Auditing Smart Contracts*

Wayne Landsman† Evgeny Lyandres‡ Edward Maydew§ Daniel Rabetti¶‖

March 2025

Abstract

We study the emerging market for audits of Decentralized Finance (DeFi) smart contracts. We examine two questions. First, what factors influence DeFi protocol developers' decisions to audit their smart contracts and their choice of auditors? Second, is having an audit associated with better outcomes post protocol launch, such as attracting more funds or reducing security breaches, and do these outcomes vary across auditors? We analyze 8,195 audit reports from 117 auditing firms and 1,575 DeFi protocols between January 2020 and October 2023. We find that the decision to audit and the choice of auditor depend on protocol characteristics, such as deployment on a popular blockchain, offering common financial services, and risk level. Protocol performance increases with auditor market share and launch rate, and decreases with auditor hack rate. Protocols audited by decentralized auditors, or "bounty hunters," are also associated with better outcomes. Additionally, audited protocols experience a milder negative response to adverse DeFi market shocks. However, we find little evidence that audits reduce future security breaches. Instead, protocols are more likely to switch auditors following a breach. Overall, our study provides evidence on the use and value of voluntary smart contract audits in the emerging decentralized finance market.

JEL classification: G15, G18, G29, K29, K42, O16.
Keywords: Auditing, DeFi, decentralized finance, smart contracts, security breaches, blockchain.

*We are thankful to the following people for providing comments on earlier drafts of our paper: Amanda Awyong, Haichen Bai, Daniel Bens, Masaki Bessho, Thomas Bourveau, Mark Bradshaw, Murillo Campello, Qiang Cheng, Jonathan Chiu, Will Cong, Xu Da, Stephanie Dong, Vivian Fang, Cam Harvey, Allen Huang, Serene Huang, Shiyang Huang, Mingyi Hung, Peiyi Jin, Bjorn Jorgensen, Peter Joos, Elsa Juliani, Bin Ke, Stella Kong, Alfred Lehar, Dan Li, , Erica Li, Mei Luo, Yuanzhen Lyu, Roni Michaely, Chris Ngoi, Christine Parlour, Yuanyu Qu, Thomas Rivera, Fahad Saleh, Fabian Schar, Joe Schroeder, Rob Smith, Jona Stinner, Tammaro Terracciano, Alexander Wehrli, Michael Wutzke, Xiao Xiao, Yu Yan, Cheng Yin, Bernard Yeung, Shuangchen Yu, Xiaojun Zhang, and Yihong Zhou. We also benefited from helpful discussions at the International Monetary Fund (IMF), ETH Denver Festival, Harvard Business School, Tokenomics Conference, Tsinghua University, Peking University, University of International Business and Economics, Cornell-PBC Summer Institute of Finance, IC3 Blockchain Camp at Cornell Tech, Swiss National Bank and University of Basel via SNB-CIF Conference on Cryptoassets and Financial Innovation, Euroasia Conference, Bank for International Settlements, Bank of Japan, Fintech Center, Payment and Settlement Systems Department, FeAT International Conference on Artificial Intelligence, Singapore Fintech Festival, Financial Markets and Corporate Governance Conference, ICMA Centre at Henley Business School, University of Reading, Capital Market Research in the Era of AI Conference at HKUST, Vietnam Symposium in Banking and Finance, and CBER Symposium in Auditing DeFi Applications. Rabetti thanks the Digital Economy and Financial Technology (DEFT) Lab at Cornell Fintech Initiative, the Research Center for Digital Financial Assets at Tsinghua University, and the Asian Institute of Digital Finance (AIDF) at the National University of Singapore for extended discussions. Lyandres thanks the Kassirer Institute at Tel Aviv University and Fintech Chair at Paris Dauphine University for financial support. Landsman and Maydew thank the Kenan-Flagler Business School for financial support. Ding Chou, Gia Anna George, Vaishnavi Gunasekaran, Xing Hexin, Yiqing Huang, Li Shengzhi, Zhenhui Xi, Huiting Zhou, Xuanhao Zeng, Yilin Zhou, and Li Ziting provided excellent research assistance. A February 2023 version of this paper circulated under the title *"Auditing Decentralized Finance (DeFi) Protocols"*. All errors are our own.

