Decentralized Finance (DeFi) Assurance: Audit Adoption and Capital Markets Effects[*]

Thomas Bourveau[†] **Janja Brendel**[‡] **Jordan Schoenfeld**[§]

May 2023

Abstract

Decentralized finance (DeFi) represents a large capital market where users conduct transactions primarily through digital smart contracts. These contracts are susceptible to cyber-attacks and coding errors that can result in significant financial losses, which has led to the emergence of smart contract audits to reduce information asymmetry and foster trust among DeFi service providers and users. Using a large hand-collected sample of these audit reports from DeFi service providers, we provide some of the first evidence showing that (1) these audits are pervasive, (2) the audit firm market is predominantly composed of new technical audit firms, (3) the scope of these audits can span a variety of contract features, and (4) the market reacts positively to the release of these audit reports, suggesting that these reports are value relevant. These findings highlight the demand for novel assurance services driven by blockchain technology.

Keywords: Auditing, Decentralized Finance, Smart Contract

JEL Classification: G23, G32, G34, M42, O33

[*] We thank Daniel Aobdia, Stefano Cascino, Will Cong, Emmanuel DeGeorge, Atif Ellahie, Aytekin Ertan, Brandon Gipper, John Kepler, Andy Leone, and Lorien Stice-Lawrence for helpful comments and discussions. We thank Yongkang Huang, Yijun Li, Jiayi Wang, and Sichen Xiao for their excellent research assistance. This project was supported by the Digital Future Initiative at Columbia Business School.

[†] Columbia University, Graduate School of Business - tb2797@columbia.edu
[‡] Chinese University of Hong Kong Business School - janjabrendel@cuhk.edu.hk
[§] University of Utah, Eccles School of Business - jordan.schoenfeld@eccles.utah.edu

1 Introduction

Decentralized Finance (DeFi) represents a growing set of financial services that attempt to replicate key functions of the conventional financial system in an open and decentralized way based on blockchain technology. This emerging form of capital markets has become economically meaningful, with the Federal Reserve estimating that the total value of digital contracts locked in DeFi applications exceeded $200 billion by early 2022, up from around $2 billion in 2020 (OECD 2022).

A key difference between DeFi and conventional finance is the degree of centralization involved when conducting transactions. In conventional finance, transactions generally adhere to a variety of regulations and oversight measures, with intermediaries such as banks playing a key role in executing financial agreements and serving as custodians of the financial system. DeFi, on the other hand, aims to create a more decentralized financial ecosystem, removing intermediaries and fostering transparency over financial transactions by employing public blockchain technology. Central to DeFi services are smart contracts, which are autonomous self-executing digital agreements with terms and conditions explicitly laid out in computer code. This code, which resides on a blockchain network, enables the contract to autonomously enforce its own terms, streamlining transactions between parties without the need for intermediaries such as banks and brokerages. The advent of such contracts presents novel challenges to the integrity of the capital markets.[1]

A major concern when using smart contracts is that non-technical users cannot judge the quality and completeness of the code behind these contracts (Makarov and Schoar 2022). Although the open-source nature of DeFi aims to prevent coding and logic errors, its effectiveness has proven to be limited, as there are numerous high-profile instances of coding bugs

[1] Aramonte et al. (2021) and Schar (2021) provide a detailed discussion of the DeFi ecosystem and its applications. Makarov and Schoar (2022) provide a detailed comparison of conventional financial intermediation and DeFi.

in smart contracts that have led to substantial thefts of crypto assets.[2] As a result, several leading financial organizations have issued white papers explicitly calling for independent third-party audits of the reliability of the code underlying smart contracts (e.g., Federal Reserve 2022; OECD 2022). In this study, we provide the first large-sample evidence of the emergence of these voluntary audits. Specifically, we address three main research questions: (1) who the audit firms are, (2) what services they provide, and (3) the value of the audit opinions to market participants.[3]

In their recent textbook summarizing the current state of DeFi, Harvey et al. (2021) note that the use of smart contracts exposes DeFi service providers to two key operational risks: (a) logic errors in the code, and (b) economic exploits, where attackers leverage a vulnerability in the code to steal from or inflict financial damage on ventures (e.g., withdrawing funds without permission). Additionally, unlike conventional financial products, smart contracts are designed not to have recourse to the legal system in the case of contract disputes, which underscores the importance of ensuring the upfront accuracy and completeness of smart contracts (Werbach and Cornell 2017). As a result, voluntary audits of smart contracts have emerged as a means to provide quality assurance for stakeholders involved in these contracts.

On a conceptual level, smart contract audits differ from financial statement audits in that while financial statement audits evaluate a firm's financial statements and integrated controls, smart contract audits evaluate the security and functionality of the underlying code and infrastructure of a specific contract. These audits are performed at the contract level and are designed to ensure that a contract behaves as intended and without exploitable bugs or loopholes. The choice to receive a smart contract audit is a voluntary choice made by DeFi ventures, similar to the voluntary financial statements audits received by some private

[2] For example, in March 2002, over $624 million was stolen in the largest ever DeFi hack to date (Source: rekt.new).

[3] Consistent with the language used by practitioners, we refer to the client engagements in our sample as *smart contract audits*. We acknowledge that existing audit research uses the terms *audit*, *assurance*, and *attestation* to represent a variety of other types of client engagements. DeFi security audits aim to identify and prevent vulnerabilities (e.g., security risks) of smart contracts to provide *assurance* to stakeholders and are commonly referred to as *smart contract audits* in the industry.

firms (Minnis 2011). To obtain data on smart contract audits, we use DeFi Yield, which is the largest public database on DeFi ventures, to retrieve 5,343 audit reports covering 4,309 unique DeFi ventures from 2017 to mid-2022.[4]

The first part of our paper investigates the audit firms serving the DeFi market. We find that our 5,343 audits are performed by 91 unique auditors. The auditors in our sample are composed exclusively of technical audit firms as opposed to the large financial audit firms, indicating that the large financial audit firms have not yet entered this space on a large scale.[5] One potential explanation is that large financial auditors are reluctant to enter a market where engagement fees are, on average, only between $250 and $15,000 (Source: cubix.co, DeFi Security Alliance). Another explanation is that financial audit firms lack the expertise to perform smart contract audits or consider this service too risky due to a lack of generally accepted criteria by which to evaluate smart contracts. In any event, recent studies suggest that if the market for smart contracts continues to grow, these contracts will enter the scope of financial audits, and auditing their underlying code will eventually become an important expertise for financial auditors (e.g., Bauer et al. 2022; Knechel 2021).

We observe that the three largest auditors performed 46% of the engagements in our sample. This market concentration in the emerging DeFi audit market is comparable to that observed in the market for audits of financial information in conventional capital markets.[6]. Since auditing in the DeFi market is unregulated and the audit is not tied to a specific time period (like the fiscal year for financial audits), DeFi ventures have the option to obtain multiple audits of their smart contracts. In our sample, 3,791 DeFi ventures obtained a single audit during our sample period while 519 purchased at least two audits (1,557 reports). Among DeFi ventures with multiple audits, we observe that over 70% chose a

[4] Note that, unlike financial statement audits for public firms, there is no central repository for smart contract audit reports.

[5] PwC appears to offer smart contract audits but is not in our sample (see `https://www.pwc.com/gx/en/services/audit-assurance/publications/halo-solution-for-cryptocurrency.html`).

[6] For evidence of concentration in financial audit engagements of public firms, see, for example, Bourveau et al. (2023) for evidence from the early 20^{th} century, and Lawrence et al. (2011) and Gerakos and Syverson (2015) for more recent time periods. For evidence on the financial audits of private firms, see Lisowsky et al. (2017) and Lisowsky and Minnis (2020).

different auditor between the first and second audit, likely reflecting the different domain expertise among emerging technical audit firms in the DeFi space.

Since DeFi audit firms typically evaluate and opine on the integrity of software code, their domain expertise differs from that of financial audit firms, although even financial audit firms increasingly employ staff with backgrounds in technologies such as artificial intelligence (Bauer et al. 2019; Law and Shen 2021; Fedyk et al. 2022). We attempt to gain an understanding of DeFi audit firm expertise by conducting two short case studies on Certik (USA) and Hacken (Ukraine), which are two of the largest DeFi audit firms. Both firms were founded in recent years and provide blockchain security services, including but not limited to smart contract audits. Certik's current CEO holds a computer science professorship and the firm has investors from both conventional capital markets (e.g., Sequoia) and new institutions from the crypto sector (e.g., Binance). Hacken's current CEO has over 10 years of work experience at Deloitte. Similar to CPA audit firms, both companies emphasize their independence from their clients. In contrast to the educational backgrounds of the workforce at financial audit firms, an analysis of LinkedIn profiles finds that Certik and Hacken employees primarily have degrees in engineering and computer science.

In the second part of our paper, we analyze a large sample of 5,343 unique smart contract audit reports with the goal of investigating the audit services and types of assurance provided by DeFi audit firms. In contrast to a financial statement audit report that spans only a few pages and provides limited detail beyond a coarse opinion on whether the client's financial statements and internal controls conform with local accounting standards, the audit reports in our sample provide a detailed look at the exact tests performed by the auditors and the outcome of those tests. The audit reports in our sample have a mean (median) length of 17 (13) pages. With respect to audit methods and tasks, the average audit in our sample combines manual and automatic verification testing and tests about 20 specific items in the code of the smart contract. For example, auditors commonly analyze whether the code properly locks the assets under consideration and safeguards against common exploits and security vulnerabilities. In reviewing these items, auditors typically separate any issues into major and minor issues. Audit clients typically have an opportunity to remedy any issues identified by the audit before the report is released, and these issues are then re-evaluated by the audit firm and, if fixed, are noted as such in the audit report. Overall, the granularity of smart contract audit reports much exceeds that of financial statement audit reports. However, just as financial audits do not guarantee against misstatements and fraud, smart contract audits do not guarantee against data breaches, thefts, or other problems.

