting from hacking damage. Not surprisingly, exchanges that are founded earlier have a higher propensity to get SOC 2 audits. These exchanges tend to have better security operations, so the indirect cost of SOC 2 audits could be lower and the potential benefits afforded could be larger (Badertscher et al. [2023], Dedman et al. [2014], Kravet et al. [2018]).

<Insert Table 8 here>

Taken together, the results in Table 8 show that exchanges with better security measures are more likely to conduct SOC 2 audits, which are consistent with the signaling channel that exchanges with high-quality security measures are more likely to use SOC 2 audits to effectively signal their quality (Spence [1973], Jensen and Meckling [1976], Kausar et al. [2016]). This signal is crucial for customers of crypto exchanges, as trust issues are widespread in the crypto market. SOC 2 audits provide credible third-party verification (Bonetti and Ormazabal [2023]), reducing information asymmetry between customers and exchanges and boosting customer trust.

6.2 The Real Effects Channel

Another possible channel for the value creation is that the audit process *itself* might influence crypto exchange security measures. On the one hand, if auditors identify material internal control

Electronic copy available at: https://ssrn.com/abstract=4536274

gaps relevant to security, managers must remediate the identified gaps to achieve SOC 2 compliance. The remediation process likely improves exchange security (Feng et al. [2015], Kravet et al. [2018]). On the other hand, if crypto exchanges already have superior security measures before initiating SOC 2 audits, auditors may not find control deficiencies. Therefore, the security measures may not change following audit completion. Therefore, whether SOC 2 audits affect crypto exchange security measures remains an empirical question.

I employ a difference-in-differences research design that compares the change of SOC 2 exchange *Security measures* after initial audit completion (the first difference) with that of non-SOC 2 exchanges (the second difference). The sample includes all exchange*year observations from 2020 to 2022. The model is specified as below:

$$Security\ measures_{jt} = \alpha_0 + \alpha_1 * SOC2_{jt} + X_{jt-1} + \mu_j + \eta_t + \epsilon_{jt} \qquad (6)$$

where $Security\ measures_{jt}$ is a measure of the quality of exchange operations related to data and information system security. *SOC2* is an indicator variable which equals one for SOC 2 exchanges in the years of conducting SOC 2 audits. *SOC2 exchange* is an indicator variable for SOC 2 exchanges. I only include *SOC2 exchange* in the regression if exchange fixed effects μ_j are not controlled for. Time fixed effects η_t are included in all models to control for common shocks to the crypto market which affect all crypto exchanges at the same time. X_{jt-1} denotes a set of control variables which potentially affect exchange security and are associated with the decision to conduct SOC 2 audits, including lagged *Security measures*, *US web traffic*, *Hacked before*, *Exchange age*, and *Exchange volume*.

The regression results are reported in Table 9. Panel A reports the results when using biannual *Security measures* data to explore greater time-series variations. Since control variables are constructed at the exchange*year level, they are not controlled for in Panel A. Panel B reports

Electronic copy available at: https://ssrn.com/abstract=4536274

the results when using annual *Security measures* data and including exchange characteristics as control variables. The coefficients on *SOC2* capture the change of security measures for SOC 2 exchanges after initial audit completion, compared with that for non-SOC 2 exchanges. In panel A, I find that the coefficients on *SOC2* lack statistical significance. In panel B, the coefficient is significantly positive only when exchange characteristics, exchange fixed effects and time effects are controlled for, providing some weak evidence that SOC 2 audits might improve exchange security operations. The coefficients on *SOC2 exchange* capture the difference of security measures between SOC 2 exchanges and non-SOC 2 exchanges that is common to both pre-and post- periods. In column (1) of both panels, the coefficients on *SOC2 exchange* are significantly positive at the one percent level, which suggests that SOC 2 exchanges have better security measures than non-SOC 2 exchanges both before and after the audit. Economically, the coefficient in Panel B implies that being a SOC 2 exchange is associated with better security measures corresponding to a 1.75 within-group standard deviation of *Security measures* (Breuer and deHaan [2024]).[28] Overall, the results corroborate the findings in the previous section that SOC 2 exchanges have better security measures even before the audits.

<Insert Table 9 here>

In summary, I do not find strong evidence that SOC 2 audits per se substantially improve crypto exchange security measures. This supports the conjecture that exchanges choosing to conduct SOC 2 audits have superior security measures, so auditors may not find material control deficiencies that the exchange could remediate. In other words, SOC 2 audits are more like verification of existing high-quality security measures that help exchanges to effectively signal.

[28] As explained by Breuer and deHaan [2024], the interpretation of regression coefficients needs to be adjusted in the presence of fixed effects. The within-group standard deviation of annual *Security measures* is 2.863. So, the coefficient on *SOC2 exchange* in Panel B column (1) implies a 1.75 (5.006/2.863) within-group standard deviation of *Security measures*.

Electronic copy available at: https://ssrn.com/abstract=4536274

Also, because SOC 2 audits must be conducted on a regular basis, the periodic verification process ensures that quality remains high over time.

7. Conclusion

This paper studies the value of System and Organization Controls 2 (SOC 2) audits to customers in cryptocurrency trading. I use the setting of crypto exchanges and find that the trading volume of cryptocurrencies listed on SOC 2 exchanges increases by more than 60 percent and the price impact decreases by approximately 40 percent in the three months after audit disclosure, providing strong evidence that SOC 2 audits build customer trust in exchange security measures and attract more customers to trade on the platform. Because a large portion of exchange revenue comes from trading fees, the increased customer demand in trading provides substantial benefits to audited exchanges in terms of revenue and cash flow. I further explore the channels through which SOC 2 audits provide value to customers. My findings suggest that exchanges with superior security measures are more likely to conduct SOC 2 audits to send a positive signal to customers. In other words, obtaining a SOC 2 audit conveys information about the exchange's security measures, as exchanges with better security practices are more willing to incur this cost to signal their quality. Additionally, since audited exchanges must conduct the audit periodically, the ongoing assurance ensures that the quality of their security does not decline.

The findings are in line with the effective signaling theory (Spence [1973]). Because of the severe information asymmetry between crypto exchanges and customers, customers face the risk of choosing an exchange with low-quality security measures. Thus, the market suffers from a lemons problem, which could lead to a market breakdown if customers lose confidence and are reluctant to participate (Akerlof [1970]). One solution to address the problem is through effective

Electronic copy available at: https://ssrn.com/abstract=4536274

signaling. My study documents how crypto exchanges send a positive signal to customers through SOC 2 audits and the extent to which customers value such signaling behaviors. Given the substantial benefits of SOC 2 audits, a natural follow-up question is: why do not all exchanges engage in the audit? One explanation could be that the market is still not in a steady equilibrium yet. As the industry of crypto exchanges evolves and exchange security measures improve, more crypto exchanges will conduct SOC 2 audits when the quality reaches a high level and the benefits of SOC 2 audits exceed the costs, mostly the indirect cost of time and resources devoted.

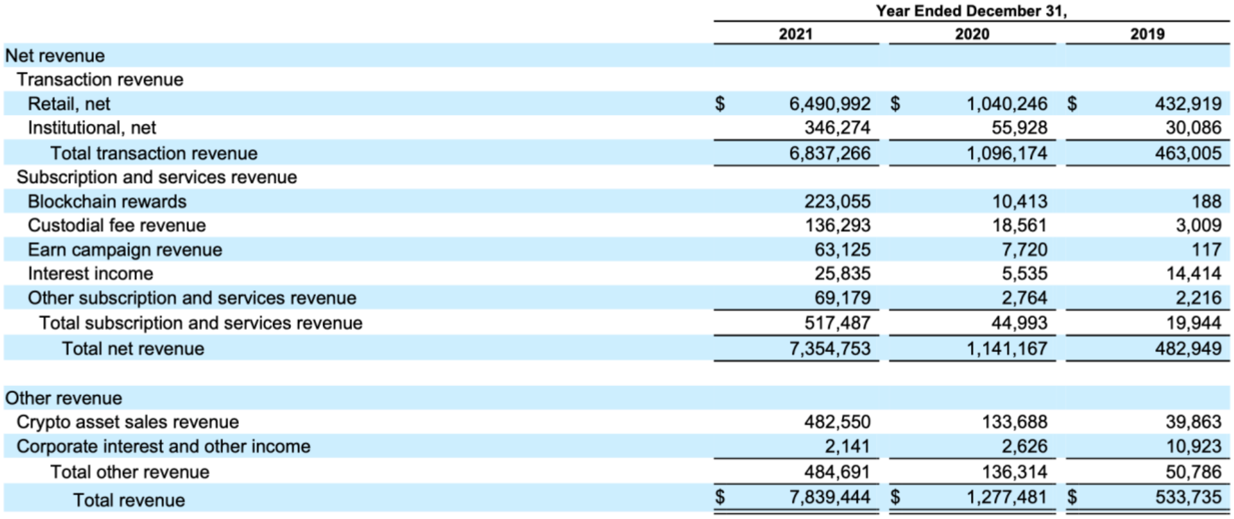
Electronic copy available at: https://ssrn.com/abstract=4536274

Appendix A: Coinbase Revenue Sources and Fees Schedules

Source: Coinbase 2021 10-K and websites

Table A.1 shows breakdowns of Coinbase revenues from 2019 to 2021, which indicates that transaction fees account for more than 90 percent of the total net revenue. Table A.2 presents Coinbase's trading volume from 2019 to 2021. Table A.3 and Table A.4 provide Coinbase Pro's fee schedules.

Table A.1 Coinbase revenue breakdown (in $thousands)

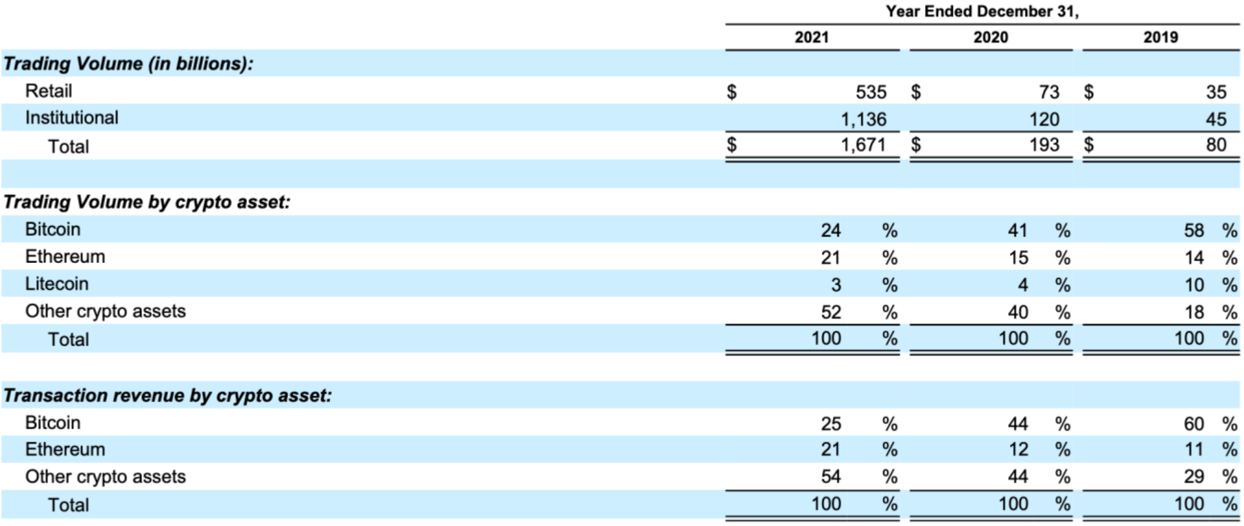


	Year Ended December 31,		
	2021	2020	2019
Net revenue			
Transaction revenue			
Retail, net	$ 6,490,992	$ 1,040,246	$ 432,919
Institutional, net	346,274	55,928	30,086
Total transaction revenue	6,837,266	1,096,174	463,005
Subscription and services revenue			
Blockchain rewards	223,055	10,413	188
Custodial fee revenue	136,293	18,561	3,009
Earn campaign revenue	63,125	7,720	117
Interest income	25,835	5,535	14,414
Other subscription and services revenue	69,179	2,764	2,216
Total subscription and services revenue	517,487	44,993	19,944
Total net revenue	7,354,753	1,141,167	482,949
Other revenue			
Crypto asset sales revenue	482,550	133,688	39,863
Corporate interest and other income	2,141	2,626	10,923
Total other revenue	484,691	136,314	50,786
Total revenue	$ 7,839,444	$ 1,277,481	$ 533,735

Electronic copy available at: https://ssrn.com/abstract=4536274

Appendix A (Continued)

Table A.2 Coinbase trading volume (in $billions)