†University of North Carolina, wayne_landsman@unc.edu.
‡Tel Aviv University and Monash University, lyandres@tauex.tau.ac.il.
§University of North Carolina, edward_maydew@unc.edu.
¶Corresponding Author: National University of Singapore (NUS) Business School, 15 Kent Ridge Drive, Singapore, 119245.
‖Harvard Business School (visiting), drabetti@hbs.edu.

"On-chain assets are fundamentally financial instruments, and the ecosystem is well past due for the establishment of crypto-specific audit and attestation standards." —David Sacks, March 7, 2025.[1]

1 Introduction

Mitigating cybersecurity risks in the age of digital assets is of paramount importance. The rapid growth of cryptocurrency markets and the increasing number of digital asset users have created a highly attractive environment for cybercriminals. With the market capitalization of cryptocurrencies surpassing $2.86 trillion in March 2025, digital assets have become a lucrative target for cyberattacks (Cong, Harvey, Rabetti, and Wu (2024)). The stakes are especially high as cryptocurrencies and blockchain technologies continue to evolve and disrupt traditional financial systems, particularly with several billions of dollars in assets tied to decentralized applications. Hacking incidents, such as the $1.5 billion security exploit on the Bybit cryptocurrency exchange in February 2025, showcase the magnitude of potential financial losses. An increasing incidence of high-profile breaches reveals that individual and institutional participants in the crypto markets are exposed to significant risks, highlighting the need for solutions to secure crypto users' assets while responsibly fostering market growth.

This study assesses the emerging market for voluntary audits of Decentralized Finance (DeFi) smart contract protocols. Smart contracts, utilizing blockchain technology, are self-executing, in the sense that the terms of the agreement between parties are directly written into code. Smart contracts are used by DeFi protocols (hereafter protocols), which enable users to engage in peer-to-peer financial transactions without reliance on centralized financial intermediaries.[2] Smart contracts are used for various financial activities, including exchange of assets, lending/borrowing, investment, derivatives, and insurance (Harvey, Ramachandran, and Santoro (2021) and Makarov and Schoar (2022)).

The DeFi market started to gain popularity in the summer of 2020. By December 2024, the amount of liquidity in thousands of protocols surpassed $200 billion, servicing roughly $30 billion worth of daily transactions.[3] As the market for smart contracts in DeFi has grown, so has the need for protocols to assure users that smart contracts would be executed as intended, particularly without exposure to bugs and security breaches, which could result in loss of funds. To provide such assurance, before opening a new protocol to the public, which is commonly referred to as a "launching", protocol developers have increasingly relied on hired auditors to find errors in smart contract code and potential sources of security breaches. As with traditional financial statement audit reports (e.g., in the

[1] Attributed to David Sacks, the "Crypto Czar," at the White House Crypto Summit regarding the importance of crypto audits. See https://tinyurl.com/ye2yvxjm.

[2] For ease of exposition, in what follows, a DeFi protocol refers to a single online platform running smart contracts to provide decentralized financial services. Each DeFi protocol encompasses as few as one and as many as thousands of smart contracts.

[3] See www.defillama.com.

context of Initial Public Offerings), smart contract audit releases may increase investors' and users' trust.

We ask two fundamental questions about the market for smart contract audits. First, what factors do protocol developers consider when deciding whether to have their smart contracts audited and what types of auditors to engage? Second, is having an audit associated with better real outcomes post protocol launch, such as the ability to attract funds or a lower likelihood of future security breaches, and do these outcomes vary across auditors of varying real or perceived quality?

Smart contracts have both advantages and disadvantages relative to traditional financial contracts. Because smart contracts do not rely on centralized intermediaries, organizational overhead is lower, reducing transaction costs (e.g., Harvey and Rabetti (2024)). Smart contracts deployed on public blockchains are open-source, leading to intense competition and fast development of smart-contract-based financial applications. Competition among protocols is intense because of low entry costs, which result from the open-source nature of smart contracts. DeFi is characterized by an unprecedented degree of interoperability and interconnectedness, at least within a given blockchain, allowing sophisticated financial engineering and efficient utilization of liquidity.[4]