Considering the differences between smart contract audits and previously studied financial audits in output, scope, clientele, and legal context, prior findings on the benefits of financial audits cannot be generalized to smart contract audits. Consequently, our final analysis investigates the benefits of smart contract audits by examining whether these audits are value relevant to market participants. Specifically, we examine abnormal returns at the DeFi venture level around the release of the audit report for a sub-sample of 483 reports covering 272 unique ventures for which the venture's token has available price data.[7] We find that, on average, the release of an audit report results in a positive and statistically significant market-adjusted return of about +10% in the two days after and including the release date.[8] Although ventures elect to release their audit reports, this finding nonetheless suggests that smart contract audits are value relevant, which is consistent with the long-standing proposition that audits serve as a mechanism to reduce information asymmetry and improve the functioning of capital markets (e.g., Watts and Zimmerman 1983).

Our results make several contributions to the literature. First, our study contributes to the emerging research on DeFi, which has only recently started to analyze the scope of the possible applications of smart contracts (John et al. 2023). Schwarcz and Bourret (2023) model how DeFi might impact capital markets by way of increased financial inclusion; Rivera

[7] Sample attrition resulting from available price data is common in this literature (e.g., Howell et al. 2020). See Section 6 for more detail.

[8] This finding is robust to several abnormal return measures adopted from recent research (e.g., Ramos et al. 2021). Note that the standard deviation of daily returns is higher in the crypto market relative to conventional equity markets (e.g., Kogan et al. 2023).

et al. (2023) examine how DeFi might change lending equilibria; and Cong and He (2019), Cong et al. (2021), and Cong et al. (2022) examine how DeFi, and the blockchain more broadly, might affect competition and the capital markets. Makarov and Schoar (2022) specifically note that the self-executing nature of smart contracts and the lack of ex-post legal mechanisms in DeFi markets increases the importance of writing these contracts as complete as possible up front, which is precisely the reason DeFi ventures are turning to verification services provided by smart contract auditors. To the best of our knowledge, prior accounting research has not examined this issue, but instead focuses on either accounting for crypto assets (e.g., Anderson et al. 2022) or the role of disclosure in the market for initial coin offerings (e.g., Fisch 2019; Howell et al. 2020; Hu et al. 2020; Bourveau et al. 2022).

Our study also contributes to the research on voluntary audit adoption and to the ongoing discussion around new types of verification services being provided in the audit market (Knechel 2021). Prior audit research typically focuses on the emergence of financial audits in public equity markets (Bourveau et al. 2023) or on the benefits of voluntary financial audits by private firms (e.g., Allee and Yohn 2009; Minnis 2011; Lennox and Pittman 2011; Kausar et al. 2016). We contribute specifically to the emerging literature on voluntary non-financial audits. For example, companies have started to adopt voluntary audits of their cyber security controls (Schoenfeld 2022) and of their non-financial "ESG" information (Gipper et al. 2022). Firms also adopt audits of their compliance with corporate environmental regulations (Duflo et al. 2013, 2018). The presence of such audits supports the theory that diverse stakeholders may not be satisfied by just financial statement audits and may demand supplemental audits of other parts of the firm (Kreps 1990).

Finally, our study contributes to the research on the value of audit opinions to the market. As Healy and Palepu (2001) note in their survey of the accounting literature, "there is a paucity of evidence on the value of audit opinions to investors." This still holds true in the literature today mainly because for public firms, it is notoriously difficult to separate the audit opinion from the 10-K when conducting market reaction tests. Researchers have instead tried to measure the market value of audit opinions based on various cross-sectional attributes of the auditor such as size and tenure (e.g., Mansi et al. 2004; Menon and Williams 2010; Willenborg 1999). However, to the best of our knowledge, there is limited research that analyzes the market reaction to an audit report that separates the audit opinion from concurrent filings made by the firm such as the 10-K.[9] The DeFi market, therefore, provides a novel setting to assess the value of audit opinions, and our evidence is consistent with audits providing value to market participants.

2 Background on DeFi and smart contracts

With DeFi and smart contracts being relatively new to the literature, we start by providing a brief primer on DeFi and the DeFi audit environment. DeFi refers to a set of financial services that are built on top of peer-to-peer blockchain networks such as Ethereum. These services are largely designed to replicate conventional financial services in an unregulated and decentralized manner. One of the largest applications of DeFi is credit services, for example the lending of crypto-assets against crypto collateral.[10] Nearly all DeFi transactions are structured using smart contracts, which are self-executing agreements whose terms and conditions are directly written into digital code. This code is hosted on a blockchain network and enables the contract to autonomously enforce its own terms, thereby facilitating transactions between parties without the need for intermediaries such as banks and brokerages. Smart contracts are highly transparent and deterministic in nature, ensuring that once the predetermined conditions are met, the encoded actions are automatically executed and funds are transferred appropriately.

Smart contracts underpin the functionality of most DeFi platforms that offer financial services such as lending, borrowing, trading, and asset management. By leveraging the

[9] Related research examines the stock market reaction to PCAOB sanctions against a firm's auditor (e.g., Dee et al. 2011).

[10] See https://www.ecb.europa.eu/pub/financial-stability/macroprudential-bulletin/focus/2022/html/ecb.mpbu202207_focus1.en.html.

streamlined nature of smart contracts, DeFi applications can potentially achieve reduced transaction costs, increased accessibility, and reduced counter-party risk. Smart contracts will continue to be the foundation of the emerging DeFi financial ecosystem, as they enable the creation of a variety of new decentralized financial instruments and institutions, such as decentralized exchanges, stablecoins, and liquidity pools. Smart contracts can also foster innovation within the DeFi landscape by providing an open-source programmable infrastructure that allows developers to easily create new financial products derived from existing ones.

Smart contracts can be used in many ways. One example is a lending agreement that is enforced by a smart contract. The smart contract would specify the terms of the loan, such as the amount borrowed, the interest rate, and the repayment schedule, and would automatically execute the transfer of funds based on the agreed-upon terms. Another example is a decentralized exchange (DEX), which allows users to trade cryptocurrencies without relying on a centralized exchange. In a DEX, users can connect their digital wallets to the blockchain network and trade directly with each other using smart contracts. The smart contracts manage the order book, execute trades, and handle the transfer of funds between buyers and sellers.

The use of smart contracts does not come without risks, a leading example of which is coding exploits. One well-known example of a smart contract hack resulting from a coding exploit is the 2016 Decentralized Autonomous Organization (DAO) attack on the Ethereum platform, which led to the loss of approximately $50 million worth of Ether at that time. The DAO was a smart contract designed to function as a decentralized venture capital fund, allowing users to pool their funds and collectively vote on investment proposals. The vulnerability that the attacker exploited was related to a design flaw in the smart contract known as a "re-entrancy attack." In a re-entrancy attack, a malicious contract exploits the targeted contract's functions by repeatedly calling them in a recursive manner before the original function has completed its execution. In the DAO's case, the attacker took advantage of a flaw in the contract's withdrawal function. When a user requested a withdrawal, the contract would first send the Ether to the user's address and then update the user's balance. The attacker exploited this sequence by creating a malicious contract that, when receiving Ether from the withdrawal function, would recursively call the withdrawal function again before the DAO contract could update the user's balance. This allowed the attacker to drain funds from the DAO multiple times.

3 Data

We collect data on smart contract audits from DEFIYIELD in 2022[11], which maintains one of the largest historical archives of which DeFi ventures receive these audits. Once ventures receive the audit reports, they can release them via their website or outlets such as a GitHub repository. Our final sample spans from 2017 to the first half of 2022 and consists of 5,424 audit reports across a variety of different types of DeFi ventures, of which 5,343 have complete data such as release date and audit purposes.[12] We augment the data with hand-collected details such as who performed these audits, how the audits are performed, the number of auditors employed on each project, the days spent on the audit, the audit methodology used, audit report length, pass scores (if available), total items checked and total issues, major and minor issues, and issues that have been fixed by the client before the report was published. Note that consistent with the language used by practitioners, we refer to the engagements in our sample as *smart contract audits*, acknowledging that terms such as *audit*, *assurance*, and *attestation* are used in existing research to denote various other client interactions.

A representative example from our sample is Certik's audit of 1inch Mooniswap v2. For this audit, the audit report spans 49 pages and the audit methodology, which is identified in the audit summary, includes both automatic and manual analyses. The audit report also

[11] See `https://blog.de.fi/introducing-the-worlds-first-web-archive-of-smart-contract-audits-902898464ea4`.

[12] 2014 and 2016 only consist of five audit reports and are dropped from the main sample.

mentions the audit team size (2 consultants), the number of days spent on the audit (15 days), the total number of items checked (36 items), and the number of major and minor issues identified (no major issues, 3 medium issues, 5 minor issues, and 28 informational issues). For these 36 issues, all were deemed as resolved or only carried advice, which we count as 36 fixed issues and no outstanding open issues. Appendix B provides more details on this example.

We also collect market data such as total value locked in a contract and venture returns from Defilama.com and Coingecko.com for available DeFi ventures and market benchmarks (CCMIX, Bitcoin, and 21Shares Crypto Basket). The total value locked, or TVL, is a key metric that represents the monetary value of digital assets held in a smart contract, such as collateral for loans or liquidity pools for trading. We also collect data on DeFi cyber attacks for the ventures in our sample from DEFIYIELD, which provides data on scams, hacks, and exploits. The variables are described further in Appendix A.

4 The landscape of smart contract audit firms

The market for smart contract audits, being relatively unstudied in the literature, requires some background information. Therefore, in the first part of our study, we provide detailed evidence on the overall market for smart contract audits, examine the types of audit firms providing smart contract audits, and examine more specific details of the audit process in two examples.