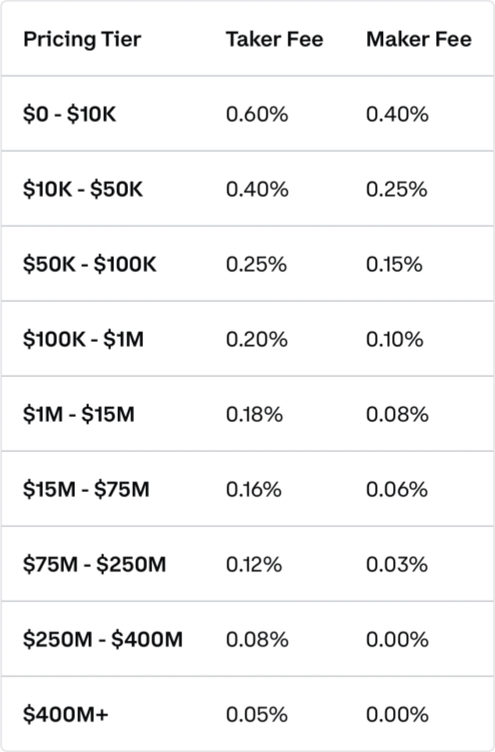


	Year Ended December 31,		
	2021	2020	2019
Trading Volume (in billions):			
Retail	$ 535	$ 73	$ 35
Institutional	1,136	120	45
Total	$ 1,671	$ 193	$ 80
Trading Volume by crypto asset:			
Bitcoin	24 %	41 %	58 %
Ethereum	21 %	15 %	14 %
Litecoin	3 %	4 %	10 %
Other crypto assets	52 %	40 %	18 %
Total	100 %	100 %	100 %
Transaction revenue by crypto asset:			
Bitcoin	25 %	44 %	60 %
Ethereum	21 %	12 %	11 %
Other crypto assets	54 %	44 %	29 %
Total	100 %	100 %	100 %

Electronic copy available at: https://ssrn.com/abstract=4536274

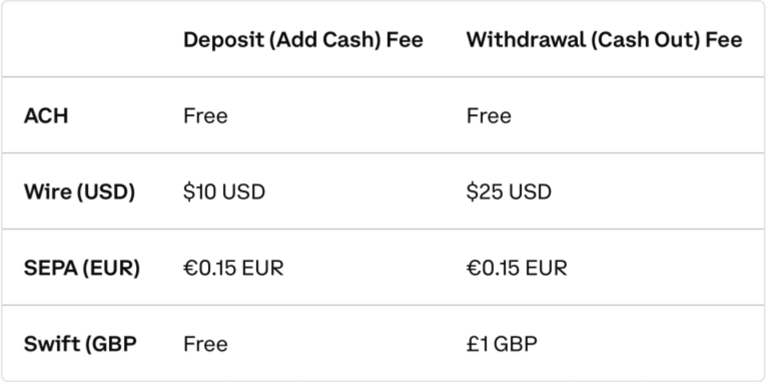
Appendix A (Continued)

Table A.3 Coinbase Pro trading fees schedule



Pricing Tier	Taker Fee	Maker Fee
$0 - $10K	0.60%	0.40%
$10K - $50K	0.40%	0.25%
$50K - $100K	0.25%	0.15%
$100K - $1M	0.20%	0.10%
$1M - $15M	0.18%	0.08%
$15M - $75M	0.16%	0.06%
$75M - $250M	0.12%	0.03%
$250M - $400M	0.08%	0.00%
$400M+	0.05%	0.00%

Table A.4 Coinbase Pro fiat deposit and withdrawal fees schedule



	Deposit (Add Cash) Fee	Withdrawal (Cash Out) Fee
ACH	Free	Free
Wire (USD)	$10 USD	$25 USD
SEPA (EUR)	€0.15 EUR	€0.15 EUR
Swift (GBP	Free	£1 GBP

Electronic copy available at: https://ssrn.com/abstract=4536274

Appendix B: AICPA Definitions of SOC 2 Trust Services Criteria

Source: AICPA [2020]

Security

Information and systems are protected against unauthorized access, unauthorized disclosure of information, and damage to systems that could compromise the availability, integrity, confidentiality, and privacy of information or systems and affect the entity's ability to achieve its objectives.

Security refers to the protection of

i. information during its collection or creation, use, processing, transmission, and storage and

ii. systems that use electronic information to process, transmit or transfer, and store information to enable the entity to meet its objectives. Controls over security prevent or detect the breakdown and circumvention of segregation of duties, system failure, incorrect processing, theft or other unauthorized removal of information or system resources, misuse of software, and improper access to or use of, alteration, destruction, or disclosure of information.

Availability

Information and systems are available for operation and use to meet the entity's objectives.

Availability refers to the accessibility of information used by the entity's systems as well as the products or services provided to its customers. The availability objective does not, in itself, set a minimum acceptable performance level; it does not address system functionality (the specific functions a system performs) or usability (the ability of users to apply system functions to the performance of specific tasks or problems). However, it does address whether systems include controls to support accessibility for operation, monitoring, and maintenance.

Processing integrity (over the provision of services or the production, manufacturing, or distribution of goods).

System processing is complete, valid, accurate, timely, and authorized to meet the entity's objectives.

Processing integrity refers to the completeness, validity, accuracy, timeliness, and authorization of system processing. Processing integrity addresses whether systems achieve the aim or purpose for which they exist and whether they perform their intended functions in an unimpaired manner, free from error, delay, omission, and unauthorized or inadvertent manipulation. Because of the number of systems used by an entity, processing integrity is usually only addressed at the system or functional level of an entity. In a SOC for Supply Chain examination, processing integrity refers to whether processing is complete, valid, accurate, timely, and authorized to produce, manufacture, or distribute goods that meet the products' specifications.

Electronic copy available at: https://ssrn.com/abstract=4536274

Appendix B (Continued)

Confidentiality

Information designated as confidential is protected to meet the entity's objectives.

Confidentiality addresses the entity's ability to protect information designated as confidential from its collection or creation through its final disposition and removal from the entity's control in accordance with management's objectives. Information is confidential if the custodian (for example, an entity that holds or stores information) of the information is required to limit its access, use, and retention and restrict its disclosure to defined parties (including those who may otherwise have authorized access within its system boundaries). Confidentiality requirements may be contained in laws or regulations or in contracts or agreements that contain commitments made to customers or others. The need for information to be confidential may arise for many different reasons. For example, the information may be proprietary, intended only for entity personnel.

Confidentiality is distinguished from privacy in that privacy applies only to personal information, whereas confidentiality applies to various types of sensitive information. In addition, the privacy objective addresses requirements regarding collection, use, retention, disclosure, and disposal of personal information. Confidential information may include personal information as well as other information, such as trade secrets and intellectual property.

Privacy

Personal information is collected, used, retained, disclosed, and disposed of to meet the entity's objectives. Although confidentiality applies to various types of sensitive information, privacy applies only to personal information.

The privacy criteria are organized as follows:

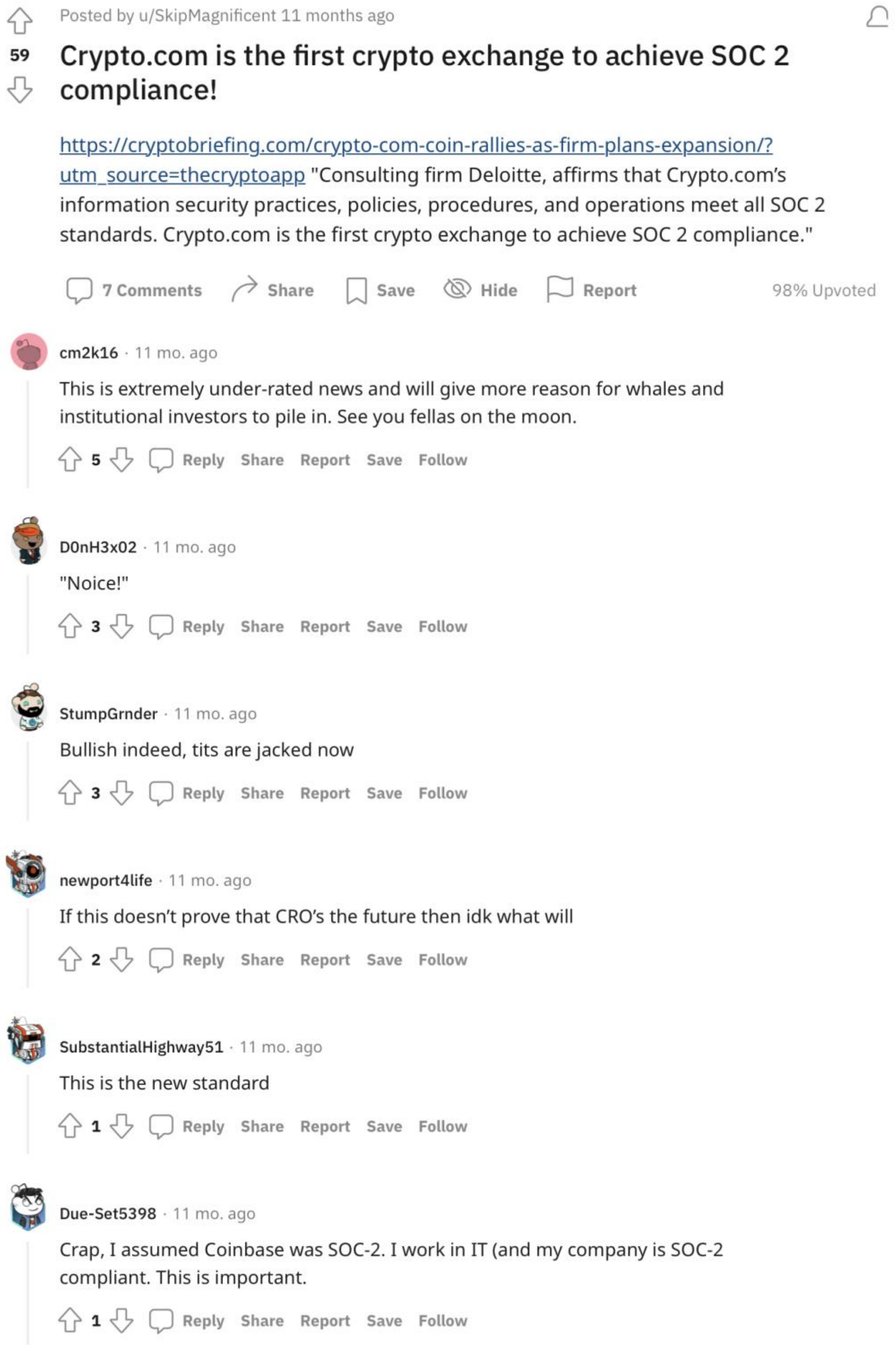
i. *Notice and communication of objectives.* The entity provides notice to data subjects about its objectives related to privacy.
ii. *Choice and consent.* The entity communicates choices available regarding the collection, use, retention, disclosure, and disposal of personal information to data subjects.
iii. *Collection.* The entity collects personal information to meet its objectives related to privacy.
iv. *Use, retention, and disposal.* The entity limits the use, retention, and disposal of personal information to meet its objectives related to privacy.
v. *Access.* The entity provides data subjects with access to their personal information for review and correction (including updates) to meet its objectives related to privacy.
vi. *Disclosure and notification.* The entity discloses personal information, with the consent of the data subjects, to meet its objectives related to privacy. Notification of breaches and incidents is provided to affected data subjects, regulators, and others to meet its objectives related to privacy.
vii. *Quality.* The entity collects and maintains accurate, up-to-date, complete, and relevant personal information to meet its objectives related to privacy.
viii. *Monitoring and enforcement.* The entity monitors compliance to meet its objectives related to privacy, including procedures to address privacy-related inquiries, complaints, and disputes.

Electronic copy available at: https://ssrn.com/abstract=4536274

Appendix C: Customer Reactions to Crypto.com SOC 2 Audit Disclosure

Source: Reddit.com, CoinMarketCap.com

Panel A: Reddit comments



Posted by u/SkipMagnificent 11 months ago

Crypto.com is the first crypto exchange to achieve SOC 2 compliance!

https://cryptobriefing.com/crypto-com-coin-rallies-as-firm-plans-expansion/?utm_source=thecryptoapp "Consulting firm Deloitte, affirms that Crypto.com's information security practices, policies, procedures, and operations meet all SOC 2 standards. Crypto.com is the first crypto exchange to achieve SOC 2 compliance."

cm2k16 · 11 mo. ago

This is extremely under-rated news and will give more reason for whales and institutional investors to pile in. See you fellas on the moon.

D0nH3x02 · 11 mo. ago

"Noice!"

StumpGrnder · 11 mo. ago

Bullish indeed, tits are jacked now

newport4life · 11 mo. ago

If this doesn't prove that CRO's the future then idk what will

SubstantialHighway51 · 11 mo. ago

This is the new standard

Due-Set5398 · 11 mo. ago

Crap, I assumed Coinbase was SOC-2. I work in IT (and my company is SOC-2 compliant. This is important.