One of the largest drawbacks of smart-contract-based DeFi protocols is risks unique to them, referred to as "smart contract risks" hereafter. Because smart contracts can be deployed permissionlessly on a public blockchain, i.e., without control or oversight, sometimes by inexperienced professionals, adventurous enthusiasts, and ambitious amateurs, they may contain logical errors and/or bugs, exposing their users to potential losses of funds as well as funds appropriation by bad actors.[5] As of the end of 2023, $7.6 billion in user funds reportedly have been lost to smart contract exploits and hacks.[6]

As an illustration of smart contract risk, consider an exploit of Euler Finance, one of the largest lending protocols in DeFi, that allows users to earn interest on deposits and borrow assets by using their crypto holdings as collateral, all governed by smart contracts. The protocol's unique feature is its customizable lending markets, enabling users to create custom collateral types and risk parameters. In March 2023, Euler Finance suffered a $200 million loss when an attacker exploited vulnerabilities in the protocol's smart contract, specifically in the liquidation and borrowing mechanisms. By using a flash loan, the attacker manipulated collateral ratios, triggering faulty liquidations and draining the protocol's funds. This incident highlights significant risks in DeFi protocols, particularly around smart contract vulnerabilities and the use of flash loans for exploiting weaknesses.[7]

[4] In the context of DeFi, interoperability refers to the ability of distinct smart contracts to communicate and interact with one another seamlessly. Interconnectedness—the degree to which various protocols are linked or integrated, allowing for transactions spanning several protocols—is an outcome of interoperability.

[5] See Harvey and Rabetti (2024) for a discussion of the advantages and risks of DeFi adoption.

[6] See https://defillama.com/hacks.

[7] See https://www.coindesk.com/business/2023/03/13/euler-defi-protocol-exploited-for-nearly-185m for a discussion of Euler Finance exploit.

Given the rapid pace of change in smart contract technology and the high degree of exposure of smart contracts to external threats, it is generally impossible to ensure that smart contracts are error-free. In the extreme, smart contract risks could severely restrict the usefulness of transacting in DeFi. Fortunately, the market has developed a mechanism for mitigating smart contract risk: smart contract audits, which involve reviewing smart contract code with a goal of identifying and rectifying bugs and vulnerabilities.

As with traditional audits, i.e., audits of financial statements, smart contract audits involve third-party certification. However, notable differences exist between auditing smart contracts and traditional auditing. First, while traditional auditing focuses on evaluating the integrity of financial statements, smart contract auditing focuses on evaluating the integrity of smart contract code. Second, unlike traditional auditing, smart contract auditing is not presently subject to formalized auditing standards. Third, while traditional auditing is regulated and mandated by legislation, the decision to have a smart contract audited is voluntary. Fourth, smart contract auditing does not require auditors to have formal education and certification. Instead, auditing firms employ individuals with cryptography or computer science expertise and experience in coding and verification of blockchain applications.

The market for smart contract audits has grown substantially in recent years, from just a few auditing firms in 2020 to over a hundred by March 2025. In some respects, the development of DeFi parallels the development of banking in the early days when regulation was limited (e.g., Frishkoff (1989) and Bourveau, Breuer, Koenraadt, and Stoumbos (2023)). In both cases, a new form of financial intermediation emerged and required mechanisms for market participants to trust the system. Early developed mechanisms included voluntary provision of financial statements, voluntary audits, and state-level regulatory supervision. Although these mechanisms provided some stability to the system, a series of bank runs and financial panics ultimately led to federal bank regulation, beginning with the Federal Reserve Act of 1913. Whether DeFi follows a similar path has yet to be determined. The setting of voluntary smart contract audits that our study examines is analogous to the low-regulation, voluntary audits of traditional financial institutions at the start of the 20th century.

We analyze 8,195 audit reports, from 117 auditing firms, and 1,575 DeFi protocols between January 2020 and October 2023. We collect audit reports and auditor information directly from the auditing firms' websites, website aggregators (such as `De.Fi`), and GitHub repositories. We also obtain protocol-level financial and security breach information from DefiLlama, pricing data from CoinGecko, and user data from Ethplorer.

We start by addressing our first research question—what factors protocols consider when deciding whether to have their smart contracts audited—by estimating logistic regressions in which the dependent variable is an indicator of whether a protocol has undergone at least one audit before its launch. The independent variables are a set of market and protocol characteristics measured at least one month before the protocol's smart contracts are audited.