4.1 The universe of DeFi auditors

We start by exploring the number and origin of audit firms in the DeFi space. After collecting audit reports from DeFi Yield, we compile a list of the firms that conduct the audits, which is tabulated alphabetically in Table 1. We find that the smart contract audits in our sample are conducted by 91 unique auditors. We next manually check the origin of these firms and find that none were started by financial statement audit firms. Rather, these firms from the outset have specialized in technical audits and typically have founders with backgrounds in computer science, engineering, and blockchain. These findings speak to Bauer et al. (2022), who classify smart contract audits as an "uncertain" area of development in the audit market that we know little about. On the one hand, Bauer et al. (2022) note that smart contract audits relate to internal controls and thus correspond to financial statement audits and the expertise of CPA firms. On the other hand, they also stress that the lack of widely-accepted criteria to benchmark smart contract audit processes will require audit-specific evaluation criteria, which may reduce the ability of audit firms to scale their services and potentially deter new entrants into the market.

The prominence of "technical" audit firms, composed primarily of engineers and computer scientists rather than accounting experts, does not imply that financial audit firms will not gain market share in the future. As financial audit firms hire more technical employees (Law and Shen 2021; Fedyk et al. 2022), they might develop the appropriate expertise and desire to enter the market for smart contract audits, especially if the fees increase for this type of engagement. They also appear to be trying to enter the space through acquisition: 2 of our 91 unique auditors have already been acquired by large accounting firms. In addition, in 2020, PwC Switzerland partnered with smart contract audit firm ChainSecurity and hired several engineers from ChainSecurity to bolster PwC's smart contract audit business.[13] In 2021, Deloitte acquired Root9B, a "generalist" company, which was founded in 2011 and is a leading provider of advanced cyber threat solutions, including smart contract audits.

4.2 Detailed examples of DeFi Auditors

DeFond and Zhang (2014, p. 294) and Efendi et al. (2006) make a strong case for the need to analyze auditors' expertise beyond financial statement audits. Therefore, to give readers a flavor of the audit firms and the boundaries of the audits we focus on in this paper,

[13] See https://www.coindesk.com/markets/2020/01/10/pwc-switzerland-incorporates-chainsecurity-team-to-expand-blockchain-audit-tools/.

we provide a description of two audit firms in the industry: Certik and Hacken.

4.2.1 Certik

Certik is a prominent DeFi smart contract audit firm established in 2018 by professors at Columbia and Yale and former senior software engineers from Google and Facebook. Certik's current CEO, Ronghui Gu, has a PhD in computer science from Yale and still holds an assistant professorship in computer science at Columbia. According to LinkedIn, Certik's workforce consists of employees with PhDs, masters degrees, and bachelors degrees in various technology-related fields. Certik service offerings include smart contract security assessments, on-chain monitoring, "know your customer" verification, penetration testing, bug bounty programs, wallet tracing and visualization, incident response, and formal verification. According to Certik's website, as of April 2023, Certik has served over 3,700 clients with a combined market value of about $370 billion, including Goldman Sachs and Sequoia partners.

To exemplify a client relationship, one of Certik's largest clients is Binance, which is one of the world's leading digital asset exchanges whose infrastructure serves as the foundation for many DeFi projects and applications. According to Certik's website, Binance engaged Certik in an effort to enhance its network safeguards across its numerous decentralized applications.[14]

Client case studies posted to Certik's website suggest that their audit process typically involves examining the client's in-scope code and then creating a report outlining the title, type, and severity of identified code issues. These issues can include, for example, explicit coding errors, general security vulnerabilities, or the failure to follow best practices. They then provide a description, recommendation, and alleviation plan for each issue. For example, they might discover a critical code issue and suggest how to correct it.

[14] For more detail on this client relationship, see `https://skynet.certik.com/projects/binance`.

4.2.2 Hacken

Hacken was established in 2017, specializes in smart contract audits, and has over 1,000 clients and 100 employees. Hacken's current CEO, Dyma Budorin, has over 10 years of work experience at Deloitte. As of April 2023, Hacken has conducted over 2,000 audits. One of Hacken's clients is CoinGecko, which is the world's largest cryptocurrency data aggregator and serves over 50 million users. According to Hacken's website, CoinGecko engaged Hacken to perform thorough penetration testing of its smart contracts whereby Hacken assessed CoinGecko's systems for vulnerabilities. Beyond smart contract audits, Hacken performed penetration testing at CoinGecko to assess a new feature added to their client application. Hacken also penetration-tested CoinGecko application processing interfaces that are used almost universally in the crypto market.

Like Certik, Hacken's audit process typically involves a thorough examination of the client's smart contracts and related code. The team identifies potential vulnerabilities, coding errors, and deviations from best practices. Once the assessment is complete, Hacken provides the client with a detailed report outlining each issue's title, type, and severity, along with recommendations and a mitigation plan to address each identified issue.

4.3 Market structure

The market for the financial statement audits of public firms is highly concentrated, with the Big 4 audit firms accounting for 74% of the audit engagements at public firms globally in 2020 (e.g., International Accounting Bulletin 2021). However, it was not always this way: this market was much less concentrated in the mid and late 20th century (Ferguson et al. 2022). To put the structure of the market for smart contract audits into perspective, in Table 2, we tabulate the market share of the 20 largest auditors in our sample. We find that the largest audit firm, TechRate, captured close to 30% of the engagements in our sample. This audit firm provides relatively homogeneous entry-level service at low cost (starting at

$250 per audit) relative to other audit firms in the industry. We also find that the next three largest audit firms combined only account for 20% of market share, with Certik holding 10% by itself. Over our sample period, only three audit firms account for more than 5% of the total engagements. These findings show that the market for smart contract audits is currently not highly concentrated.

Table 3 reports venture characteristics for our sample, specifically focusing on the average number of audits and auditors per project. For the full sample, the average number of audits per venture is 1.24, with a median of 1.00 and a maximum of 20.00. The average number of auditors per venture is 1.10, with a median and minimum of 1.00 and a maximum of 17.00. For the sub-sample with market prices, the average number of audits per venture increases to 1.78, with a median of 1.00 and a maximum of 19.00. The average number of auditors per venture is slightly higher at 1.35, with a median and minimum of 1.00 and a maximum of 5.00.

As Table 3 highlights, DeFi ventures have the option to obtain multiple audits of their smart contracts. Multiple audits may be useful to help gain added assurance or if the venture alters the code of the smart contract. In our sample, 3,791 DeFi ventures received a single audit during our sample period, while 518 ventures received at least two audits (1,552 reports). Among DeFi ventures with multiple audits, we observe that over 63% (326 ventures) chose a different auditor between the first and second audits. We also observe that 85% of the ventures who do not change auditors were not using TechRate as an auditor. We also find that among ventures that changed auditors, 54% (70) of those using TechRate as their first auditor chose a different auditor for their second audit. These findings suggest that DeFi ventures may be selecting audit firms based on the differences in services they offer, as TechRate typically provides only a basic vanilla service.

4.4 Audit pricing

We next provide some information on the pricing of smart contract audits. Unlike public firms, DeFi ventures are not required to disclose their audit fees and so we do not have data on audit pricing for our sample. We therefore instead collect pricing data from institutional sources.

We observe large variations in smart contract audit pricing that appear to be driven by the quality and scope of the service provided, similar to financial statement audits. According to the ranking of smart contract auditor firms provided by Boxmining (a leading resource on news related to digital assets), the top 10 DeFi auditors ranked by quality include: Hacken, Quantstamp, Trail of Bits, OpenZeppelin, ConsenSys Diligence, Certik, LeastAuthority, Chainsecurity, Slowmist, and Runtime Verification.[15] Next, we obtain general pricing data from the DeFi Security Alliance.[16]. We find that higher ranked auditors charge higher fees. For instance, the fees of Quantstamp, OpenZeppelin, and Trail of Bits are set at $\$5,000$. Hacken's fees start at $\$9,000$, which is consistent with Hacken's website that notes a smart contract audit typically requires between two to 14 days and costs between $12,000 and $18,000 per contract.[17] The most prominent auditor in our sample in terms of the number of projects audited is TechRate, which offers more homogeneous entry-level services that range in price from $250 to $1,500.

Overall, it appears that the pricing of a smart contract audit depends on the complexity and length of the smart contract code, the expertise and reputation of the auditing firm, the scope of the audit, and other factors. Intuitively, more complex smart contracts with more lines of code typically require more review and analysis, leading to higher audit costs. Additionally, the level of customization and unique features within the smart contract can also impact pricing. Auditor reputation and industry expertise are also likely to be priced into the audit fees.

[15] See https://boxmining.com/top-blockchain-security-firms/

[16] See https://defisec.info/members

[17] See `https://hacken.io/services/blockchain-security/smart-contract-security-audit/`.

5 The smart contract audit process

We build on the previous section by next focusing on the smart contract audit process. We rely on general institutional details enriched by our own understanding gained from the granular coding of 5,343 audit reports from 2017 to 2022. To put these details into context, we draw comparisons to financial statement audits when appropriate.

We begin by looking at various audit methodologies provided on the websites of the leading audit firms in the DeFi space, including Certik and Solidity. We find that the audit process is usually a collaborative process that starts with the client sending to the audit firm its source code, deployment scripts, and any available technical documentation or white paper to help understand what the code aims to achieve. In contrast to financial statement audits whose audit teams typically obtain detailed prior working papers (e.g., Bonner and Majors 2022), the majority of the ventures in our sample only acquire one audit of their smart contract, which means the audit work usually starts from scratch. Also unlike financial statement audits, the smart contract audit process is not governed by a standard setter (Bauer et al. 2022).

After the audit firm acquires the appropriate documentation, it begins the audit of the smart contract. Table 4 reports information about the audit process collected from our large sample of audit reports. In over 80% of the cases, the report states that a team performed the audit, without specifying the exact number of team members (See Panel A). In less than 2% of the cases, the report states that a single individual ran the audit process, while in around 12% of the cases, the report explicitly refers to a team of either two or three members. In terms of duration, the majority of the audit reports (75%) do not mention the time spent in completing the audit (see Panel B). Among the remaining reports, roughly half mention spending more than one day but less than a week on the report while the other half reports spending over a week on the audit.