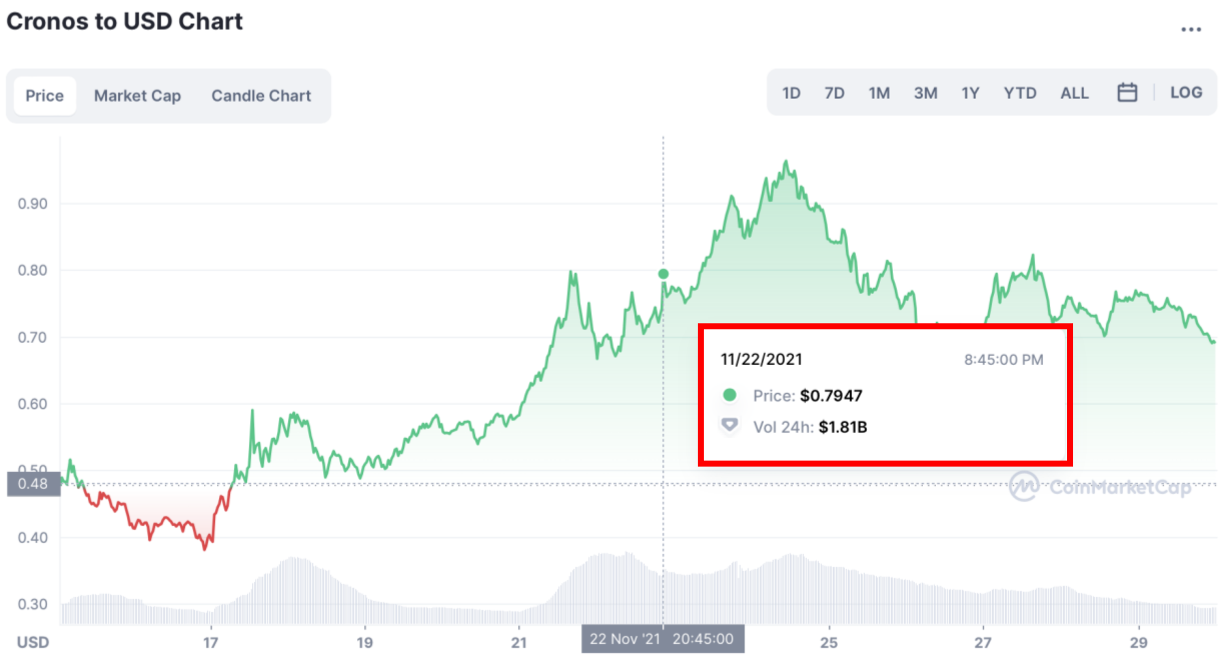
Electronic copy available at: https://ssrn.com/abstract=4536274

Appendix C (Continued)

Panel B: Price surge of Crypto.com exchange token CRO

Exchange tokens are digital assets issued by cryptocurrency exchanges. The primary purpose of exchange tokens is to incentive trading and liquidity provision. For example, exchanges could offer customers exchange tokens proportional to their trading volume and offer transaction fee discounts when paying with exchange tokens. Crypto.com's exchange token is Cronos (CRO). Like other cryptocurrencies, the price of CRO is influenced by current user adoption and future CRO network growth (Biais et al. [2023], Liu and Tsyvinski [2021]).

Panel B presents the price movements of CRO in the 7 days before and after Crypto.com SOC 2 audit disclosure on November 22, 2021. CRO price surged more than 20 percent from November 22 to November 23.

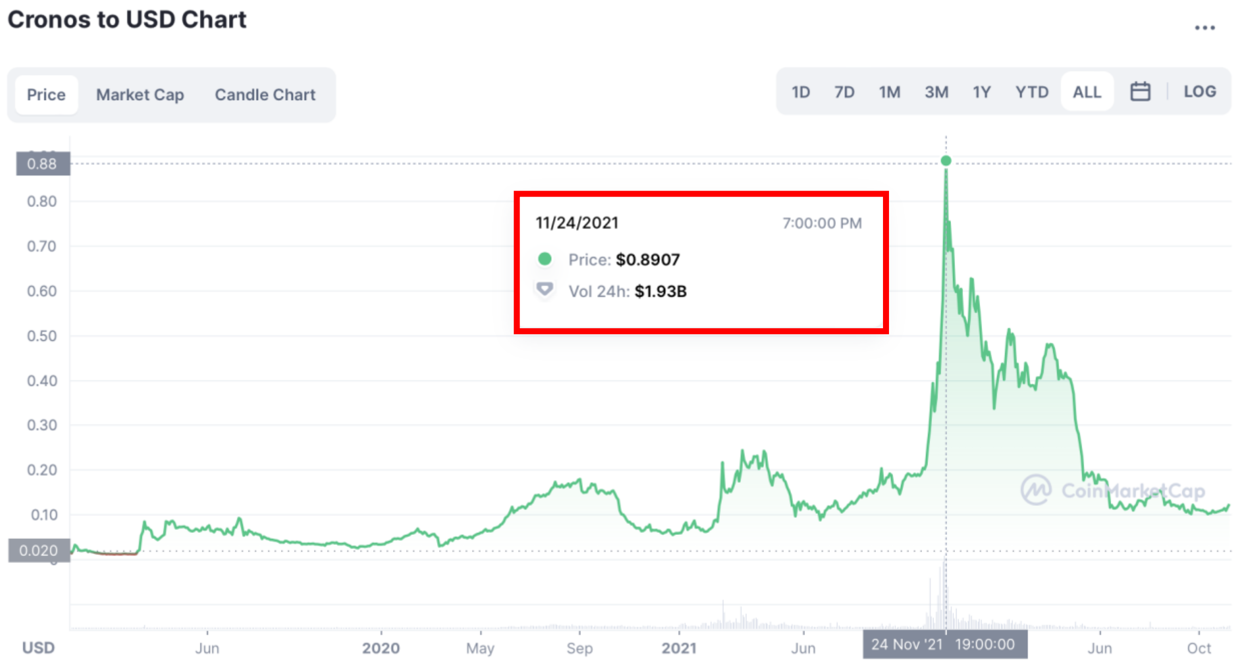


Electronic copy available at: https://ssrn.com/abstract=4536274

Appendix C (Continued)

Panel C: Historical price of CRO

Panel C shows that CRO reached the highest price in history on the 2nd day following audit disclosure.

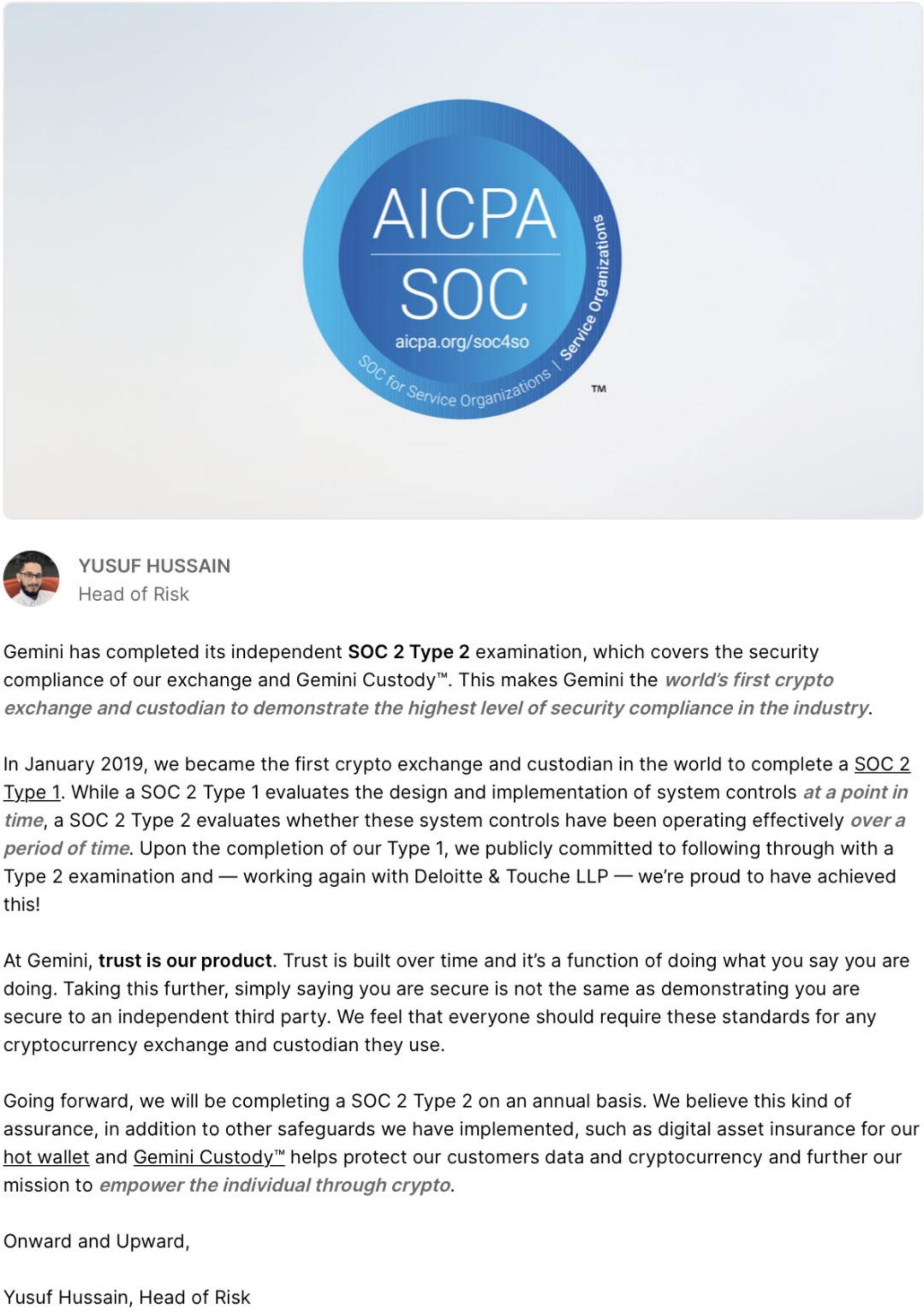


Electronic copy available at: https://ssrn.com/abstract=4536274

Appendix D: Gemini's SOC 2 Audit Disclosures

Source: Gemini websites, Twitter.com

Panel A: Disclosure on the company blog upon initial audit completion



YUSUF HUSSAIN
Head of Risk

Gemini has completed its independent **SOC 2 Type 2** examination, which covers the security compliance of our exchange and Gemini Custody™. This makes Gemini the ***world's first crypto exchange and custodian to demonstrate the highest level of security compliance in the industry***.

In January 2019, we became the first crypto exchange and custodian in the world to complete a SOC 2 Type 1. While a SOC 2 Type 1 evaluates the design and implementation of system controls ***at a point in time***, a SOC 2 Type 2 evaluates whether these system controls have been operating effectively ***over a period of time***. Upon the completion of our Type 1, we publicly committed to following through with a Type 2 examination and — working again with Deloitte & Touche LLP — we're proud to have achieved this!

At Gemini, **trust is our product**. Trust is built over time and it's a function of doing what you say you are doing. Taking this further, simply saying you are secure is not the same as demonstrating you are secure to an independent third party. We feel that everyone should require these standards for any cryptocurrency exchange and custodian they use.

Going forward, we will be completing a SOC 2 Type 2 on an annual basis. We believe this kind of assurance, in addition to other safeguards we have implemented, such as digital asset insurance for our hot wallet and Gemini Custody™ helps protect our customers data and cryptocurrency and further our mission to ***empower the individual through crypto***.