Our findings identify three factors—one supply-side and two demand-side— associated with the decision to

perform a smart contract audit. First, on the supply side, smart contracts are more likely to undergo an audit when they are deployed on a popular blockchain, such as Ethereum—the first and largest blockchain enabling smart contracts—or offer common financial services such as asset exchanges or lending/borrowing. Protocols deployed on popular blockchains and those that offer common financial services have a larger supply of potential auditors to hire. Second, on the demand side, projects that have raised external funds before launch are more likely to have their smart contracts audited. Third, also on the demand side, smart contracts that provide more complex financial services and rely on sources of information external to the blockchain and/or protocol ("oracles") are more likely to undergo an audit because they impose larger risks on their users.

Among audited smart contracts, we also examine whether the decision to engage a high-quality auditor is associated with the same set of market and protocol characteristics. We adopt common measures of auditor quality (e.g., DeFond and Zhang (2014) and Knechel and Willenborg (2016)), to the smart contract setting.[8] We measure auditor quality using three non-mutually exclusive proxies: *Auditor Market Share*—the fraction of all audit reports performed by a given auditor out of all audit reports during the last six months; *Auditor Launch Rate*—the ratio of protocols audited by a given auditor during the last six months that launched successfully relative to all audits performed by the auditor in the same period; and, *Low Auditor Hack Rate*—one minus the fraction of protocols audited by a given auditor that were hacked within six months of the launch date. We find that across all three measures of auditor quality, protocols that are deployed on more popular blockchains and those that offer common financial services, as well as protocols that expose users to risk from using off-chain information via oracles are likely to hire higher-quality auditors.

In addition to hiring an auditing firm, projects can also engage with so-called "bounty hunters." Auditing firms in DeFi markets are centralized and are similar to auditors in traditional financial markets in that they are paid a fixed fee for their auditing services. In contrast, bounty hunters can be thought of as *Decentralized Auditors*: they are freelancers who provide specialized code reviews, the payment for which depends on the number of vulnerabilities found in smart contract code and their severity.[9] We find that protocols that operate on more popular blockchains and protocols that offer more common financial services, as well as riskier protocols are more likely to hire decentralized auditors. Collectively, this first set of findings highlights characteristics of protocols and smart contracts that are associated not just with the decision to have smart contracts audited but also with the choice of high-quality and/or decentralized auditors.

We next address our second research question: whether having an audit is associated with real outcomes post-protocol launch. We do this by examining whether three important post-launch outcome variables, are associated

[8] Throughout we use the terms auditor quality and auditor reputation interchangeably.

[9] See an example of a marketplace for bounty hunters here: https://immunefi.com/.

with whether an audit was conducted before smart contract deployment. Our primary outcome variable, *Total Value Locked* (*TVL*), represents the total dollar value of all assets deposited in a protocol (e.g., Cong, Prasad, and Rabetti (2023), Parlour (2023), and DeSimone, Jin, and Rabetti (2025)). *TVL* is roughly analogous to deposits as a measure of economic activity in the context of traditional financial institutions. We find that having a smart contract audit tends to be associated with a larger TVL, especially for longer post-launch windows. For example, within three months of protocol launch, audited protocols achieve 7% higher TVL than non-audited protocols, which is equivalent to an additional $1M TVL.

Our second outcome variable, *Market Capitalization*, is the market value of a protocol's governance tokens (e.g., Lyandres, Palazzo, and Rabetti (2022) and Amiram, Lyandres, and Rabetti (2024)). Governance tokens' market cap is the DeFi equivalent of the market value of equity in the traditional setting. The third outcome variable is the number of on-chain holders of governance tokens, *Holders*, measuring the number of investors in and users of a protocol. We find that protocols with audited smart contracts command 4% higher market valuations on average and have 17% more token holders than their non-audited peers. Because the sample size for the last two measures is significantly smaller than the sample size for *TVL*, we use *TVL* as the main outcome variable in most of the analysis.