The inspection phase of the audit typically proceeds in two steps. First, the formal verification process starts with automated testing. Ideally, this process checks every variable of a smart contract against each value it may take. Put differently, every possible state of a smart contract is calculated. The spirit of that process resembles stress testing of financial institutions (Goldstein and Sapra 2014). Audit firms often employ so-called formal automated verification engines that should find any inputs that result in issues that work against the smart contact's logical integrity.

Second, a manual review follows the automated inspection. During the manual review, the audit team goes through each line of code and inspects it for known vulnerabilities and coding errors. Common vulnerabilities encountered include, for example, centralization risk, lack of proper input validation, or reliance on third-party dependencies. The manual review ensures that issues missed by the automated process are identified to reduce the risk of harmful exploits. In our sample of smart contract audits, around half of the reports do not provide information on the methods used. While there is again no private or public standards imposing the use of automated and manual testing methods, nearly all the audit reports that disclose information about their methods state that they combine automated testing with a manual review (See Panel C of Table 4). Interestingly, revealing the testing method seems to be associated with the quality and depth of the service. Indeed, none of the reports from TechRate, the "low-cost" player in the space, mention any information related to the testing methodology, while the Top ranked audit firms (as ranked by Boxmining) systematically refer to a combination of automated and manual testing processes.

In conventional public capital markets, auditors conduct an audit to obtain sufficient evidence to obtain reasonable assurance as to whether the management of the firm has prepared financial statements in accordance with local accounting standards. Historically, this process was summarized in a coarse audit opinion. Recent regulatory interventions have led to a new generation of expanded audit reports that now include disclosures about significant matters in a company's financial reporting processes and its audit (e.g., Minutti-Meza 2020). The goal of such expanded audit reports was to increase the information content and usefulness of audit opinions and help stakeholders better monitor auditors and managers. Smart contract audit reports are similar in this regard.

First, in terms of length, smart contract audit reports are much longer than expanded audit reports. Recent studies found that expanded audit reports among public firms in the United Kingdom typically are still rather short, at about one and a half page long (Gutierrez et al. 2022). In contrast, smart contract audit reports about DeFi ventures are, on average, 17 pages long (See Table 5). The length of the reports presents considerable variation, with those reports being 9 (19) pages long at the 25^{th} (75^{th}) percentile of the distribution, with the maximum reaching up to 277 pages. When comparing the auditors deemed to deliver high-quality audits with the remaining auditors, they provide significantly longer reports (21 pages).

Second, in terms of outputs, both types of reports highlight sources of risk. For example, a recent study by Lennox et al. (2022) documents that expanded audit reports from UK firms contain around four risks of material misstatements. In smart contract audit reports, issues are normally categorized according to their severity, into, for example, minor or major issues. Absent private and public standards, auditors often come up with their own classification of issues. For example, in its 2020 audit report about the smart contract of 88MPH, Peckshield detailed its "Vulnerability Severity Classification", a two-dimensional matrix based on the likelihood of occurrence and impact of an issue (See Figure 1). We find that, on average, audit reports in our sample highlight 0.55 major issue and 5 minor issues. High-quality auditors find on average significantly more major (1 issue) and minor issues (8 issues) (see Table 5 Panel B).[18] In the Fall of 2019, Trail of Bits audited the smart contract of Aave Protocol, an open-source protocol aiming to create non-custodial liquidity markets to earn interest on supplying and borrowing assets with a variable or stable rate. In its reports, Trail of Bits documents 15 issues. One major (high severity) issue pertains to the lack of access controls over the function used to update the borrower's information. The report notes

[18] The major issue category includes any disclosed major and critical issue, whereas the minor issue category includes minor, medium and informational issues.

that this particular function could be called by any user, allowing an attacker to potentially manipulate some state variables for specific users. The report also identified a minor (low severity) issue about the repayment function that allowed the return of the funds borrowed to be repaid on behalf of other users, allowing for some potential front-running.

It should be noted that the amount of reported issues does not speak strictly about the quality of the code. Indeed, absent audit standards, the issues identified in the reports are a function of both the underlying quality of the code and the effort and expertise of the audit team. In fact, in our sample, top-quality auditors (as ranked by Boxmining) are far more likely to report issues than TechRate, which almost exclusively reports clean sheets. In the next section, we highlight that this finding likely reflects audit effort and the selection of high-quality auditors by high-quality ventures as ventures audited by top-quality auditors are far more likely to get listed on an exchange, a typical measure of entrepreneurial success in that space (e.g., Howell et al. 2020).

While both financial audits and smart contract audit reports summarize the issues and risks encountered during the audit process, smart contract audit reports also contain information about the inputs and detailed process. This is not surprising given that absent private or public audit standards audit firms will follow different audit processes of varying depth and quality. As a result, smart contract audit reports typically contain a list of specific items checked on the code. In our sample, auditors state that, on average, their audit process checked 20 unique items on the code of the smart contract. Unsurprisingly, we also observe variation with 15 (21) items checked at the 25^{th} (75^{th}) percentile of the distribution, with the maximum reaching up to 184 items. Interestingly, some auditors have developed and update their proprietary audit standards that they apply to multiple engagements. For example, Certik built a proprietary static analysis tool to scan the code of smart contracts searching for specific potential issues. We reproduce the list of issues that they try to detect in Figure 2 (as extracted from the smart contract audit report of Certik in 2019).

Auditing of public companies is currently organized around a clearly mandated separation of audit and consulting services, leading the audit process to focus exclusively on reviewing the adequate preparation of financial statements with respect to accounting standards. In the unregulated audit market for DeFi ventures, auditors provide varying degrees of services. Some "low-cost" auditors, like TechRate, only opine on detecting vulnerabilities in the code. Other auditors differentiate their services by offering technical solutions to their detected issues. For example, in the previously mentioned report of Aave Protocol, Trail of Bits included a series of high-level short-term and long-term modifications to improve the code from the detected vulnerabilities, followed with technical suggestions about how to modify the function in the code to implement the suggested corrections. The audit process is also iterative as the higher quality auditors offer to iterate with the DeFi venture to certify whether some identified issues have been resolved or not. For example, the initial report for Aave Protocol was released on September 6, 2019. After modifications of the code, some functions were retested by Trail of Bits and an additional appendix was added to the report and released publicly on September 25, 2019. In our large sample of smart contract audit reports, we find that, on average, 2.43 issues per audit report have been fixed through iterations between the developers of the DeFi venture and the audit team. Again the top-quality auditors have significantly more issues resolved during the audit process than the rest of the auditors (almost 5 issues fixed per report),

Finally, we observe variation in terms of the nature of assurance provided. Some reports simply state whether they found any issues and discuss their severity, whereas other reports provide more specific details and certification. For example, Certik's report of 12 SHIPS stresses that "Certik believes that this smart contract passes security qualifications to be listed on digital asset exchanges." Similar to financial audits, smart contract audit reports do not guarantee the integrity of a smart contract; rather they advise caution in relying on the report. Reports often highlight that audits should not be used as investment advice.[19]

6 The value relevance of smart contract audit reports

We next use returns to measure the usefulness of smart contract audit reports to stakeholders. We cannot answer this question with existing audit research because there are substantive differences in the institutional features of our setting compared to previously studied audits such as financial statement audits. First, the incentives of our audit firms and DeFi ventures differ from those of conventional audit firms and public companies. For example, DeFi ventures' investors are not investors in the traditional sense: although they can hold their investment (or "token") for investment purposes, they can also redeem it for a product or service. Second, unlike financial audits, smart contract audits are not targeted at reducing information asymmetry between managers and investors, but rather between firms and customers. Third, unlike financial audits whose costs are ultimately borne by shareholders, DeFi ventures themselves pay for smart contract audits. Fourth, smart contract audits are not regulated like financial audits, and legal protections are largely absent in this market. Fifth, the nature of the audit outputs differ: smart contract audit reports provide a detailed explanation of any problems identified by the audit team and whether these problems were corrected by the client, whereas financial statement audits provide only a coarse opinion on the client's financial statements and integrated internal controls. Thus, the value of smart contract audits is an empirical question.

We must also consider the possibility of unraveling in the disclosure sense because audit clients can decide whether or not to release the audit report. If not releasing an audit report is interpreted as a worse signal than releasing an audit report that identifies problems, we

[19] For example, the smart contract audit report of Aave Protocol by Peckshield states on page 9: "Note that this security audit is not designed to replace functional tests required before any software release, and does not give any warranties on finding all possible security issues of the given smart contract(s), i.e., the evaluation result does not guarantee the nonexistence of any further findings of security issues. As one audit-based assessment cannot be considered comprehensive, we always recommend proceeding with several independent audits and a public bug bounty program to ensure the security of smart contract(s). Last but not least, this security audit should not be used as investment advice."

would observe the release of both "good" and "bad" news audit reports and see a spectrum of positive and negative returns in our sample (Verrecchia 1983). Relatedly, as with any disclosure choice, the venture releasing the audit report may not be able to accurately predict the market reaction to the audit report, which could again lead us to observe a mix of positive and negative returns around the release of the audit report (Dye 1985). For example, although a smart contract's code is open source, a client may be uncertain about whether stakeholders can accurately evaluate the quality of a smart contract on their own. If they can, there might be no systematic market reaction to the release of the audit report—something a client would learn only after releasing the report. Finally, ex-ante, it is not possible to determine the exact magnitude of any returns reaction, which may be large because the audit report is in effect an opinion on whether a smart contract functions as intended. Therefore, the direction and magnitude of any returns effect are ambiguous, which leads us to our main returns tests.[20]

We adopt a widely used method to measure the usefulness of audit reports from prior studies on financial statement audits, which typically examine the market return around the release date of these reports.[21] Menon and Williams (2010), for example, examine returns to going-concern audit opinions over the three days beginning with the event date. One advantage of our setting over financial statement audits is that the release of our audit reports is not bundled with the release of the information it is auditing (e.g., Gipper et al. 2019). We first measure returns at the venture associated with the smart contract audit report over the windows of [0, +1 day], [0, +3 days], and [0, +5 days], where day 0 is the release date of the audit report. We then subtract from these values a returns baseline constructed by applying the market model to compute an expected return over an estimation

[20] Prior empirical research also finds mixed results on how the market reacts to differences in financial statement audit reports, further compelling us to investigate returns around our audit reports (for a survey of these results, see Section II of Menon and Williams 2010).