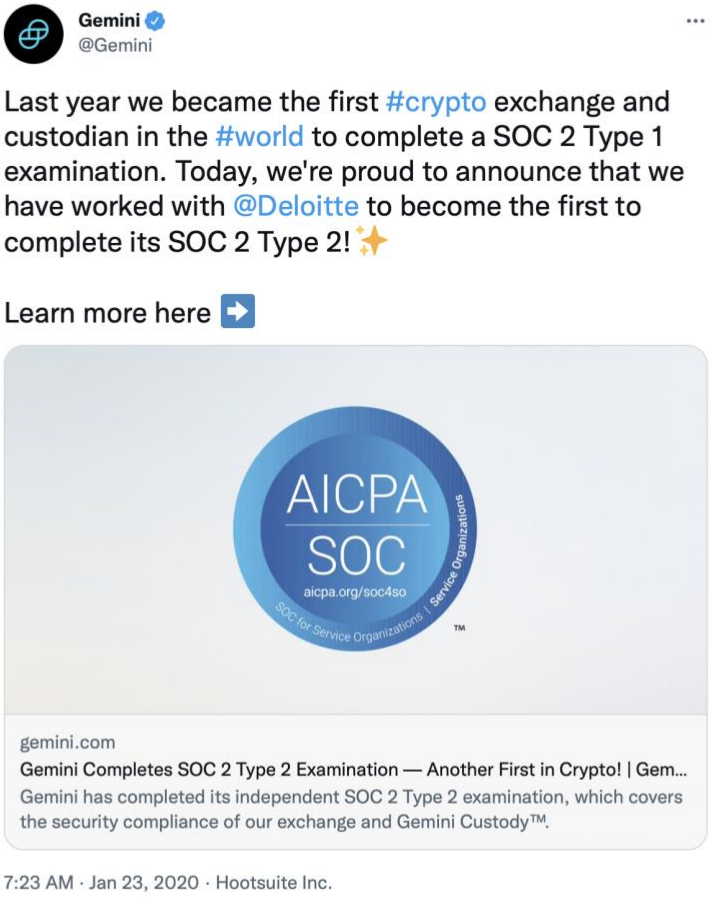
Onward and Upward,

Yusuf Hussain, Head of Risk

Electronic copy available at: https://ssrn.com/abstract=4536274

Appendix D (Continued)

Panel B: Disclosure on Twitter upon initial audit completion



Gemini
@Gemini

Last year we became the first #crypto exchange and custodian in the #world to complete a SOC 2 Type 1 examination. Today, we're proud to announce that we have worked with @Deloitte to become the first to complete its SOC 2 Type 2! ✨

Learn more here ➡️

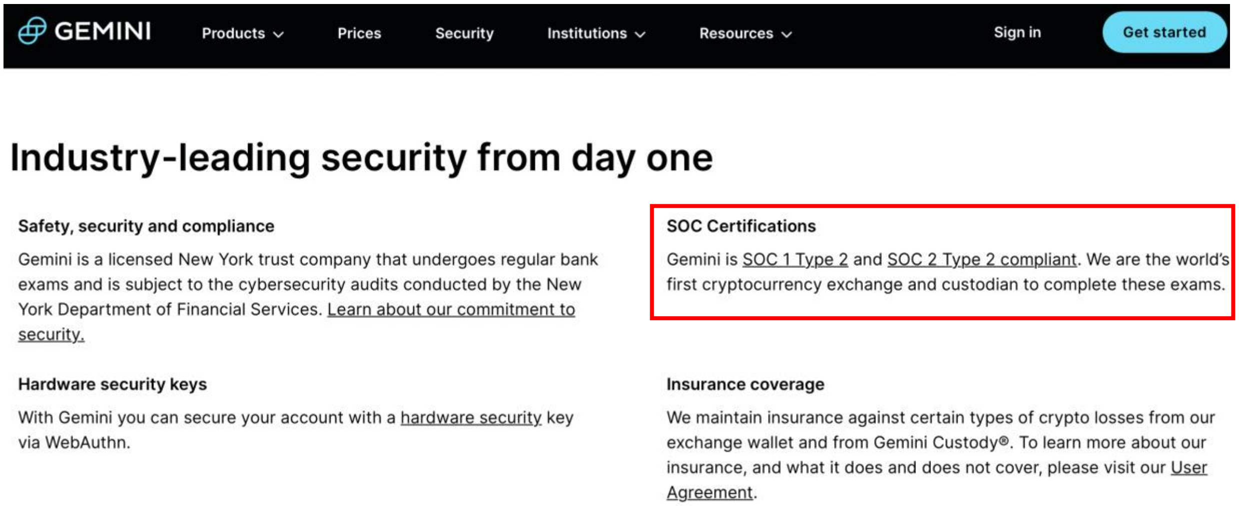
gemini.com
Gemini Completes SOC 2 Type 2 Examination — Another First in Crypto! | Gem...
Gemini has completed its independent SOC 2 Type 2 examination, which covers the security compliance of our exchange and Gemini Custody™.

7:23 AM · Jan 23, 2020 · Hootsuite Inc.

Electronic copy available at: https://ssrn.com/abstract=4536274

Appendix D (Continued)

Panel C: Disclosure on Gemini's home page



Industry-leading security from day one

Safety, security and compliance

Gemini is a licensed New York trust company that undergoes regular bank exams and is subject to the cybersecurity audits conducted by the New York Department of Financial Services. Learn about our commitment to security.

SOC Certifications

Gemini is SOC 1 Type 2 and SOC 2 Type 2 compliant. We are the world's first cryptocurrency exchange and custodian to complete these exams.

Hardware security keys

With Gemini you can secure your account with a hardware security key via WebAuthn.

Insurance coverage

We maintain insurance against certain types of crypto losses from our exchange wallet and from Gemini Custody®. To learn more about our insurance, and what it does and does not cover, please visit our User Agreement.

Electronic copy available at: https://ssrn.com/abstract=4536274

Appendix E: Variable Definitions

Variable	Definition
Dependent Variables	
Trading Volume	The natural logarithm of average daily trading volume in USD of cryptocurrency pair i listed on exchange j in month t. Source: CryptoCompare.
Amihud Ratio	The natural logarithm of the average of daily absolute returns divided by daily trading volume in USD for cryptocurrency pair i listed on exchange j in month t (Amihud [2002]). Source: CryptoCompare.
Security measures	A measure of the quality of exchange operations related to data and information system security. Detailed methodology is provided in Appendix F. Source: CryptoCompare.
Independent Variables	
SOC2	An indicator variable which equals one in the years following crypto exchanges' SOC 2 audit disclosure in the exchange-level analyses. An indicator variable that equals one for all trading pairs on SOC 2 exchanges in the three months following audit disclosure in the exchange*pair-level analyses.
SOC2 exchange	An indicator variable which equals one for SOC 2 exchanges.
Hacked before	An indicator variable which equals one if exchange j has been hacked or had data breaches as of year t during the sample period.
Exchange volume	The natural logarithm of exchange j's average monthly volume in year t. Source: CryptoCompare.
Exchange age	The number of years since exchange j was founded.
US web traffic	The percentage of web traffic originating in the United States. Source: Semrush.
Returns	The log return of cryptocurrency pair i's base currency in month t. Source: CryptoCompare.
HighVol	An indicator variable equals one if the cryptocurrency pair is in the top half of pairs with high trading volume in the pre-disclosure period.
HighMktCap	An indicator variable equals one if the cryptocurrency pair's base currency is in the top half of pairs with high market capitalization. The market capitalization data are for Oct 10, 2022 from CryptoCompare.
Return Volatility	The standard deviation of daily log returns for cryptocurrency pair i's base currency in month t. Source: CryptoCompare.

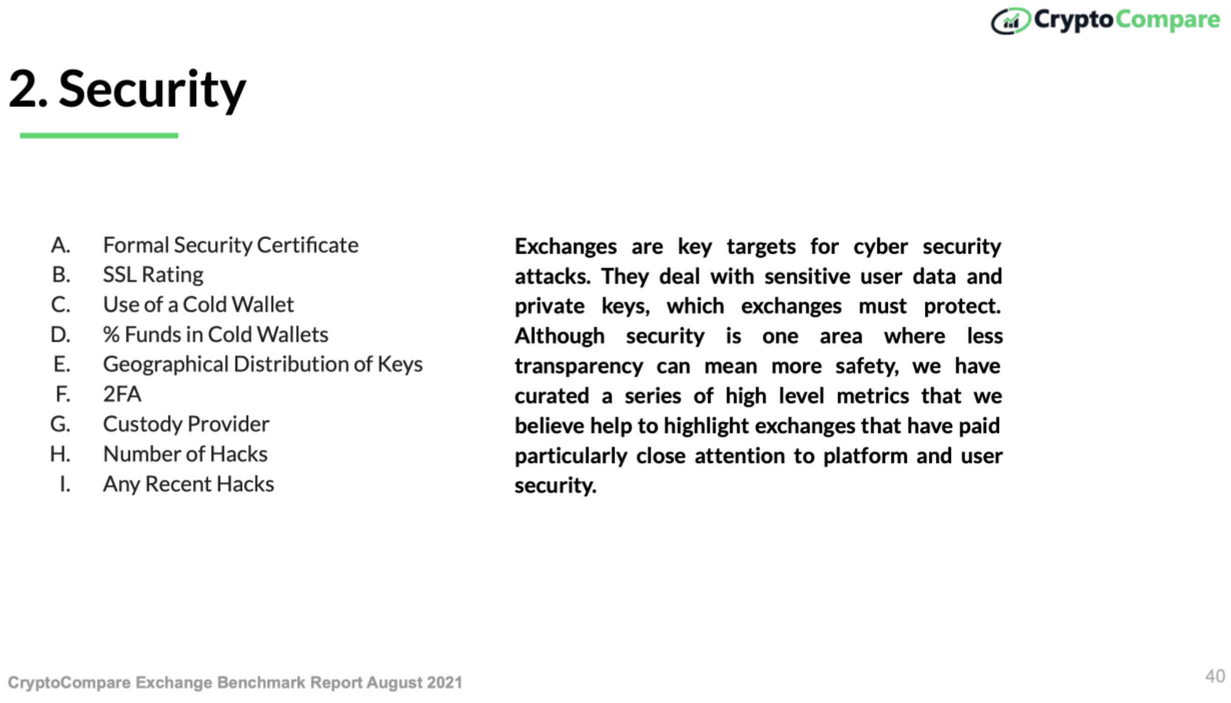
Electronic copy available at: https://ssrn.com/abstract=4536274

Appendix F: Detailed Methodology of Security Measures From CryptoCompare

Source: CryptoCompare Exchange Benchmark Report [2021]

CryptoCompare Exchange Benchmark was established in 2019 as a tool to bring clarity to the crypto exchange sector. The team collects both qualitative and quantitative information and evaluates crypto exchanges along several dimensions, including legal/regulation, security, KYC/Transaction risk, data provision, team/exchange, asset quality/diversity, market quality, and negative events penalty. Each dimension includes multiple metrics, which are converted into a series of points based on defined criteria. The team updates the scores twice a year. In the graphs below, I show the metrics of the security dimension and the grading criteria of each metric.

To construct *Security measures*, I aggregate the scores of multiple metrics, including SSL rating, the use of a cold wallet, the percentage of funds in cold wallets, geographical distribution of keys, two-factor authentication (2FA), and custody provider. Note that I do not include *Formal Security Certificate* in constructing *Security measures* because including the metric, of which SOC 2 is considered one, will introduce a mechanical positive relation between *SOC2* and *Security measures*, so it must be excluded. I also do not include the *Number of hacks* and *Any recent hacks* because 1). Conceptually *Security measures* is constructed to measure exchange security at the operational level, while hacking incidents speak more to the outcome, and 2). I separately control for the effect of hacking incidents using *Hacked before.* In untabulated tests, my results still hold when including the *Number of hacks* and *Any recent hacks* in constructing *Security measures.*



CryptoCompare

2. Security

A. Formal Security Certificate
B. SSL Rating
C. Use of a Cold Wallet
D. % Funds in Cold Wallets
E. Geographical Distribution of Keys
F. 2FA
G. Custody Provider
H. Number of Hacks
I. Any Recent Hacks

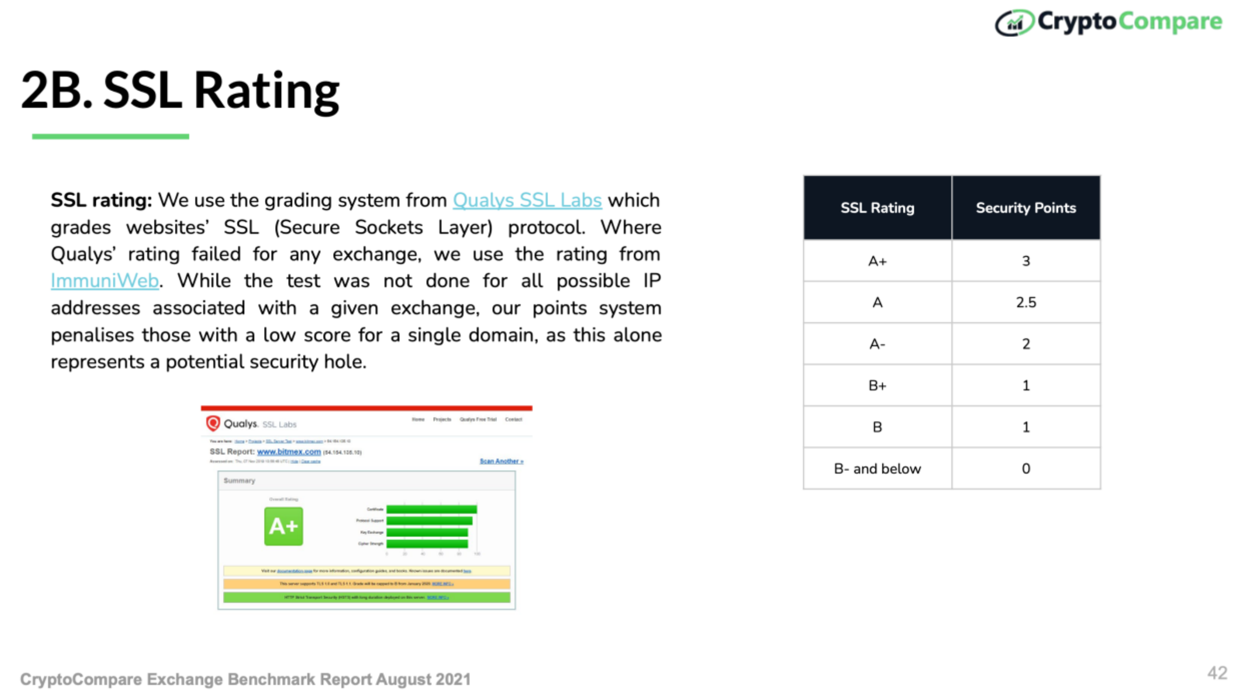
Exchanges are key targets for cyber security attacks. They deal with sensitive user data and private keys, which exchanges must protect. Although security is one area where less transparency can mean more safety, we have curated a series of high level metrics that we believe help to highlight exchanges that have paid particularly close attention to platform and user security.