To examine the causal nature of the relation between smart contract audits and post-protocol-launch outcomes, we follow Cong et al. (2023) and exploit two quasi-natural experiments that caused a substantial reduction in market trust, which was likely to lead to increased demand for smart contracts auditing. The first event is the Terra-Luna crash in May 2022, which resulted in roughly 40 billion dollars of direct losses to investors.[10] The second event is the collapse and bankruptcy in November 2022 of FTX, one of the largest crypto exchanges globally, leading to losses of a similar magnitude. This collapse was triggered by a liquidity crisis, allegations of misuse of customer funds, and risky financial practices. The fallout affected the broader crypto market, leading to a significant loss of trust among investors, plummeting cryptocurrency prices, and causing a ripple effect that affected many other crypto firms and projects. We hypothesize that in the aftermath of such shocks to market trust, protocols with audited smart contracts are more resilient in retaining *TVL*. We test this hypothesis by employing a difference-in-differences (DiD) design around these two events, where we expect a differential effect of the shocks on audited smart contracts and on matched unaudited ones. Consistent with these events inducing a substantial reduction in trust by market participants, unaudited smart contracts lost 22-23% and 9-11% of their *TVL* on average following Terra-Luna and FTX shocks, respectively. The loss in TVL was approximately 36% to 55% smaller for audited smart contracts than for unaudited ones.

[10] The Terra-Luna crash, which was part of the broader Terra ecosystem collapse in May 2022, resulted from the de-pegging of its associated stablecoin, TerraUSD (UST), from the US dollar. UST was supposed to maintain its value through a complex algorithmic mechanism linked to the blockchain's native currency, Luna, but massive sell-offs led to UST losing its peg. As the system tried to stabilize UST by creating more Luna, the supply of Luna surged, causing its price to plummet.

We next examine, within a subsample of audited smart contracts, whether variation in post-launch *TVL* is associated with the three measures of perceived auditor quality, *Auditor Market Share*, *Auditor Launch Rate*, and *Low Auditor Hack Rate*, and with the use of *Decentralized Auditors*. Consistent with auditors providing some measure of assurance, we find that audits by low-hack-rate auditor, high-launch-rate auditor, as well as decentralized ones are associated with greater post-launch *TVL*. Collectively, these findings suggest that smart contract audits increase trust in audited protocols if performed by auditors with a prior history of success, as reflected by low past hack rates and high past launch rates, or by properly incentivized auditors.

Our interpretation that smart contract audits convey a sense of trust to market participants raises the question of whether such trust is warranted. Over the past few years, there have been at least 186 security breaches involving smart contracts, leading to cumulative losses exceeding 7.6 billion dollars.[11] We examine two related questions. First, is there an association between having smart contracts audited and the likelihood of future security breaches? Second, conditional on smart contracts having been audited, is the likelihood of future security breaches lower for protocols audited by auditors of higher perceived quality or better aligned incentives? Surprisingly, we find a positive relation between protocol audits and the likelihood of that protocol's future security breaches. This result may reflect that protocols tend to hire auditors if they believe their smart contracts are more likely to be subject to future hacks. On the other hand, consistent with protocols updating their beliefs of their auditors' quality, future security breaches are significantly lower for smart contracts audited by auditors with a prior lower hack rate.

Auditing activities do not stop at protocol launch. Protocols, especially successful ones, are under users' scrutiny and tend to undergo post-launch audits from time to time, especially during times of smart contracts updates and new version launched. Continued audits ensure that protocols align with industry standards, comply with legal or regulatory requirements, and improve protocol resilience. Protocols continue to have a wide choice of auditors post-launch. The last question we address is whether protocols are likely to replace their smart contract auditors following security breaches. We expect that a security breach is likely to lead to a downward revision in a protocol's assessment of the quality of its incumbent auditor(s) and to increase the likelihood that the protocol would change auditors. Consistent with this reasoning, we find evidence that protocols are more likely to switch auditors following security breaches. Auditors that are especially likely to be replaced following a hack are those with high market shares and high post-launch rates, likely because these characteristics are less relevant for post-launch auditor choice. Auditors with proven record of low past hack rates are not more likely to be replaced following a hack.

[11] See Appendix D for more details on the time-series evolution of smart contract security breaches. Security breaches have become pervasive because of the increasing sophistication of cybercriminals despite advances in blockchain forensics (e.g., Amiram, Jørgensen, and Rabetti (2022), Cong et al. (2024) and Cong, Grauer, Rabetti, and Updegrave (2023)).