[21] Specifically, we use the release date of the report, as shown in the report file, as the date on which the information gets released to market participants. The ventures often post the reports on their website, GitHub repository, and/or their auditor's repository on the same date as the release date noted in the report. For a random sub-sample of reports, we check and find no evidence of release dates that differ between the report and when the report was published to one of these repositories.

window leading up to but not including day 0. In selecting the returns benchmarks, we follow prior research (Ramos et al. 2021) and use different indices to proxy for the market return, including the Crescent Crypto Market Index (CCMIX), which is a cryptocurrency market index that evaluates the performance of the largest and most liquid cryptocurrencies. We also incorporate other benchmarks such as Bitcoin and a 21Shares Crypto Basket containing Bitcoin, Ethereum, Polkadot, Solana, and Binance Coin. Note that our returns analysis has significant sample attrition because detailed returns data are not available for all our ventures, which is common in this literature. Howell et al. (2020, Table 1), for example, lose about 60% of their sample of 1,520 initial coin offerings due to the lack of available returns data.

Table 6 presents empirical results on the market reaction to the release of smart contract audit reports, with the results divided into two panels. Panel A provides descriptive statistics for the cumulative abnormal return (CAR) at different event windows: [0, +1 day], [0, +3 days], and [0, +5 days]. The mean CAR values are positive and statistically significant for each event window, indicating that on average, the market reacts positively to the release of smart contract audit reports. The mean CAR values increase as the event window lengthens from [0, +1 day] to [0, +5 days], with a +11.6% effect for [0, +1 day], a +23.6% effect for [0, +3 days], and a +35.3% effect for [0, +5 days] (1% level for all). The magnitudes of the mean returns also account for a meaningful proportion of the standard deviation in the returns, which is a testament to the economic significance of the results. Table 6, Panel B focuses on univariate returns tests (against zero) for three different benchmarks: CCMIX, Bitcoin, and a 21Shares Crypto "Basket" containing Bitcoin, Ethereum, Polkadot, Solana and Binance Coin (Ramos et al. 2021). For each benchmark, the CAR values across the three event windows are largely consistent with those reported in Panel A and are again statistically significant. This further supports the notion that the market generally reacts positively to the release of these audit reports. Moreover, the consistency of CAR values and statistical significance across different benchmarks suggests that the observed market reactions are robust and not confined to a single benchmark.

We next turn to cross-sectional variation in the returns. Our first cross-sectional test focuses on firms that receive single versus multiple smart contract audits. Table 7, Panel A shows that returns are higher for audit reports when the report is the sole report received by the venture, relative to an audit report that is one of multiple audit reports released by a venture. This differential in returns increases in magnitude as we lengthen the return window. This finding is consistent with there being diminishing marginal returns to audits, which could happen for at least a couple of reasons. First, the audit scope at the same venture is likely to have at least some overlap across multiple audits, which would reduce the informativeness of the audit reports. Second, stakeholders are likely to assume at least some persistence in the quality of the venture's smart contract, which would also reduce the informativeness of the audit report (i.e., a previous smart contract audit report is likely informative about the quality of future smart contracts).

Our next cross-sectional test compares the returns for smart contract audits that identify no major issues to those that do identify major issues. Table 7, Panel B shows that audits that identify no major issues have higher returns than those that identify major issues, although both types of audit reports have positive returns overall. The differential in returns is small in the [0, +1 day] window but increases in magnitude as we lengthen the return window. That both types of audit reports exhibit similar positive returns is not unusual, as smart contract audits give the client the chance to remediate any issues identified by the audit before the audit report is created. Indeed, even audits that identify major issues appear to be interpreted as a positive signal by stakeholders on net.

Our next cross-sectional test examines whether returns vary according to whether ventures have experienced a cyber attack prior to the audit. Table 7, Panel C shows that ventures that experienced such an attack see lower returns for their smart contract audits, with on average returns that are not statistically different from zero. Firms that have *not* experienced such an attack see larger returns for their smart contract audits, with on average returns that increase from the overall sample average in Table 6, Panel B. One interpretation of this result is that after a venture experiences an attack, trust in the venture is largely lost, and not even an audit can help the venture regain it.

We also perform several untabulated tests. We examine whether returns vary based on the audit firm's market share. We find that returns are consistently larger for audit reports from smaller audit firms, but this difference is not statistically significant. This finding contradicts the assumption in the financial statement audit literature that audit quality improves with audit firm size due to increased reputation costs and litigation risks that escalate with size (DeFond and Zhang 2014, p. 278). Nonetheless, it is important to note that the smart contract market is subject to a significantly distinct legal and reputational environment compared to that of public equities. Specifically, in a young and growing audit market such as this one, smaller audit firms may be incentivized to provide a higher quality product to gain market share. We also examine whether the returns vary based on audit report length, as measured by page length. One possibility is that a longer audit report might be associated with audit quality, i.e., it might be more informative and detailed than a shorter report and result in a larger market reaction. This effect, however, may be negated if a longer audit report indicates more qualifications to the audit or reveals more issues or complexity. We do not find that returns are substantively different for longer versus shorter audit reports.

To summarize, we provide some of the first evidence that returns are consistently positive and economically significant around the release of the smart contract audit reports in our sample, suggesting that these audits add value to the clients that receive them.

7 Conclusion

In today's capital markets, smart contracts play an increasingly important role in structuring and executing common financial transactions such as loans and venture capital funding, with more than $200 billion now locked in such contracts (OECD 2022). A major risk when using smart contracts is theft that can result from coding errors and incomplete contracts (Makarov and Schoar 2022). As a result, several leading financial organizations have issued white papers explicitly calling for independent third-party audits of the code underlying smart contracts (e.g., Federal Reserve 2022; OECD 2022). Using hand-collected data from DeFi ventures, we provide some of the first large-sample evidence on the emergence of voluntary smart contract audits. We find that (1) these audits are pervasive in our sample, (2) the audit firm market is composed of many new entrants, (3) the scope of these audits mainly covers technical issues such as the smart contract's underlying code, and (4) the market reaction to the release of the audit reports is unambiguously positive and economically significant at +10%, on average. Smart contract audits are thus an important example of how blockchain technology is affecting the demand for audit services.

Overall, our research speaks to the numerous recent critiques of the accounting literature that emphasize the need to broaden our understanding of the market for audit services by analyzing new settings and new data (e.g., Bloomfield et al. 2016; Gerakos and Syverson 2017; Gow et al. 2016; Knechel and Willenborg 2016; Leuz 2018; Leuz and Wysocki 2016). Studying other areas of the evolving DeFi market where external verification plays a role may be a fruitful path for future research.

References

Allee, K. and Yohn, T. (2009). 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*, 84:1–25.

Anderson, C., Fang, V., and Moon, J. Shipman, J. (2022). Accounting for cryptocurrencies. *Working Paper (Available at: SSRN link).*

Aramonte, S., Huang, W., and Schrimpf, A. (2021). DeFi risks and the decentralisation illusion. *BIS Quarterly Review.*

Bauer, T., Boritz, E., Fiolleau, K., Pomeroy, B., Vitalis, A., and Wang, P. (2022). Cataloguing the marketplace of assurance services. *Working Paper (Available at: SSRN link).*

Bauer, T., Estep, C., and Malsch, B. (2019). One Team or Two? Investigating Relationship Quality between Auditors and IT Specialists: Implications for Audit Team Identity and the Audit Process. *Contemporary Accounting Research*, 36:2142–2177.

Bloomfield, R., Nelson, M., and Soltes, E. (2016). Gathering Data for Archival, Field, Survey, and Experimental Accounting Research. *Journal of Accounting Research*, 54(2):341–395.

Bonner, S. and Majors, T. (2022). The effects of formality of documentation on auditors' acquisition of knowledge from prior year workpapers. *Working Paper (Available at: SSRN link).*

Bourveau, T., Breuer, M., Koenraadt, J., and Stoumbos, R. (2023). Public company auditing around the Securities Exchange Act. *Working Paper (Available at: SSRN link).*

Bourveau, T., De George, E., Ellahie, A., and Macciocchi, D. (2022). The role of disclosure and information intermediaries in an unregulated capital market: Evidence from Initial Coin Offerings. *Journal of Accounting Research*, 60:129–167.

Cong, L. and He, Z. (2019). Blockchain Disruption and Smart Contracts. *Review of Financial Studies*, 32:1754–1797.

Cong, L., Li, Y., and Wang, N. (2021). Tokenomics: Dynamic adoption and valuation. *Review of Financial Studies*, 34:1105–1155.

Cong, L., Li, Y., and Wang, N. (2022). Token-based plateform finance. *Journal of Financial Economics*, 144:972–991.

Dee, C., Lulseged, A., and Zhang, T. (2011). Client stock market reaction to PCAOB sanctions against a Big Four auditor. *Contemporary Accounting Research*, 28:263–291.

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

Duflo, E., Greenstone, M., Pande, R., and Ryan, N. (2013). Truth-telling by Third-party Auditors and the Response of Polluting Firms: Experimental Evidence from India. *Quarterly Journal of Economics*, 128:1499–1545.

Duflo, E., Greenstone, M., Pande, R., and Ryan, N. (2018). The Value of Regulatory Discretion: Estimates From Environmental Inspections in India. *Econometrica*, 86:2123–2160.

Dye, R. (1985). Disclosure of Nonproprietary Information. *Journal of Accounting Research*, 23:123–145.

Efendi, J., Mulig, E. V., and Smith, L. M. (2006). Information Technology and Systems Research Published in Major Accounting Academic and Professional Journals. *Journal of Emerging Technologies in Accounting*, 3:117–128.

Federal Reserve (2022). Decentralized Finance (DeFi): Transformative Potential & Associated Risks. `https://www.federalreserve.gov/econres/feds/decentralized-finance-defi-transformative-potential-and-associated-risks.htm`.