CryptoCompare Exchange Benchmark Report August 2021

40

Electronic copy available at: https://ssrn.com/abstract=4536274

Appendix F (Continued)



CryptoCompare

2B. SSL Rating

SSL rating: We use the grading system from Qualys SSL Labs which grades websites' SSL (Secure Sockets Layer) protocol. Where Qualys' rating failed for any exchange, we use the rating from ImmuniWeb. While the test was not done for all possible IP addresses associated with a given exchange, our points system penalises those with a low score for a single domain, as this alone represents a potential security hole.

Qualys. SSL Labs

SSL Report: www.bitmex.com (54.154.126.10)

Scan Another »

Summary

Overall Rating

A+

Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.

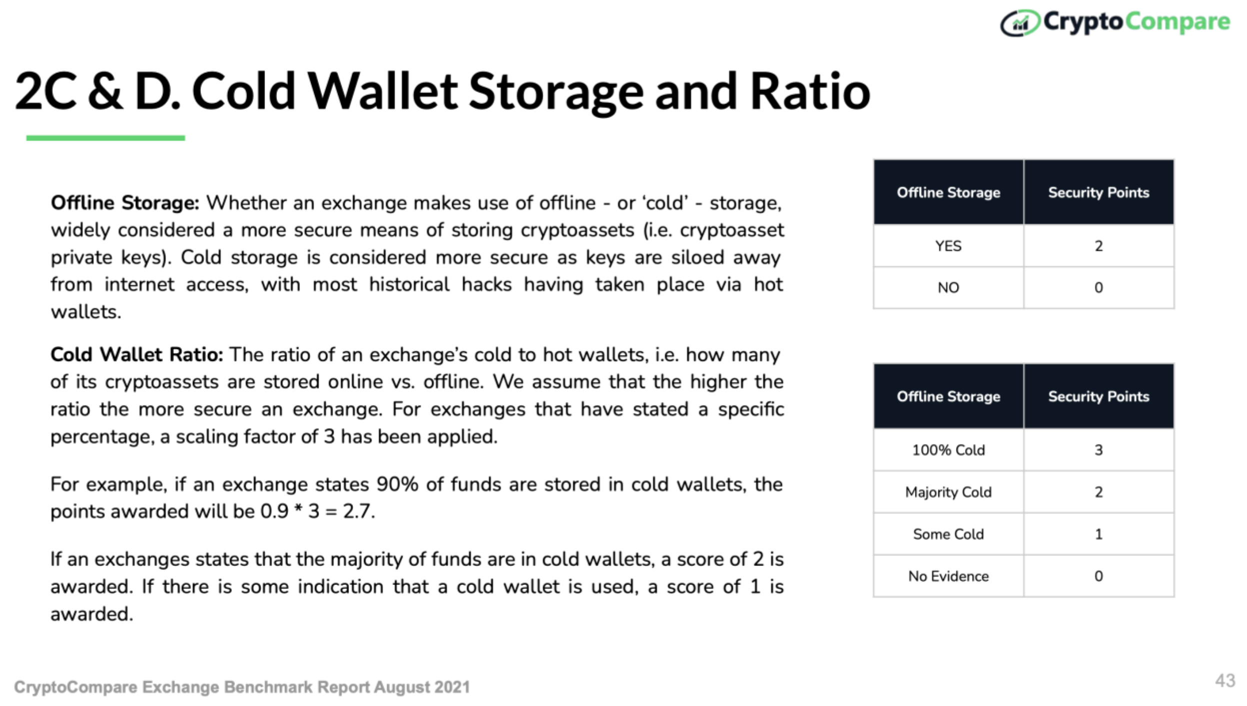
This server supports TLS 1.0 and TLS 1.1. Grade will be capped to B from January 2020. MORE INFO »

HTTP Strict Transport Security (HSTS) with long duration deployed on this server. MORE INFO »

SSL Rating	Security Points
A+	3
A	2.5
A-	2
B+	1
B	1
B- and below	0

CryptoCompare Exchange Benchmark Report August 2021

42



CryptoCompare

2C & D. Cold Wallet Storage and Ratio

Offline Storage: Whether an exchange makes use of offline - or 'cold' - storage, widely considered a more secure means of storing cryptoassets (i.e. cryptoasset private keys). Cold storage is considered more secure as keys are siloed away from internet access, with most historical hacks having taken place via hot wallets.

Cold Wallet Ratio: The ratio of an exchange's cold to hot wallets, i.e. how many of its cryptoassets are stored online vs. offline. We assume that the higher the ratio the more secure an exchange. For exchanges that have stated a specific percentage, a scaling factor of 3 has been applied.

For example, if an exchange states 90% of funds are stored in cold wallets, the points awarded will be 0.9 * 3 = 2.7.

If an exchanges states that the majority of funds are in cold wallets, a score of 2 is awarded. If there is some indication that a cold wallet is used, a score of 1 is awarded.

Offline Storage	Security Points
YES	2
NO	0

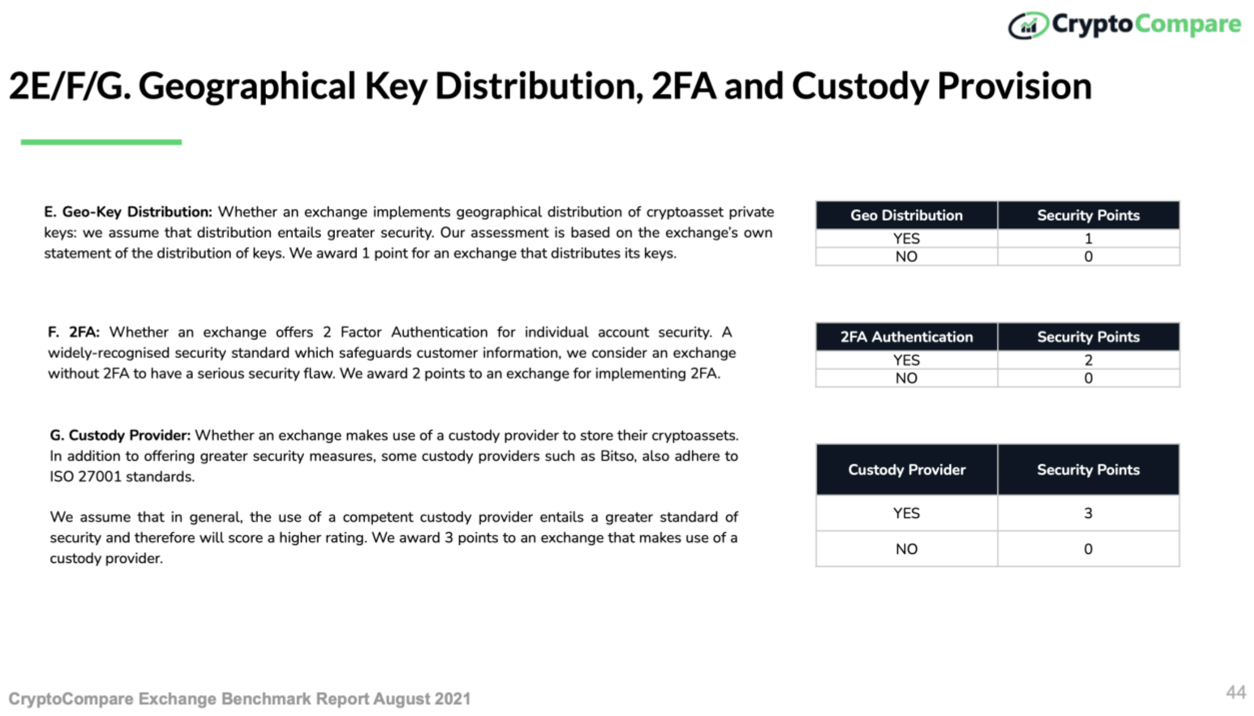
Offline Storage	Security Points
100% Cold	3
Majority Cold	2
Some Cold	1
No Evidence	0

CryptoCompare Exchange Benchmark Report August 2021

43

Electronic copy available at: https://ssrn.com/abstract=4536274

Appendix F (Continued)



CryptoCompare

2E/F/G. Geographical Key Distribution, 2FA and Custody Provision

E. Geo-Key Distribution: Whether an exchange implements geographical distribution of cryptoasset private keys: we assume that distribution entails greater security. Our assessment is based on the exchange's own statement of the distribution of keys. We award 1 point for an exchange that distributes its keys.

Geo Distribution	Security Points
YES	1
NO	0

F. 2FA: Whether an exchange offers 2 Factor Authentication for individual account security. A widely-recognised security standard which safeguards customer information, we consider an exchange without 2FA to have a serious security flaw. We award 2 points to an exchange for implementing 2FA.

2FA Authentication	Security Points
YES	2
NO	0

G. Custody Provider: Whether an exchange makes use of a custody provider to store their cryptoassets. In addition to offering greater security measures, some custody providers such as Bitso, also adhere to ISO 27001 standards.

We assume that in general, the use of a competent custody provider entails a greater standard of security and therefore will score a higher rating. We award 3 points to an exchange that makes use of a custody provider.

Custody Provider	Security Points
YES	3
NO	0

CryptoCompare Exchange Benchmark Report August 2021

44

Electronic copy available at: https://ssrn.com/abstract=4536274

References

AICPA. "Statement on Standards for Attestation Engagements (SSAE) No. 18." 2016. https://us.aicpa.org/content/dam/aicpa/research/standards/auditattest/downloadabledocuments/ssae-no-18.pdf (accessed 30 January 2023).

AICPA. "2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy." 2020. https://us.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/trust-services-criteria.pdf (accessed 30 January 2023).

AICPA. "SOC 2 - SOC for Service Organizations: Trust Services Criteria." 2022. https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/aicpasoc2report.html (accessed 30 January 2023).

Akerlof, G. A. "The Market for 'Lemons': Quality Uncertainty and the Market Mechanism." *The Quarterly Journal of Economics* 84 (1970): 488–500.

Alexander, C., and M. Dakos. "A Critical Investigation of Cryptocurrency Data and Analysis." *Quantitative Finance* 20 (2020): 173–88.

Allee, K. D., and T. L. Yohn. "The Demand for Financial Statements in an Unregulated Environment: An Examination of the Production and Use of Financial Statements by Privately Held Small Businesses." *The Accounting Review* 84 (2009): 1–25.

Amihud, Y. "Illiquidity and Stock Returns: Cross-Section and Time-Series Effects." *Journal of Financial Markets* 5 (2002): 31–56.

Amiram, D.; W. H. Beaver; W. R. Landsman; and J. Zhao. "The Effects of Credit Default Swap Trading on Information Asymmetry in Syndicated Loans." *Journal of Financial Economics* 126 (2017): 364–82.

Anderson, C. M.; V. W. Fang; J. Moon; and J. E. Shipman. "Accounting for Cryptocurrencies." 2022. Available at SSRN https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4294133

Armstrong, C.; J. D. Kepler; D. Samuels; and D. Taylor. "Causality Redux: The Evolution of Empirical Methods in Accounting Research and the Growth of Quasi-Experiments." *Journal of Accounting and Economics* 74 (2022): 101521.

Armstrong, C. S.; K. Balakrishnan; and D. Cohen. "Corporate Governance and the Information Environment: Evidence from State Antitakeover Laws." *Journal of Accounting and Economics* 53 (2012): 185–204.

Armstrong, C. S.; W. R. Guay; and J. P. Weber. "The Role of Information and Financial Reporting in Corporate Governance and Debt Contracting." *Journal of Accounting and Economics* 50 (2010): 179–234.

Augustin, P.; A. Rubtsov; and D. Shin. "The Impact of Derivatives on Spot Markets: Evidence from the Introduction of Bitcoin Futures Contracts." 2020. Available at SSRN https://doi.org/10.2139/ssrn.3648406.