Our study is among the first to examine the role auditing plays in the burgeoning decentralized finance markets.[12] We connect the DeFi literature with the accounting and auditing literature.[13] To date, the DeFi market has been characterized by low regulation and high risk relative to traditional financial markets. Our findings from provide insights that may inform current debate regarding the need for DeFi regulation. In particular, understanding how DeFi protocols address security risks, including their decisions of whether to hire auditors, and the effects of such decisions on real outcomes, may provide insights to policy makers regarding whether and how to adapt the auditing regulatory apparatus to the DeFi market.[14]

Our paper adds to the literature examining the effectiveness of voluntary auditing (e.g., Allee and Yohn 2009; Minnis 2011; Lennox and Pittman 2011; Minnis and Shroff 2017; Lisowsky and Minnis 2020; Schoenfeld 2024; Lennox, Schmidt, and Thompson 2023). This literature finds that voluntary auditing is generally associated with positive outcomes, such as improved credit ratings, lower cost of capital, and easier access to credit markets. Our result that voluntary smart contract audits are generally associated with positive economic outcomes is consistent with this evidence. However, audits do not tend to lead to lower future hack rates, except for audits performed by auditors with a prior history of lower hack rates. Overall, our results suggests that auditing may be effective at attracting and retaining users and investors, but it may not be as effective at mitigating bugs and vulnerabilities of audited smart contracts.

Our study builds upon the literature in archival auditing, which studies determinants of auditing quality (e.g., Simunic 1980; Watts and Zimmerman 1983; DeFond and Subramanyam 1998; Deng, Lu, Simunic, and Ye 2014; Lennox and Pittman 2010; Reichelt and Wang 2010; Kaplan and Williams 2013; DeFond, Erkens, and Zhang 2017; Lobo, Paugam, Zhang, and Casta 2017; Duguay, Minnis, and Sutherland 2020; Fedyk, Hodson, Khimich, and Fedyk 2022).[15] This literature typically finds that large auditors (e.g., "Big 4" auditors) perform higher-quality audits, as reflected by fewer restatements, less fraud, and less earnings management.[16] In contrast to this extant literature, we find that in the smart contract auditing setting, an auditor's market share is not necessarily related to post-audit outcomes.

The remainder of the paper is organized as follows. Section 2 contains background information on smart contracts, focusing on the smart contract audit market. Section 3 discusses our data sources, sample, and summary

[12] Other contemporaneous studies include Bourveau et al. (2023), Du and Wang (2023), and Bhambhwani and Huang (2024).

[13] See DeFond and Zhang (2014) and Knechel and Willenborg (2016) for a review of the auditing literature. See Harvey et al. (2021), Makarov and Schoar (2022), John, Kogan, and Saleh (2023), and Harvey and Rabetti (2024) for a review of the DeFi literature.

[14] See https://www.davispolk.com/insights/client-update/crypto-market-structure-bill-draws-closer-floor-vote-house for an example of pending proposed legislation to develop a regulatory framework for digital assets. Changes in the regulation of digital assets can lead to potential changes in the regulation of the DeFi market.

[15] See Lee, Pinto, Rabetti, and Sadka, 2024 and Luo, Rabetti, and Yu, 2024 for blockchain adoption benefits in the corporate setting.

[16] See, e.g., Magee and Tseng 1990; Antle and Nalebuff 1991; Dye 1991; Mutchler and McKeown 1997; Blacconiere and DeFond 1997; Francis, Maydew, and Sparks 1999; Clarkson and Simunic 1994; Gul, Fung, and Jaggi 2009; Kausar, Shroff, and White 2016; Ashraf, Michas, and Russomanno 2020.

statistics. Section 4 examines factors associated with the decision by a protocol to have its smart contracts audited. Section 5 examines the relation between smart contract audits and real outcomes post-protocol-launch. In Section 6, we analyze whether audits are associated with a lower likelihood of future hacks and exploits. The last section concludes.

2 Smart Contracts and Smart Contract Audits

2.1 Smart contracts

Smart contracts are self-executing agreements whose terms are directly written into code. They automatically perform predefined actions when specific conditions are met. One of the key advantages of smart contracts lies in their ability to automate and streamline a wide range of transactions and agreements, potentially revolutionizing traditional contract mechanisms across various industries.