Fedyk, A., Hodson, J., Khimich, N., and Fedyk, T. (2022). Is artificial intelligence improving the audit process? *Review of Accounting Studies*, 27:938–985.

Ferguson, C., Pinnuck, M., and Skinner, D. (2022). The evolution of audit market structure and the emergence of the Big 4: Evidence from Australia. *Working Paper (Available at: SSRN link)*.

Fisch, C. (2019). Initial coin offerings (ICOs) to finance new ventures. *Journal of Business Venturing*, 34:1–22.

Gerakos, J. and Syverson, C. (2015). Competition in the audit market: Policy implications. *Journal of Accounting Research*, 53:725–775.

Gerakos, J. and Syverson, C. (2017). Audit firms face downward-sloping demand curves and the audit market is far from perfectly competitive. *Review of Accounting Studies*, 22:1582–1594.

Gipper, B., Leuz, C., and Maffett, M. (2019). Public oversight and reporting credibility: Evidence from the PCAOB audit inspection regime. *Review of Financial Studies*, 33:4532–4579.

Gipper, B., Ross, S., and Shi, S. (2022). ESG assurance in the United States. *Working Paper (Available at: SSRN link)*.

Goldstein, I. and Sapra, H. (2014). Should banks' stress test results be disclosed? An analysis of the costs and benefits. *Foundations and Trends in Finance*, 8(1):1–54.

Gow, I., Larcker, D., and Reiss, P. (2016). Causal inference in accounting research. *Journal of Accounting Research*, 54(2):477–523.

Gutierrez, E., Minutti-Meza, M., Tatum, K., and Vulducheva, M. (2022). Consequences of expanded audit reports: Evidence from the United Kingdom's alternative investment market. *Working Paper (Available at: SSRN link).*

Harvey, C., Ramachandran, A., and Santoro, J. (2021). *DeFi and the Future of Finance.* Wiley.

Healy, P. and Palepu, K. (2001). Information Asymmetry, Corporate Disclosure, and the Capital Markets: A Review of the Empirical Disclosure Literature. *Journal of Accounting and Economics*, 31:405–440.

Howell, S., Niessner, M., and Yermack, D. (2020). Initial coin offerings: Financing growth with cryptocurrency token sales. *Review of Financial Studies*, 33:3925–3974.

Hu, D., Leone, A., and Zhang, V. (2020). Credible disclosure signals in unregulated markets: Evidence from initial coin offerings. *Working Paper (Available at: University link).*

International Accounting Bulletin (2021). Accounting giants continue to dominate the market despite pandemic. `https://www.internationalaccountingbulletin.com/news/accounting-giants/`.

John, K., Kogan, L., and Saleh, F. (2023). Smart contracts and decentralized finance. *Annual Review of Financial Economics (forthcoming).*

Kausar, A., Shroff, N., and White, H. (2016). Real effects of the audit choice. *Journal of Accounting and Economics*, 62:157–181.

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

Knechel, W. R. and Willenborg, M. (2016). Economics-based Auditing Research Published in JAR. *Journal of Accounting Research.* Virtual Issue.

Kogan, S., Makarov, I., Niessner, M., and Schoar, A. (2023). Are cryptos different? Evidence from retail trading. *Working Paper (Available at: SSRN link).*

Kreps, D. (1990). *A Course in Microeconomic Theory.* Princeton University Press.

Law, K. and Shen, M. (2021). How does artificial intelligence shape audit firms? *Working Paper (Available at: SSRN link).*

Lawrence, A., Minutti-Meza, M., and Zhang, P. (2011). Can Big 4 versus non-Big 4 differences in audit-quality proxies be attributed to client characteristics? *The Accounting Review*, 86:259–286.

Lennox, C. and Pittman, J. (2011). Voluntary audits versus mandatory audits. *The Accounting Review*, 86:1655–1678.

Lennox, C., Schmidt, J., and Thompson, A. (2022). Why are expanded audit reports not informative to investors? evidence from the United Kingdom. *Review of Accounting Studies (forthcoming).*

Leuz, C. (2018). Evidence-based policymaking: promise, challenges and opportunities for accounting and financial markets research. *Accounting and Business Research*, 48(5):582–608.

Leuz, C. and Wysocki, P. (2016). The Economics of Disclosure and Financial Reporting Regulation: Evidence and Suggestions for Future Research. *Journal of Accounting Research*, 54(2):525–622.

Lisowsky, P. and Minnis, M. (2020). The silent majority: Private U.S. firms and financial reporting choices. *Journal of Accounting Research*, 58:547–588.

Lisowsky, P., Minnis, M., and Sutherland, A. (2017). Economic growth and financial statement verification. *Journal of Accounting Research*, 55:745–794.

Makarov, I. and Schoar, A. (2022). Cryptocurrencies and decentralized finance (DeFi). *Working Paper (Available at: NBER link).*

Mansi, S., Maxwell, W., and Miller, D. (2004). Does auditor quality and tenure matter to investors? Evidence from the bond market. *Journal of Accounting Research*, 42:755–793.

Menon, K. and Williams, D. (2010). Investor reaction to going concern audit reports. *The Accounting Review*, 85:2075–2105.

Minnis, M. (2011). The value of financial statement verification in debt financing: Evidence from private U.S. firms. *Journal of Accounting Research*, 49:457–506.

Minutti-Meza, M. (2020). The art of conversation: The expanded audit report. *Working Paper (Available at: SSRN link).*

OECD (2022). Why Decentralised Finance (DeFi) Matters and the Policy Implications. `https://www.oecd.org/daf/fin/financial-markets/Why-Decentralised-Finance-DeFi-Matters-and-the-Policy-Implications.pdf`.

Ramos, S., Pianese, F., Leach, T., and Oliveras, E. (2021). A great disturbance in the crypto: Understanding cryptocurrency returns under attacks. *Blockchain: Research and Applications*, 2:100021.

Rivera, T., Saleh, F., and Vandeweyer, Q. (2023). Equilibrium in a DeFi lending market. *Working Paper (Available at: SSRN link).*

Schar, F. (2021). Decentralized finance: On blockchain- and smart contract-based financial markets. *Federal Reserve Bank of St. Louis Review*, Second Quarter:153–174.

Schoenfeld, J. (2022). Cyber risk and voluntary service organization control (SOC) audits. *Review of Accounting Studies (forthcoming).*

Schwarcz, S. and Bourret, R. (2023). Fractionalizing investment securities: Using FinTech to expand financial inclusion. *Ohio State Law Journal (forthcoming)*.

Verrecchia, R. (1983). Discretionary disclosure. *Journal of Accounting and Economics*, 5:179–194.

Watts, R. and Zimmerman, J. (1983). Agency problems, auditing, and the theory of the firm: Some evidence. *Journal of Law and Economics*, 26:613–633.

Werbach, K. and Cornell, N. (2017). Contracts ex machina. *Duke Law Journal*, 67:313–382.

Willenborg, M. (1999). Empirical analysis of the economic demand for auditing in the initial public offerings market. *Journal of Accounting Research*, 37:225–238.

Appendix A: Variable Definitions

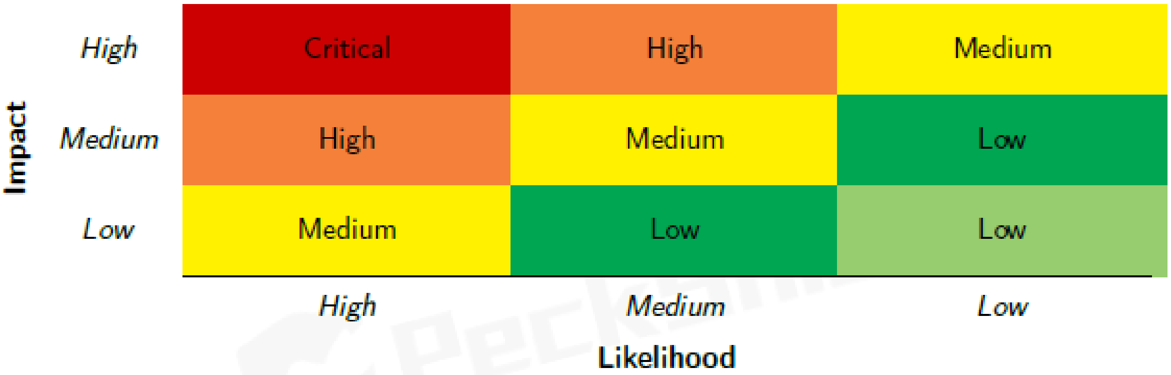
Variable	Definition	Source
Venture	Project or protocol that gets audited.	*defiyield.app*
Audit report	Audit report in .pdf format that is released online by the auditor on the release date.	*defiyield.app*
Auditor	Firm that conducts the audit of the venture.	*defiyield.app*
Release date	The date at which the audit report was made public/released as shown in the PDF.	*defiyield.app*
Page number	Number of total pages of an audit report.	*audit report*
Items checked	Number of total items in an audit report that was checked during the audit process.	*audit report*
Major issues	Number of major issues in an audit report that was found during the audit process. Included are major and critical issues.	*audit report*
Minor issues	Number of minor issues in an audit report that was found during the audit process. Included are minor, informational, and medium issues in this category.	*audit report*
Number of fixed issues per report	Number of issues in an audit report that was fixed during the audit process.	*audit report*
Number of open issues per report	Number of still open issues in an audit report. It is calculated as the residual of total issues found minus the resolved/fixed issues.	*audit report*
Number of days an audit is performed	disclosed number of days of the audit process in an audit report.	*audit report*
Team size	Disclosed number of auditors during an audit process in an audit report, "team" was counted as more than two people	*audit report*
Manual	Type of audit being performed, incl. manually checking the code of the venture	*audit report*
Automatic	Type of audit being performed, incl. for example whitebox testing of the venture's code and protocols	*audit report*
Manual & Automatic	The type of audit being performed includes both manual and automatic methods being used to audit the venture	*audit report*
CAR [0,1]	Cumulative abnormal return (CAR) over the window (0/+1) surrounding the audit report disclosure. cumulative abnormal returns are calculated using the market model as in Ramos et al. (2021), using three different benchmarks, incl. CCMIC, bitcoin and a 21Shares Crypto Basket containing Bitcoin, Ethereum, Polkadot, Solana and Binance Coin.	*coingecko, coinmarketcap.com*
CAR [0,3]	Cumulative abnormal return (CAR) over the window (0/+3) surrounding the audit report disclosure. cumulative abnormal returns are calculated using the market model as in Ramos et al. (2021), using three different benchmarks, incl. CCMIC, bitcoin and a 21Shares Crypto Basket containing Bitcoin, Ethereum, Polkadot, Solana and Binance Coin.	*coingecko, coinmarketcap.com*
CAR [0,5]	Cumulative abnormal return (CAR) over the window (0/+5) surrounding the audit report disclosure. cumulative abnormal returns are calculated using the market model as in Ramos et al. (2021), using three different benchmarks, incl. CCMIC, bitcoin and a 21Shares Crypto Basket containing Bitcoin, Ethereum, Polkadot, Solana and Binance Coin.	*coingecko, coinmarketcap.com*