Badertscher, B. A.; J. Kim; W. R. Kinney; and E. Owens. "Assurance Level Choice, CPA Fees, and Financial Reporting Benefits: Inferences from U.S. Private Firms." *Journal of Accounting and Economics*, September (2022), 101551.

Barton, J., and G. Waymire. "Investor Protection under Unregulated Financial Reporting." *Journal of Accounting and Economics* 38 (2004): 65–116.

Bauer, T. D.; C. Estep; and B. Malsch. "One Team or Two? Investigating Relationship Quality between Auditors and IT Specialists: Implications for Audit Team Identity and the Audit Process." *Contemporary Accounting Research 36* (2019): 2142–77.

Electronic copy available at: https://ssrn.com/abstract=4536274

Baur, D. G.; K. Hong; and A. D. Lee. “Bitcoin: Medium of Exchange or Speculative Assets?” *Journal of International Financial Markets, Institutions and Money* 54 (2018): 177–89.

Bertrand, M., and S. Mullainathan. “Enjoying the Quiet Life? Corporate Governance and Managerial Preferences.” *Journal of Political Economy* 111 (2003): 1043–75. https://doi.org/10.1086/376950.

Biais, B.; C. Bisiere; M. Bouvard; C. Casamatta; and A. J. Menkveld. “Equilibrium Bitcoin Pricing.” *The Journal of Finance 78* (2023): 967–1014.

Blankespoor, E. “The Impact of Information Processing Costs on Firm Disclosure Choice: Evidence from the XBRL Mandate.” J*ournal of Accounting Research* 57 (2019): 919–67.

Bonetti, P., and G. Ormazabal. “Boosting Foreign Investment: The Role of Certification of Corporate Governance.” *Journal of Accounting Research* 61 (2023): 95–140.

Borri, N., and K. Shakhnov. “Cryptomarket Discounts.” *Journal of International Money and Finance* 139 (2023): 102963.

Bourveau, T.; J. Brendel; and J. Schoenfeld. “Decentralized Finance (DeFi) Assurance: Early Evidence.” *Review of Accounting Studies*, July (2024).

Breuer, M., and E. Dehaan. “Using and Interpreting Fixed Effects Models.” *Journal of Accounting Research* 62 (2024): 1183–1226.

Brown, N. C.; H. Stice; and R. M. White. “Mobile Communication and Local Information Flow: Evidence from Distracted Driving Laws.” *Journal of Accounting Research* 53 (2015): 275–329.

Bushman, R. M., and A. J. Smith. “Financial Accounting Information and Corporate Governance.” *Journal of Accounting and Economics* 32 (2001): 237–333.

Cameron, A. C.; J. B. Gelbach; and D. L. Miller. “Bootstrap-Based Improvements for Inference with Clustered Errors.” *The Review of Economics and Statistics* 90 (2008): 414–27.

Chordia, T.; T C. Green; and B. Kottimukkalur. “Rent Seeking by Low-Latency Traders: Evidence from Trading on Macroeconomic Announcements.” *The Review of Financial Studies* 31 (2018): 4650–87.

Conley, T.; S. Gonçalves; and C. Hansen. “Inference with Dependent Data in Accounting and Finance Applications.” *Journal of Accounting Research* 56 (2018): 1139–1203.

Coinbase. “10-K Form.” 2021. https://investor.coinbase.com/financials/sec-filings/sec-filings-details/default.aspx?FilingId=15601874 (accessed 30 January 2023).

Coinbase. “Exchange Fees.” 2022. https://help.coinbase.com/en/exchange/trading-and-funding/exchange-fees (accessed 30 January 2023).

Costello, A. M. “Mitigating Incentive Conflicts in Inter-Firm Relationships: Evidence from Long-Term Supply Contracts.” *Journal of Accounting and Economics* 56 (2013): 19–39.

Cryptocompare Research. “Exchange Benchmark Report.” 2021. https://data.cryptocompare.com/reports/exchange-benchmark-august-2021 (accessed 30 January 2023).

Dedman, E.; A. Kausar; and C. Lennox. “The Demand for Audit in Private Firms: Recent Large-Sample Evidence from the UK.” *European Accounting Review* 23 (2014): 1–23.

DeFond, M., and J. Zhang. “A Review of Archival Auditing Research.” *Journal of Accounting and Economics* 58 (2014): 275–326.

Du, K., and S.-J. Wu. “Does External Assurance Enhance the Credibility of CSR Reports? Evidence from CSR-Related Misconduct Events in Taiwan.” *Auditing: A Journal of Practice & Theory* 38 (2019): 101–130.

Electronic copy available at: https://ssrn.com/abstract=4536274

Feng, M.; C. Li; S. E. McVay; and H. Skaife. "Does Ineffective Internal Control over Financial Reporting Affect a Firm's Operations? Evidence from Firms' Inventory Management." *The Accounting Review* 90 (2015): 529–557.

Gormley, T. A., and D. A. Matsa. "Growing Out of Trouble? Corporate Responses to Liability Risk." *The Review of Financial Studies* 24 (2011): 2781–2821.

Gow, I. D.; G. Ormazabal; and D. J. Taylor. "Correcting for Cross-Sectional and Time-Series Dependence in Accounting Research." *The Accounting Review* 85 (2010): 483–512.

Jensen, M. C., and W. H. Meckling. "Theory of the Firm: Managerial Behavior, Agency Costs and Ownership Structure." *Journal of Financial Economics* 3 (1976): 305–360.

Kausar, A.; N. Shroff; and H. White. "Real Effects of the Audit Choice." *Journal of Accounting and Economics* 62 (2016): 157–181.

Kravet, T. D.; S. E. McVay; and D. P. Weber. "Costs and Benefits of Internal Control Audits: Evidence from M&A Transactions." *Review of Accounting Studies* 23 (2018): 1389–1423.

Lennox, C. S., and J. A. Pittman. "Voluntary Audits versus Mandatory Audits." *The Accounting Review* 86 (2011): 1655–1678.

Lester, R. "Made in the U.S.A.? A Study of Firm Responses to Domestic Production Incentives." *Journal of Accounting Research* 57 (2019): 1059–1114.

Li, T.; D. Shin; and B. Wang. "Cryptocurrency Pump-and-Dump Schemes." 2021. Available at SSRN https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3267041

Lisowsky, P., and M. Minnis. "The Silent Majority: Private U.S. Firms and Financial Reporting Choices." *Journal of Accounting Research* 58 (2020): 547–588.

Lisowsky, P.; M. Minnis; and A. Sutherland. "Economic Growth and Financial Statement Verification." *Journal of Accounting Research* 55 (2017): 745–794.

Liu, Y., and A. Tsyvinski. "Risks and Returns of Cryptocurrency." *The Review of Financial Studies* 34 (2021): 2689–2727.

Makarov, I., and A. Schoar. "Trading and Arbitrage in Cryptocurrency Markets." *Journal of Financial Economics* 135 (2020): 293–319.

Michels, J. "Disclosure Versus Recognition: Inferences from Subsequent Events." *Journal of Accounting Research* 55 (2017): 3–34.

Minnis, M. "The Value of Financial Statement Verification in Debt Financing: Evidence from Private U.S. Firms." *Journal of Accounting Research* 49 (2011): 457–506.

Navarro, P., and S. G. Sutton. "Investors' Judgment and Decisions after a Cybersecurity Breach: Understanding the Value Relevance of Cybersecurity Risk Management Assurance." 2021. Available at SSRN https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3817763.

Roodman, D.; M. Ø. Nielsen; J. G. MacKinnon; and M. D. Webb. "Fast and Wild: Bootstrap Inference in Stata Using boottest." *The Stata Journal* 19 (2019): 4–60.

Ontario Securities Commission. "QuadrigaCX: A Review by Staff of the Ontario Securities Commission." 2020. https://www.osc.ca/quadrigacxreport/ (accessed 30 January 2023).

Schipper, K., and R. Thompson. "The Impact of Merger-Related Regulations on the Shareholders of Acquiring Firms." *Journal of Accounting Research* 21 (1983): 184–221.

Schoenfeld, J. "Cyber Risk and Voluntary Service Organization Control (SOC) Audits." *Review of Accounting Studies* 29 (2024): 580–620.

Sockin, M., and W. Xiong. "A Model of Cryptocurrencies." *Management Science* 69 (2023): 6684–6707.

Spence, M. "Job Market Signaling." *The Quarterly Journal of Economics* 87 (1973): 355–374.

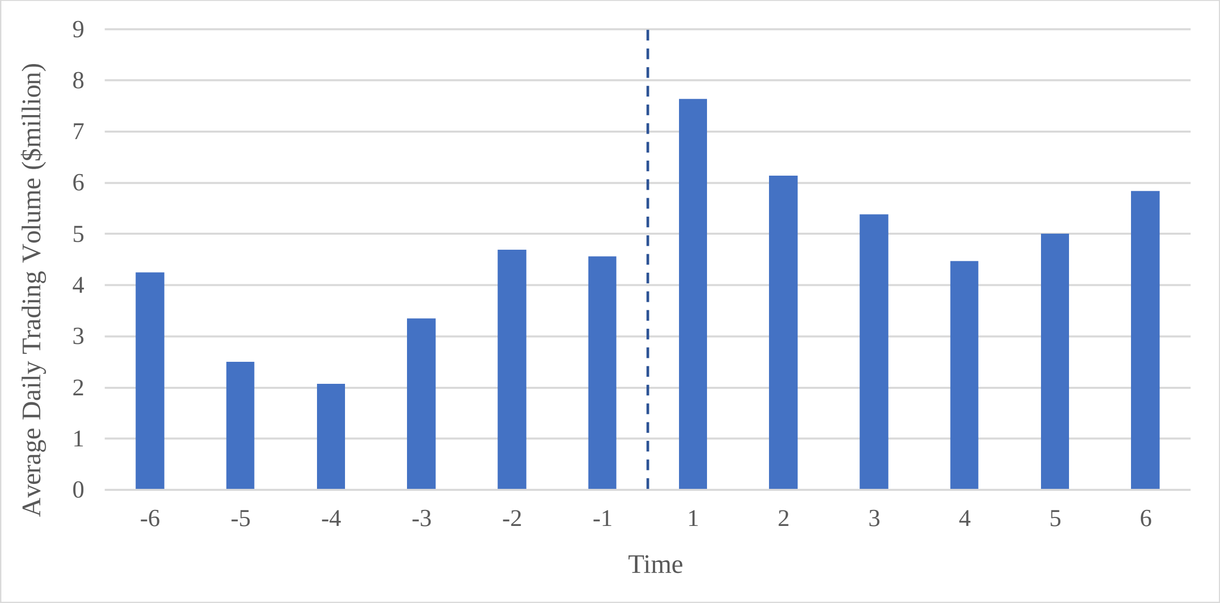
Electronic copy available at: https://ssrn.com/abstract=4536274

Tang, V. W., and T. Q. Zhang. "Regulation, Tax, and Cryptocurrency Pricing." 2021. Available at SSRN https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4195170

Watts, R. "Corporate Financial Statements, a Product of the Market and Political Process." *Australian Journal of Management* (April 1977): 53–75.

Electronic copy available at: https://ssrn.com/abstract=4536274

Figure 1: Average Daily Trading Volumes of Cryptocurrency Pairs on SOC 2 Exchanges in the Six Months Before and After Audit Disclosure

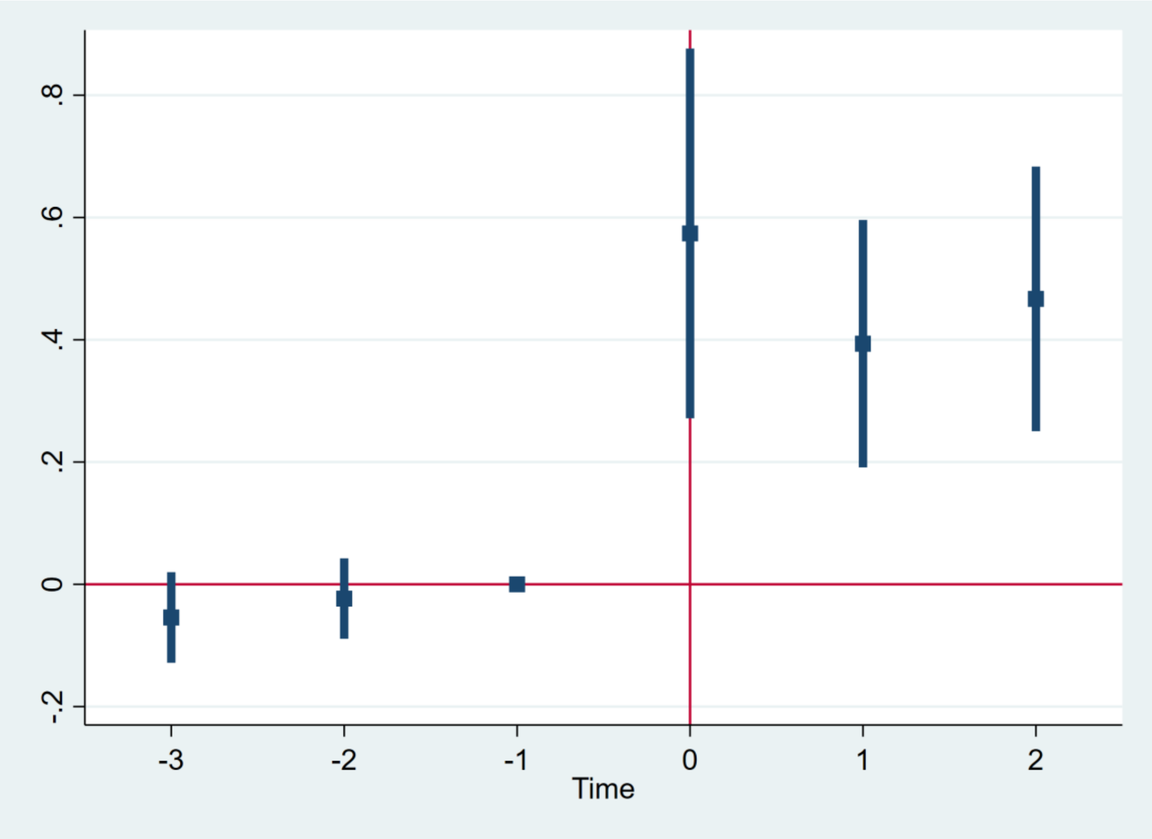


This figure plots the average daily trading volumes ($million) of cryptocurrency pairs on SOC 2 exchanges in the six months before and after audit disclosure. For each month, I calculate an average of all treatment pairs' average daily trading volumes in that month. The horizontal axis *time* represents the tth month before/after audit disclosure.