Smart contracts operate on top of blockchains, which maintain an immutable and transparent ledger of transactions via a network of nodes ("validators"). Once a smart contract is deployed on a public blockchain, its code and execution typically cannot be modified, ensuring the integrity of the agreed-upon terms. All transactions and interactions with smart contracts are recorded on the blockchain, allowing for transparent verification of (financial) activities. Smart contracts are at the core of DeFi protocols, in that they enable automated transactions that do not rely on compliance by the counterparties, i.e. "trustless" transactions (e.g., Harvey and Rabetti (2024)). Beyond the financial sector, smart contracts have applications in supply chain management, insurance, and escrow services, and may offer higher levels of transparency, security, and efficiency.

Despite the potential of smart contracts to change the landscape of financial arrangements, there are legitimate concerns about potential security breaches and vulnerabilities within the smart contract code. Because of the irreversible and automated nature of smart contract execution, any flaws in smart contract code can have severe consequences, leading to financial losses or exploitation by malicious actors.[17] These security concerns have led to the development of the smart contract audit market to assure DeFi users that smart contracts would execute their intended functionality and that users' funds would be secure.

2.2 Smart Contract Audits

Smart contract auditors provide independent assurance of the completeness and correctness of smart contract code. The auditing process of smart contracts begins with a comprehensive code review. This step involves exam-

[17] A famous example of a security breach involving smart contracts occurred in 2016 with "The DAO" (Decentralized Autonomous Organization), a crowdfunding project on the Ethereum blockchain. A hacker exploited a contract code vulnerability, draining part of the DAO's funds. See Sheen (2021) for a detailed description of the DAO hack.

ining smart contract code to identify vulnerabilities, potential exploits, and bugs. Auditors also check whether the smart contract code adheres to best coding practices and principles and correctly implements the intended functionality, i.e., it does what it is supposed to do.

After smart contract auditors complete their code review, they typically proceed to "static analysis." This involves examining the code without actually executing it—a process, which can help identify common coding errors and potential vulnerabilities that may have been missed during the code review. Static analysis tools are designed to scrutinize the code, parsing each line and structure. Smart contract auditors often follow up with a "dynamic analysis," which involves running the code in a controlled environment to observe its behavior. Dynamic analysis helps auditors identify vulnerabilities that might not be detectable through static analysis alone, such as runtime errors or issues with memory management.

Economic analysis forms another crucial part of smart contract auditing, in which an auditor considers economic incentives and mechanisms of users' interactions with smart contracts. For instance, auditors may analyze how a lending protocol sets interest rates, and how lenders within the protocol contribute to the protocol's stability. Auditors may scrutinize collateralization mechanisms embedded in smart contracts to assess their effectiveness in mitigating default risks. Overall, economic analysis helps to ensure that smart contract logic does not create opportunities for manipulation or abuse, thereby safeguarding the interests of protocol users.

After protocol developers address the issues identified during the smart contract audit, an auditor conducts re-testing. This step may be repeated several times before the final audit report is released. Overall, the auditing process tends to be time-consuming, often spanning weeks and sometimes months.

Smart contract audits share some similarities with traditional audits. For example, audit fees in both are generally independent of the outcome of the audit report. However, notable differences exist between the two types of audit. First, although traditional auditing focuses on ensuring compliance with accounting standards, smart contract audits concentrate on evaluating the integrity of the smart contract codes. Second, in contrast to traditional financial statement audits, which rely on Generally Accepted Auditing Principles (GAAP), smart contract auditors are not required to follow a standardized framework. Third, unlike traditional audits, which are regulated and mandated by legislation, smart contract audits and their disclosure are voluntary.[18] Finally, smart contract auditing does not require auditors to possess formal education and certification.

In addition to hiring centralized smart contract auditors, protocols can hire decentralized auditors, commonly referred to as bounty hunters. Bounty hunters are recognized experts, who offer freelance code reviews via platforms that connect them to protocols offering bounties for finding smart contract errors and vulnerabilities. In contrast

[18] Although the vast majority of audits are disclosed to the public, either by the audited protocol or by the auditing firm, we cannot rule out that some audits, especially for smaller protocols, are kept private (e.g., Feng, Hitsch, Qin, Gervais, Wattenhofer, Yao, and Wang (2023). See Yuyama, Katayama, and Brigner (2023) for a proposal for principles of DeFi disclosure.

to the compensation to centralized auditors, decentralized auditors' compensation depends on the severity of smart contract vulnerabilities that they discover.