Appendix B: Coding Example using Certik’s 2020 Smart Contract Audit of 1inch Mooniswap v2

Variable	Definition	Example	Coding Value
Page number	Number of pages of an audit report.	Number of the whole PDF (including all pages available)	49
Manual & Automatic	The type of audit methods being used	Audit summary under method of audit (page 3)	1
Team size	Disclosed number of auditors during an audit process in an audit report, ”team” was counted as more than two people	Audit summary under consultants engaged (page 3)	2
# of days an audit	Disclosed number of days of the audit process in an audit report.	Audit summary under timeline (”December 2nd, 2020 - December 16th, 2020”) (page 3)	15
Items checked	Number of total items in an audit report that was checked during the audit process.	The total number of items checked was not disclosed in full. Hence, at least the items similar to the number of all issues found is assumed to be the list of items checked.	36
Major issues	Number of major issues in an audit report that was found during the audit process. Contains critical and major issues.	Audit summary under vulnerability summary (page 3)	0
Minor issues	Number of minor issues in an audit report that was found during the audit process. Contains all minor, informational, and medium issues.	Audit summary under vulnerability summary (page 3)	36
# of fixed issues per report	Number of issues in an audit report that was fixed during the audit process.	Findings (page 9 and 10)	36
# of open issues per report	Number of still open issues in an audit report.	Items found disclosed as resolved. Items with advice were not counted as open.	0

Figure 1: Example of the Vulnerability Severity Classification by a Technology Service Company that Provides DeFi Audits

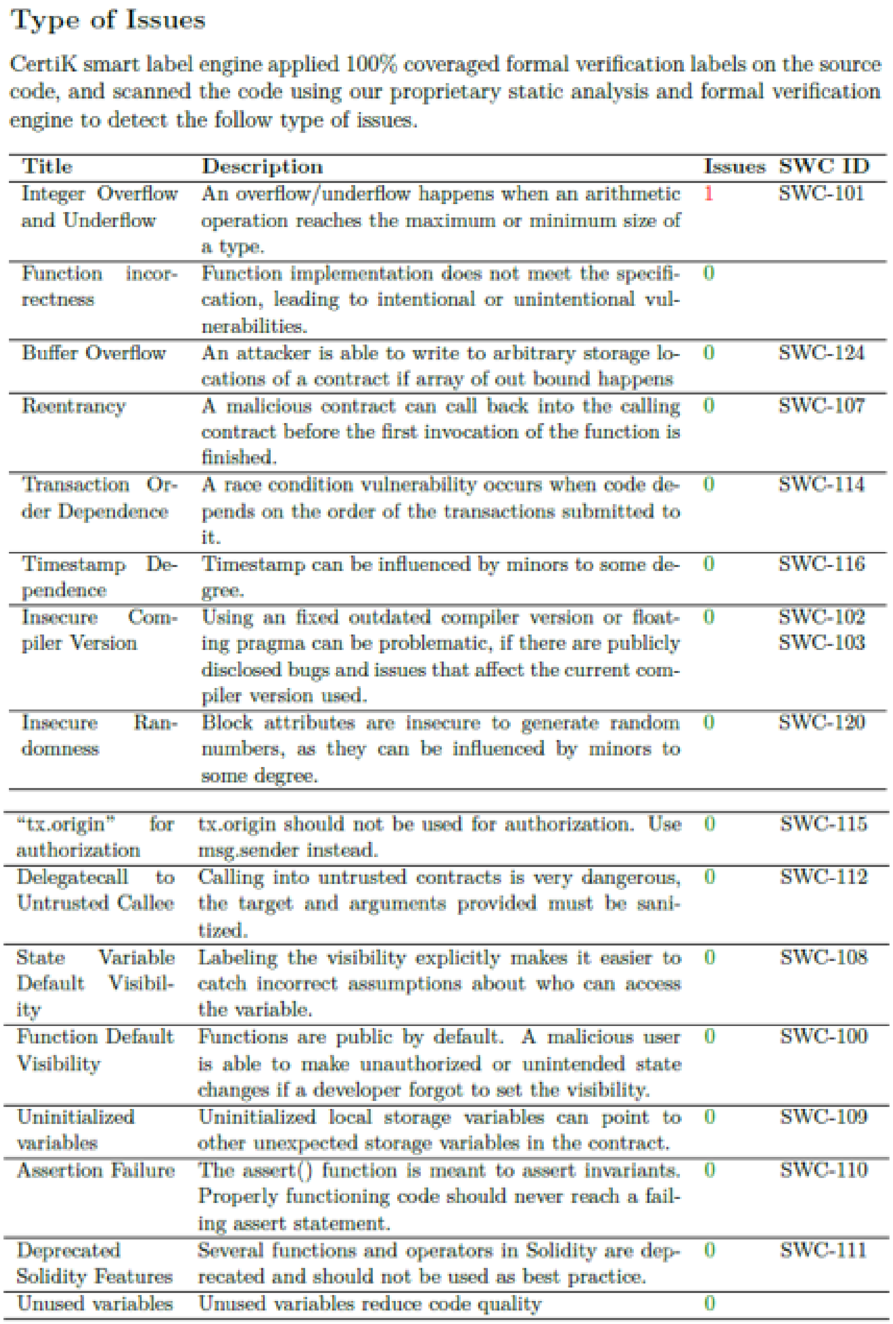
This figure shows the vulnerability severity classification of the issues reported by PeckShield in the report on 88mph as of 11 January 2020. The issues are shown to be critical, high, medium, and low. The likelihood captures how likely a particular vulnerability might be exploited and the impact captures the loss/damage incurred by an attack.



Impact				
	High	Critical	High	Medium
	Medium	High	Medium	Low
	Low	Medium	Low	Low
		High	*Medium*	*Low*
			Likelihood	

Figure 2: Ex-Ante List of Issues

This figure depicts the ex-ante issues as presented in the Certik report on 12Ships as of 22 August 2019.



Type of Issues

CertiK smart label engine applied 100% coveraged formal verification labels on the source code, and scanned the code using our proprietary static analysis and formal verification engine to detect the follow type of issues.

Title	Description	Issues	SWC ID
Integer Overflow and Underflow	An overflow/underflow happens when an arithmetic operation reaches the maximum or minimum size of a type.	1	SWC-101
Function incorrectness	Function implementation does not meet the specification, leading to intentional or unintentional vulnerabilities.	0	
Buffer Overflow	An attacker is able to write to arbitrary storage locations of a contract if array of out bound happens	0	SWC-124
Reentrancy	A malicious contract can call back into the calling contract before the first invocation of the function is finished.	0	SWC-107
Transaction Order Dependence	A race condition vulnerability occurs when code depends on the order of the transactions submitted to it.	0	SWC-114
Timestamp Dependence	Timestamp can be influenced by minors to some degree.	0	SWC-116
Insecure Compiler Version	Using an fixed outdated compiler version or floating pragma can be problematic, if there are publicly disclosed bugs and issues that affect the current compiler version used.	0	SWC-102 SWC-103
Insecure Randomness	Block attributes are insecure to generate random numbers, as they can be influenced by minors to some degree.	0	SWC-120
"tx.origin" for authorization	tx.origin should not be used for authorization. Use msg.sender instead.	0	SWC-115
Delegatecall to Untrusted Callee	Calling into untrusted contracts is very dangerous, the target and arguments provided must be sanitized.	0	SWC-112
State Variable Default Visibility	Labeling the visibility explicitly makes it easier to catch incorrect assumptions about who can access the variable.	0	SWC-108
Function Default Visibility	Functions are public by default. A malicious user is able to make unauthorized or unintended state changes if a developer forgot to set the visibility.	0	SWC-100
Uninitialized variables	Uninitialized local storage variables can point to other unexpected storage variables in the contract.	0	SWC-109
Assertion Failure	The assert() function is meant to assert invariants. Properly functioning code should never reach a failing assert statement.	0	SWC-110
Deprecated Solidity Features	Several functions and operators in Solidity are deprecated and should not be used as best practice.	0	SWC-111
Unused variables	Unused variables reduce code quality	0	

Table 1: Overview of DeFi Auditors

This table represents the DeFi auditors based on the hand-collected 5,343 audit reports from 2017-2022.