Electronic copy available at: https://ssrn.com/abstract=4536274

Figure 2: The Parallel Trend and the Dynamic Effect of SOC 2 Audits

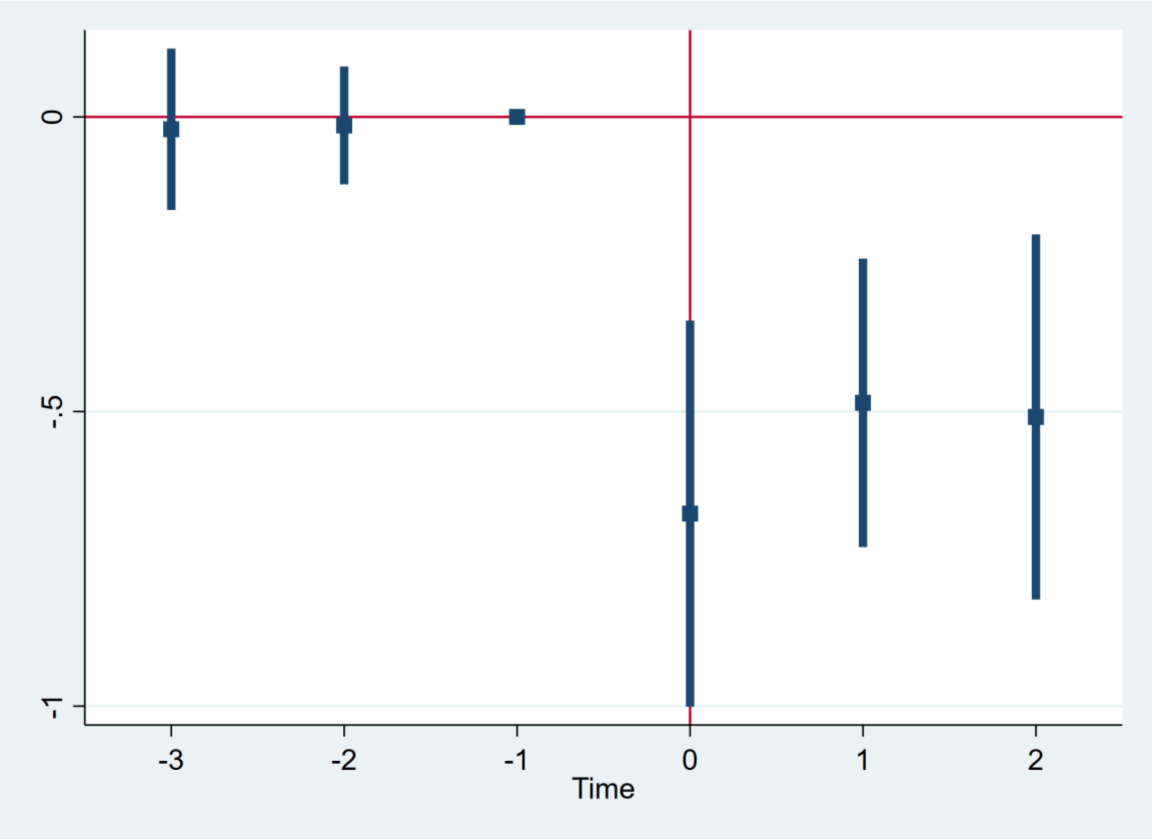
Panel A: The effect on trading volume



Electronic copy available at: https://ssrn.com/abstract=4536274

Figure 2 (Continued)

Panel B: The effect on Amihud Ratio



This figure displays the results of the parallel trend analysis and the dynamic effect of SOC 2 audits on exchange trading volume and liquidity. Panel A shows the effect on *Trading Volume*. Panel B shows the effect on *Amihud Ratio*. *Trading Volume* is the natural logarithm of the average daily trading volume in USD for trading pair i on exchange j in month t. *Amihud Ratio* is the natural logarithm of the average daily absolute return scaled by daily volume in USD for trading pair i on exchange j in month t. Estimated coefficients and the 95 percent confidence intervals for *SOC2_Pret* and *SOC2_Postt* in Table 4 are plotted. The estimated coefficients represent the difference in *Trading Volume* and *Amihud Ratio* between the treatment and control sample at each month relative to the difference in the last month before audit disclosure (Time=-1).

Electronic copy available at: https://ssrn.com/abstract=4536274

Table 1 Sample Selection

Panel A: SOC 2 exchanges

Exchange	Announcement date	Type 1 vs. Type 2	Scope	Trust Services Criteria	Auditor
Gemini	Jan 29, 2019	Type 1	Exchange and custodian	Security, availability, and confidentiality	Deloitte & Touche LLP
Gemini	Jan 23, 2020	Type 2	Exchange and custodian	Security, availability, and confidentiality	Deloitte & Touche LLP
Coinbase	Feb 12, 2020	Type 2	Custodian[29]	Not disclosed	Grant Thornton LLP
ItBit	Mar 02, 2021	Type 2	Exchange and custodian	Not disclosed	Ernst & Young LLP
Crypto.com	Nov 22, 2021	Not disclosed	Exchange	Security, availability, confidentiality, and privacy	Deloitte & Touche LLP

[29] Even though Coinbase custody (Coinbase Custody Trust Company, LLC) conducted SOC 2 audits rather than Coinbase exchange, the solution offered by Coinbase custody has been used by Coinbase's exchange since 2012. So, the custody's SOC 2 compliance directly affects the exchange's internal controls related to security.

Electronic copy available at: https://ssrn.com/abstract=4536274

Table 1 (Continued)

Panel B: Sample selection procedures of the treatment sample

	Gemini 2019	Gemini 2020	Coinbase	ItBit	Crypto.com	Total
All trading pairs listed on SOC 2 exchanges three months before and after announcements	15	15	65	5	277	377
Less:						
Trading pairs which are traded in less than 10 days each month	-	-	-	-	5	5
Trading pairs listed only in the pre or post period	5	1	9	-	57	72
Trading pairs with missing trading volume (USD) in the pre periods	4	2	3	-	64	73
Trading pairs listed only on the SOC 2 exchange	-	-	9	-	21	30
Trading pairs in the final sample	6	12	44	5	130	197

Panel A lists the sample of SOC 2 exchanges as of February 2022 and a summary of the information disclosed. Panel B shows the sample selection procedures of cryptocurrency pairs listed on SOC 2 exchanges (treatment sample) in the three months before and after audit disclosure.

Electronic copy available at: https://ssrn.com/abstract=4536274

Table 2 Descriptive Statistics

Panel A: Descriptive statistics of the full sample

Variable	N	Min	p5	p25	p50	Mean	p75	p95	Max	SD
# daily obs per month	2,345	11.00	28.00	30.00	31.00	29.91	31.00	31.00	31.00	2.62
Average daily volume ($K)	2,345	2.07	29.07	179.06	600.46	4,907.60	2,293.53	18,498.01	140,802.00	17,228.09
Trading Volume	2,345	7.64	10.28	12.10	13.31	13.39	14.65	16.73	18.76	2.02
Amihud Ratio	2,345	-22.73	-20.32	-17.89	-16.39	-16.45	-15.04	-12.91	-8.89	2.38
Return	2,345	-0.61	-0.46	-0.23	-0.05	-0.02	0.15	0.51	0.82	0.29
Return Volatility	2,345	0.00	0.02	0.04	0.05	0.05	0.06	0.10	0.14	0.03

Electronic copy available at: https://ssrn.com/abstract=4536274

Table 2 (Continued)

Panel B: Comparison between treatment and control sample in the three months before audit disclosure

	Treatment currency pairs		Control currency pairs		Difference
Variables	N	Mean	N	Mean	
# daily obs per month	591	30.33	591	30.33	-0.01
Trading Volume	591	13.28	591	13.18	0.10
Amihud Ratio	591	-16.38	591	-16.23	-0.15
Return	591	0.08	591	0.09	-0.01
Return Volatility	591	0.05	591	0.05	0.00

Electronic copy available at: https://ssrn.com/abstract=4536274

Table 2 (Continued)

Panel C: Comparison between treatment and control sample in the three months after audit disclosure

	Treatment currency pairs		Control currency pairs		Difference
Variables	N	Mean	N	Mean	
# daily obs per month	591	29.96	572	29.00	0.96***
Trading Volume	591	13.85	572	13.26	0.60***
Amihud Ratio	591	-16.95	572	-16.26	-0.70***
Return	591	-0.13	572	-0.13	0.00
Return Volatility	591	0.05	572	0.06	-0.00*

Panel A presents the descriptive statistics of the full sample of cryptocurrency pairs. Panel B shows the comparison between the treatment and control sample in the three months before audit disclosure. Panel C reports the comparison between the treatment and control sample in the three months after audit disclosure. *# daily obs per month* is the number of daily observations with trading data for trading pair i on exchange j in month t. *Average daily volume ($K)* is the average daily trading volume in $1,000 for pair i on exchange j in month t. *Trading Volume* is the natural logarithm of the average daily trading volume in USD for trading pair i on exchange j in month t. *Amihud Ratio* is the natural logarithm of the average daily absolute return scaled by daily volume in USD for trading pair i on exchange j in month t (Amihud [2002]). *Return* is the log return of pair i on exchange j in month t. *Return Volatility* is the standard deviation of daily log returns for pair i on exchange j in month t. All continuous variables are winsorized at one percent and 99 percent and defined in Appendix E. ***, **, and * indicate statistical significance at the one percent, 5 percent, and 10 percent levels (two-tailed).

Electronic copy available at: https://ssrn.com/abstract=4536274

Table 3 The Effect of SOC 2 Audits on Crypto Exchange Trading and Liquidity

Panel A: The effect on trading volume

Dep. Var. =	***Trading Volume***		
	(1)	(2)	(3)
SOC2	0.498*** (4.070)	0.506*** (4.237)	0.506*** (4.169)
Exchange*currency pair FE	Yes	Yes	Yes
Year-month FE	Yes	No	No
Base currency*year-month FE	No	Yes	Yes
Quote currency*year-month FE	No	No	Yes
Observations	2,345	2,345	2,345
Adjusted R-squared	0.897	0.929	0.931

Electronic copy available at: https://ssrn.com/abstract=4536274

Table 3 (Continued)

Panel B: The effect on Amihud illiquidity ratio

Dep. Var. =	*Amihud Ratio*		
	(1)	(2)	(3)
SOC2	-0.541*** (-3.788)	-0.546*** (-3.954)	-0.546*** (-3.874)
Exchange*currency pair FE	Yes	Yes	Yes
Year-month FE	Yes	No	No
Base currency*year-month FE	No	Yes	Yes
Quote currency*year-month FE	No	No	Yes
Observations	2,345	2,345	2,345
Adjusted R-squared	0.893	0.909	0.909

This table presents the results of the effect of SOC 2 audits on crypto exchanges' trading volume and liquidity in the three months after audit disclosure. The unit of analysis is at the exchange*cryptocurrency pair*year-month level. The dependent variables are *Trading Volume* and *Amihud Ratio* in Panels A and B, respectively. *Trading Volume* is the natural logarithm of the average daily trading volume in USD for trading pair i on exchange j in month t. *Amihud Ratio* is the natural logarithm of the average daily absolute return scaled by daily volume in USD for trading pair i on exchange j in month t (Amihud [2002]). *SOC2* is an indicator variable which equals one for all trading pairs on SOC 2 exchanges in the three months following audit disclosure and zero otherwise. All continuous variables are winsorized at one percent and 99 percent and defined in Appendix E. Standard errors are two-way clustered at the exchange and base currency level. ***, **, and * indicate statistical significance at the one percent, 5 percent, and 10 percent levels (two-tailed).