DeFi - Auditors - Overview: Whole Sample					
#	Name	#	Name	#	Name
1	0xGuard	32	Dedaub	63	RD Auditors
2	ABDK	33	DeFi Safety	64	Root9B
3	Anchain	34	Dessert Finance	65	Rugfreecoins
4	Ape Audits	35	eNebula	66	Runtime Verification
5	Arachnid	36	Ether Authority	67	Scott Bigelow
6	Arcadia Group	37	FairyProof	68	Secbit
7	Armors Labs	38	Hacken	69	Sentnl
8	Beosin	39	Haechi	70	ShellBoxes
9	Blockchain Consilium	40	Halborn	71	Sigma Prime
10	BlockChainLabs	41	HashEx	72	SlowMist
11	BlockSec	42	Igor Gulamov	73	SmartDec
12	Bramah Systems	43	Immune Bytes	74	Soken
13	Callisto	44	Inspex	75	Solidified
14	Certik	45	InterFi	76	Solidity Finance
15	Certora	46	iosiro	77	Solidproof
16	ChainSecurity	47	Knownsec	78	Somish
17	ChainsGuard	48	Kudelski Security	79	Sooho
18	Chainsulting	49	Least Authority	80	SpyWolf
19	Code 423n4	50	Midgard	81	TakaSecurity
20	CoinBae	51	MixBytes	82	Tech Audit
21	CoinFabrik	52	NCC Group	83	TechRate
22	Coinscope	53	Noneage	84	TechAuditUSA
23	Coinspect	54	Oak Security	85	Theori
24	ConsenSys Diligence	55	Obelisk	86	Trail of Bits
25	Cryptic Labs	56	OpenZeppelin	87	Trustlook Blockchainlabs
26	CryptoManiacs	57	Paladin	88	Víarr the Auditor
27	Cryptonics	58	PeckShield Inc.	89	Zeropool
28	CTDSec	59	Pessimistic	90	ZK Labs
29	Cure53	60	Provide Technologies	91	Zokyo
30	CyberUnit.Tech	61	Quantstamp		
31	Dapp.org	62	QuillAudits		

Table 2: Descriptive Statistics

This table tabulates the top 20 auditors in the DeFi market based on their number of audited reports for the sample of 5,343 reports from 2017 to 2022, with only the top three auditors being responsible for more than 5 percent of the overall audited reports. Approximately 20 percent are represented by others. Panel B illustrates the distribution of audit reports over time for the whole and market samples from 2017 to 2022. 2022 represents only half a year.

Panel A: Top 20 Auditors and their % of Market Share

#	Auditor	# of Audit reports	% Share
1	TechRate	1,563	29.25%
2	Certik	547	10.24%
3	Hacken	369	6.91%
4	Solidproof	214	4.01%
5	Tech Audit	186	3.48%
6	Solidity Finance	178	3.33%
7	Soken	161	3.01%
8	PeckShield Inc.	147	2.75%
10	Solidified	137	2.56%
11	Dessert Finance	114	2.13%
12	Paladin	89	1.67%
13	DeFi Safety	85	1.59%
14	Halborn	77	1.44%
15	Least Authority	74	1.38%
16	Quantstamp	59	1.10%
17	RD Auditors	59	1.10%
18	SlowMist	56	1.05%
19	Trail of Bits	56	1.05%
20	OpenZeppelin	54	1.01%
	Others	975	18.25%
Total		5,343	

Panel B: Audit Reports over Time

	Whole Sample		Market Sample	
Year	# of Reports	% Share	# of Reports	% Share
2022	381	7.1%	-	-
2021	4,054	75.8%	367	76.0%
2020	597	11.2%	101	20.9%
2019	161	3.0%	8	1.7%
2018	113	2.1%	7	1.4%
2017	37	0.7%	-	-
	5,343		483	

Table 3: Venture Characteristics

This table presents the average number of audits per venture and the average number of auditors per venture for the whole sample as well as the sub-sample with market data. Variable definitions can be found in Appendix A.

Venture Characteristics								
Full sample								
	N	Mean	Median	Std dev.	Min.	Q1	Q3	Max.
Average number of audits per venture	5,343	1.24	1.00	0.98	1.00	1.00	1.00	20.00
Average number of auditors per venture	5,343	1.10	1.00	0.53	1.00	1.00	1.00	17.00
Sub-sample with Market Prices								
	N	Mean	Median	Std dev.	Min.	Q1	Q3	Max.
Average number of audits per venture	483	1.78	1.00	1.78	1.00	1.00	2.00	19.00
Average number of auditors per venture	483	1.35	1.00	0.79	1.00	1.00	1.00	5.00

Table 4: DeFi Audit Process

This table tabulates information on the team size, methods used, and days spent on an audit. Variable definitions can be found in Appendix A.

Panel A: Team Size		
Number of Auditors Used	N	
1 auditor	79	1.5%
2 auditors	417	7.8%
3 auditors	281	5.3%
4 auditors	84	1.6%
5 auditors	26	0.5%
More than 5 auditors	24	0.4%
Team (no exact number given)	4,414	82.6%
No information given	18	0.3%
Total	5,343	

Panel B: Methods Used		
Methods	N	
Manual	121	2.3%
Automatic	69	1.3%
Manual & Automatic	2,539	47.5%
No information given	2,614	48.9%
Total	5,343	

Panel C: Days Spent		
Days Spent	# of Audits	
More than 100 days	15	0.3%
More than 60 days	40	0.7%
More than 30 days	105	2.0%
More than 7 days	547	10.2%
More than 1 days	542	10.1%
0 day or 1 day	70	1.3%
No information given	4,024	75.3%
Total	5,343	

Table 5: Audit Report Characteristics

This table presents in Panel A the report characteristics for the whole sample of 5,343 audit reports. Panel B compares the top-quality auditors' with the remaining auditors' report characteristics for the whole sample of 5,343 audit reports using a paired t-test for difference in means at the 95% confidence level. The ten top-quality auditors are Hacken, Quantstamp, Trail of Bits, OpenZeppelin, ConsenSys Diligence, Certik, LeastAuthority, Chainsecurity, Slowmist, and Runtime Verification. Variable definitions can be found in Appendices A and B.

Panel A: Whole Sample								
Characteristics	N	Mean	Median	Std dev.	Min.	Q1	Q3	Max.
Page number	5,343	16.77	13.00	14.58	1.00	9.00	19.00	277.00
Items checked	5,313	19.57	21.00	10.37	0.00	15.00	21.00	184.00
Major issues	4,957	0.55	0.00	1.50	0.00	0.00	0.00	24.00
Minor issues	4,956	4.85	2.00	8.30	0.00	1.00	6.00	161.00
Number of fixed issues per report	4,834	2.43	0.00	5.61	0.00	0.00	2.00	68.00
Number of open issues per report	4,833	3.00	1.00	6.17	0.00	0.00	3.00	161.00

Panel B: Topquality Auditors vs. Non-Topquality Auditors						
Characteristics	N	Mean	N	Mean	*Difference*	*P-value*
Page number	1,303	21.71	4,040	15.18	*6.53*	*0.00*
Items checked	1,293	18.36	4,020	19.96	*-1.60*	*0.01*
Major issues	1,224	0.97	3,733	0.41	*0.55*	*0.00*
Minor issues	1,225	8.55	3,731	3.64	*4.91*	*0.00*
Number of fixed issues per report	1,189	4.77	3,645	1.66	*3.11*	*0.00*
Number of open issues per report	1,189	4.82	3,644	2.40	*2.42*	*0.00*

Table 6: Market Tests

These tables show the baseline results of the t-test analyzing the differences between projects with attacks and no attacks for sub-sample. Only the attacks before the audit are considered. The cumulative abnormal returns use three different market benchmarks, CCMIX, Bitcoin, and Basket. The returns are winsorized at 1% and 99%. The windows start at day zero, which is the release date of the report. Variable definitions can be found in Appendix A.

Panel A: Descriptive Statistics								
	N	Mean	Median	Std dev.	Min.	Q1	Q3	Max.
Benchmark - CCMIX: CAR [0,1]	483	0.116	0.009	0,677	-0.383	-0.053	0.083	5.388
Benchmark - CCMIX: CAR [0,3]	483	0.236	0.012	1.211	-0.679	-0.064	0.123	9.293
Benchmark - CCMIX: CAR [0,5]	483	0.353	0.019	1.927	-1.006	-0.087	0.148	15.971

Panel B: Market Tests - Baseline			
	CAR [0,1]	CAR [0,3]	CAR [0,5]
All ventures: Benchmark - CCMIX	0.116	0.236	0.353
p-value	*0.000*	*0.022*	*0.067*
All ventures: Benchmark - Bitcoin	0.116	0.237	0.356
p-value	*0.000*	*0.020*	*0.056*
All ventures: Benchmark - Basket	0.115	0.231	0.351
p-value	*0.000*	*0.035*	*0.073*

Table 7: Cross-sectional Market Tests

This table tabulates various cross-sectional differences using CCMIX as the benchmark market return. Panel A compares ventures with single audits versus ventures with multiple audits. Panel B compares ventures with major issues versus ventures with no major issues. Panel C compares ventures that experienced attacks before the audit. Attacks include coding exploits, flash loans, honeypots, access controls, and exit scams. Variable definitions can be found in Appendix A.

Panel A: Single vs. Multiple Audits			
	CAR[0,1]	CAR[0,3]	CAR[0,5]
Ventures with single audits	0.178	0.436	0.616
p-value	*0.026*	*0.003*	*0.008*
Ventures with multiple audits	0.093	0.163	0.256
p-value	*0.003*	*0.002*	*0.003*
Difference	0.085	0.273	0.361
p-value	*0.315*	*0.079*	*0.141*
Panel B: Major With Issues vs. Without Major Issues			
	CAR[0,1]	CAR[0,3]	CAR[0,5]
Ventures with no major issues	0.113	0.256	0.382
p-value	*0.013*	*0.002*	*0.003*
Ventures with major issues	0.100	0.144	0.211
p-value	*0.033*	*0.034*	*0.048*
Difference	0.013	0.112	0,172
p-value	*0.844*	*0.297*	*0.304*
Panel C: Attacks			
	CAR[0,1]	CAR[0,3]	CAR[0,5]
Ventures with attacks before audits	-0.006	0.016	-0.004
p-value	*0.755*	*0.652*	*0.904*
All other ventures	0.127	0,256	0.385
p-value	*0.000*	*0.023*	*0.065*
Difference	-0,133	-0.240	-0.389
p-value	*0.001*	*0.001*	*0.000*