Electronic copy available at: https://ssrn.com/abstract=4536274

Table 4 The Parallel Trend Analysis and the Dynamic Effect of SOC 2 Audits

Dep. Var. =	*Trading Volume*	*Amihud Ratio*
	(1)	(2)
SOC2_Pre3	-0.054	-0.021
	(-1.502)	(-0.327)
SOC2_Pre2	-0.023	-0.014
	(-0.766)	(-0.284)
SOC2_Post1	0.574***	-0.673***
	(4.082)	(-4.307)
SOC2_Post2	0.394***	-0.485***
	(3.911)	(-3.761)
SOC2_Post3	0.467***	-0.509***
	(4.414)	(-3.308)
Exchange*currency pair FE	Yes	Yes
Base currency*year-month FE	Yes	Yes
Quote currency*year-month FE	Yes	Yes
Observations	2,345	2,345
Adjusted R-squared	0.931	0.909

This table presents the results of the parallel trend analysis and the dynamic effect of SOC 2 audits on crypto exchanges' trading volume and liquidity in the three months after audit disclosure. The unit of analysis is at the exchange*cryptocurrency pair*year-month level. *Trading volume* is the natural logarithm of the average daily trading volume in USD for trading pair i on exchange j in month t. *Amihud Ratio* is the natural logarithm of the average daily absolute return scaled by daily volume in USD for trading pair i on exchange j in month t. *SOC2_Pret* is an indicator variable which equals one for all trading pairs on SOC 2 exchanges in the t month before audit disclosure and zero otherwise. *SOC2_Postt* is an indicator variable which equals one for all trading pairs on SOC 2 exchanges in the t month after audit disclosure and zero otherwise. All continuous variables are winsorized at one percent and 99 percent and defined in Appendix E. Standard errors are two-way clustered at the exchange and base currency level. ***, **, and * indicate statistical significance at the one percent, 5 percent, and 10 percent levels (two-tailed).

Electronic copy available at: https://ssrn.com/abstract=4536274

Table 5 The Effect of SOC 2 Audits on Exchange Trading and Liquidity Using a Propensity Score Matched Exchange Sample

Panel A: The effect of SOC 2 audits on exchange trading volume

Dep. Var. =	***Trading Volume***		
	(1)	(2)	(3)
SOC2	0.560*** (3.733)	0.552*** (4.856)	0.554*** (4.891)
Exchange*currency pair FE	Yes	Yes	Yes
Year-month FE	Yes	No	No
Base currency*year-month FE	No	Yes	Yes
Quote currency*year-month FE	No	No	Yes
Observations	2,022	2,022	2,022
Adjusted R-squared	0.890	0.915	0.916

Electronic copy available at: https://ssrn.com/abstract=4536274

Table 5 (Continued)

Panel B: The effect of SOC 2 audits on exchange liquidity

Dep. Var. =	***Amihud Ratio***		
	(1)	(2)	(3)
SOC2	-0.754*** (-3.913)	-0.747*** (-4.947)	-0.746*** (-4.835)
Exchange*currency pair FE	Yes	Yes	Yes
Year-month FE	Yes	No	No
Base currency*year-month FE	No	Yes	Yes
Quote currency*year-month FE	No	No	Yes
Observations	2,022	2,022	2,022
Adjusted R-squared	0.874	0.885	0.882

This table reports the regression results of the effect of SOC 2 audits on exchange trading and liquidity using the propensity score matched exchange sample. The unit of analysis is at the exchange*cryptocurrency pair*year-month level. *Trading volume* is the natural logarithm of the average daily trading volume in USD for trading pair i on exchange j in month t. *Amihud Ratio* is the natural logarithm of the average daily absolute return scaled by daily volume in USD for trading pair i on exchange j in month t (Amihud [2002]). *SOC2* is an indicator variable which equals one for all trading pairs on SOC 2 exchanges in the three months after audit disclosure and zero otherwise. All continuous variables are winsorized at one percent and 99 percent and defined in Appendix E. Standard errors are two-way clustered at the exchange and base currency level. ***, **, and * indicate statistical significance at the one percent, 5 percent, and 10 percent levels (two-tailed).

Electronic copy available at: https://ssrn.com/abstract=4536274

Table 6 Cross-Sectional Tests

Panel A: Cross-sectional tests by trading volume

Dep. Var. =	***Trading Volume***	***Amihud Ratio***
	(1)	(2)
SOC2*HighVol	-0.008	-0.046
	(-0.056)	(-0.260)
SOC2	0.509***	-0.523***
	(3.638)	(-3.140)
Exchange*currency pair FE	Yes	Yes
Base currency*year-month FE	Yes	Yes
Quote currency*year-month FE	Yes	Yes
Observations	2,345	2,345
Adjusted R-squared	0.931	0.909

Electronic copy available at: https://ssrn.com/abstract=4536274

Table 6 (Continued)

Panel B: Cross-sectional tests by market capitalization

Dep. Var. =	***Trading Volume***	***Amihud Ratio***
	(1)	(2)
SOC2*HighMktCap	-0.068	0.033
	(-0.374)	(0.144)
SOC2	0.553***	-0.569***
	(3.664)	(-3.322)
Exchange*currency pair FE	Yes	Yes
Base currency*year-month FE	Yes	Yes
Quote currency*year-month FE	Yes	Yes
Observations	2,345	2,345
Adjusted R-squared	0.931	0.909

This table reports the results of cross-sectional tests. The dependent variables are *Trading Volume* and *Amihud Ratio*. The unit of analysis is at the exchange*cryptocurrency pair*year-month level. *SOC2* is an indicator variable which equals one for all trading pairs on SOC 2 exchanges in the three months following the announcements and zero otherwise. In Panel A, the variable of interest is the interaction term of the *HighVol* dummy (indicating the cryptocurrency pairs with high trading volume) and *SOC2*. In Panel B, the variable of interest is the interaction term of the *HighMktCap* (indicating the cryptocurrency pairs of which the base currency has high market capitalization) dummy and *SOC2*. All continuous variables are winsorized at one percent and 99 percent and defined in Appendix E. Standard errors are two-way clustered at the exchange and base currency level. ***, **, and * indicate statistical significance at the one percent, 5 percent, and 10 percent levels (two-tailed).

Electronic copy available at: https://ssrn.com/abstract=4536274

Table 7 Descriptive Statistics of the Exchange Sample

Panel A: Descriptive statistics of the exchange full sample

Variable	N	Min	p5	p25	p50	Mean	p75	p95	Max	SD
Security measures	321	3.00	3.00	6.00	7.94	7.92	9.85	13.40	13.94	2.92
US web traffic	321	0.00	0.00	0.01	0.04	0.10	0.10	0.47	0.92	0.17
Hacked before	321	0.00	0.00	0.00	0.00	0.12	0.00	1.00	1.00	0.32
Exchange age	321	2.00	2.00	3.00	5.00	5.53	8.00	9.00	11.00	2.41
Exchange volume ($M)	321	0.02	0.59	44.83	562.82	10,177.32	6,552.48	61,879.21	151,531.40	24,407.21

Electronic copy available at: https://ssrn.com/abstract=4536274

Table 7 (Continued)

Panel B: Comparison between SOC 2 exchanges and control exchanges

	SOC 2 exchanges		Control exchanges		Difference
Variables	N	Mean	N	Mean	
Security measures	12	12.06	309	7.76	4.30***
US web traffic	12	0.46	309	0.09	0.37***
Hacked before	12	0.33	309	0.11	0.22**
Exchange age	12	9.00	309	6.43	2.57***
Exchange volume	12	21.66	309	19.77	1.88*

Panel A presents the descriptive statistics for the full sample of exchanges, and Panel B shows the comparison between SOC 2 exchanges and non-SOC 2 exchanges. *Security measures* is a measure of the quality of exchange operations related to data and information system security. *US web traffic* is the percentage of web traffic originating in the United States. *Hacked before* is a dummy variable indicating whether the exchange has been hacked in the past. *Exchange age* is the number of years since exchange j was established. *Exchange volume* is the natural logarithm of exchange j's average monthly volume in millions of USD in year t (Panel A reports the values without log transformation). All continuous variables are winsorized at one percent and 99 percent and defined in Appendix E. ***, **, and * indicate statistical significance at the one percent, 5 percent, and 10 percent levels (two-tailed).

Electronic copy available at: https://ssrn.com/abstract=4536274

Table 8 Factors Associated with Crypto Exchanges' Decisions to Conduct SOC 2 Audits

Dep. Var. =	$\boldsymbol{SOC2_t}$	
	(1)	(2)
$Security\ measures_{t-1}$	0.987***	4.150***
	(3.629)	(4.591)
$US\ web\ traffic_{t-1}$		56.370***
		(4.972)
$Hacked\ before_t$		6.892***
		(4.808)
$Exchange\ age_{t-1}$		1.088***
		(3.321)
$Exchange\ volume_{t-1}$		-1.528**
		(-2.555)
Constant	-14.484***	-59.036***
	(-4.638)	(-3.589)
Year FE	Yes	Yes
Observations	321	321
Pseudo R-squared	0.408	0.918

This table reports the logistic regression results of regressing crypto exchanges' decision to have SOC 2 audits on lagged exchange characteristics. The unit of analysis is at the exchange*year level. The dependent variable is *SOC2*, which is an indicator variable which equals one for SOC 2 exchanges in the years following audit disclosure and zero otherwise. *Security measures* is a measure of the quality of exchange operations related to data and information system security. *US web traffic* is the percentage of web traffic originating in the United States. *Exchange age* is the number of years since exchange j was established. *Hacked before* is a dummy variable indicating whether the exchange has been hacked in the past. *Exchange volume* is the natural logarithm of exchange j's average monthly volume in millions of USD. All continuous variables are winsorized at one percent and 99 percent and defined in Appendix E. Standard errors are clustered at the exchange level. ***, **, and * indicate statistical significance at the one percent, 5 percent, and 10 percent levels (two-tailed).

Electronic copy available at: https://ssrn.com/abstract=4536274

Table 9 The Effect of SOC 2 Audits on Crypto Exchange Security

Panel A: Using biannual *Security measures* data

Dep. Var. =	***Security measures***	
	(1)	(2)
SOC2	-0.030	0.289
	(-0.088)	(1.490)
SOC2 exchange	6.015***	-
	(16.341)	
Constant	6.988***	7.092***
	(36.971)	(2,974.217)
Exchange FE	No	Yes
Time FE	Yes	Yes
Observations	1,059	1,059
Adjusted R-squared	0.073	0.847

Electronic copy available at: https://ssrn.com/abstract=4536274

Table 9 (Continued)

Panel B: Using annual *Security measures* data with control variables

Dep. Var. =	***Security measures***	
	(1)	(2)
SOC2	0.340	0.609**
	(0.815)	(2.104)
SOC2 exchange	5.006***	-
	(19.495)	
$Security\ measures_{t-1}$		0.169*
		(1.721)
$US\ web\ traffic_{t-1}$		-0.938
		(-1.294)
$Hacked\ before_{t}$		0.517
		(0.828)
$Exchange\ age_{t-1}$		0.610***
		(3.863)
$Exchange\ monthly\ volume_{t-1}$		0.004
		(0.058)
Constant	7.775***	3.172*
	(32.395)	(1.701)
Exchange FE	No	Yes
Time FE	Yes	Yes
Observations	321	321
Adjusted R-squared	0.122	0.877

This table presents the results of the impact of SOC 2 audits on crypto exchange security operations. Panel A reports the results of using biannual *Security measures* data, and Panel B reports the results of using annual data and controlling for exchange characteristics. The unit of analysis is at the exchange*year level. *Security measures* is a measure of the quality of exchange operations related to data and information system security. *SOC2* is an indicator variable which equals one for SOC 2 exchanges in the years following audit disclosure. *SOC2 exchange* is a dummy variable indicating SOC 2 exchanges. *US web traffic* is the percentage of web traffic originating in the United States. *Hacked before* is a dummy variable indicating whether the exchange has been hacked in the past. *Exchange age* is the number of years since exchange j was established. *Exchange volume* is the natural logarithm of exchange j's average monthly volume in millions of USD. All continuous variables are winsorized at one percent and 99 percent and defined in Appendix E. Standard errors are clustered at the exchange level. ***, **, and * indicate statistical significance at the one percent, 5 percent, and 10 percent levels (two-tailed).

Electronic copy available at: https://ssrn.com/abstract=4536274