2.3 Examples of Smart Contract Auditors

To provide some context on the state of the smart contract audit industry, this subsection describes three smart contract auditors—Certik, Hacken, and Peckshield—that audited approximately 17 percent of all smart contracts during our sample period. See Appendix E for the list of smart contract auditors and the number of audited reports by each.

Certik. Headquartered in New York, Certik was founded by professors from Columbia and Yale and funded by several leading venture capital funds (see `https://www.certik.com/`). Certik is known for using several auditing processes, including automated auditing and formal verification methods. It claims to be the first auditor of smart contracts that has received SOC II certification—a security standard that offers guidelines to service organizations for protection of sensitive data from unauthorized access, security incidents, and other vulnerabilities.

Hacken. Headquartered in Estonia, Hacken is an international cybersecurity company with Ukrainian roots (see `https://hacken.io/audits/`). Hacken has over 1,000 global clients, including large ans successful blockchains. crypto exchanges, and DeFi protocols such as Binance, Avalanche, Kyber Network, Huobi, Kucoin, Sandbox, and DAO Marker. Besides auditing smart contracts, Haken provides other services, including tokenomics, penetration tests that simulate cyberattacks to identify vulnerabilities, and a real-time smart contract protection tool. Appendix A1 provides an example of an audit report conducted by Hacken.

PeckShield. Located in Hangzhou, China, PeckShield was formed by seasoned security professionals and senior researchers from companies such as Microsoft, Intel, Juniper, and Alibaba (see `https://peckshield.com/`). Founded in 2018, PeckShield also offers blockchain forensics services (e.g., transaction mapping and real-time blockchain monitoring). PeckShield has audited several large market players in the DeFi space, including BNB Chain, Polygon, EOS, Maker, Aave, Dydx, Bancor, and 1inch.

3 Data and Summary Statistics

3.1 Data

We collect audit reports from auditing firms' websites, data aggregators, and GitHub repositories. After removing audit reports we identified as duplicates, incomplete, or issued by non-auditing firms, we have a final sample of 8,195 unique audit reports issued by 117 auditing firms from January 2020 to October 2023. We then match each audit report with financial and security breach information from DefiLlama (`https://defillama.com`), pricing

data from CoinGecko (www.coingecko.com), and wallet data from Ethplorer (https://ethplorer.io).

Figure 1 depicts the monthly combined total value locked (*TVL*, dashed red line) and the monthly number of smart contract audits (solid blue line). The figure suggests a high correlation between the overall value of funds deposited in DeFi protocols and the number of smart contract audits.

[Figure 1 here]

3.2 Summary Statistics

Table 1 presents summary statistics of smart contract protocols, post-protocol launch outcomes, and auditors, each of which is discussed in the following subsections.

[Table 1 here]

3.2.1 Protocol Characteristics

This section provides descriptive statistics of smart control protocol characteristics that are hypothesized to be potentially related to dependent variables in our analysis.

Ethereum, is an indicator variable that equals one if smart contracts are deployed on the Ethereum blockchain (potentially among others). Ethereum is the first smart-contract-enabling blockchain, launched in 2015, and, is the second-largest blockchain (behind Bitcoin) by market capitalization of native blockchain currency, ETH. 37% of protocols are deployed on Ethereum. Nearly three-quarters (74%) of protocols are deployed on at least one Ethereum-Virtual-Machine (EVM)-compatible blockchain, *EVM*. Smart contracts written in Solidity, which is the main programming language on Ethereum, can be deployed on any EVM-compatible blockchain with minor adjustments. Deployment on Ethereum and EVM compatibility are considered a risk-reducing factor for several reasons. First, Ethereum is the first, oldest, and most widely adopted blockchain for smart contracts. Consequently, developers on EVM-compatible chains have access to several tools that support smart contract coding, making EVM-compatible chains less susceptible to bugs and exploits. Second, smart contracts in the Ethereum ecosystem are scrutinized by the largest coding community in the blockchain space. Finally, auditing firms encounter fewer challenges in finding experts proficient in Solidity compared to non-EVM-compatible chains, protocols on which are often written in other, less widespread coding languages.

Approximately two-thirds of protocols belong to at least one of the following three categories. 28% are decentralized exchanges *DEX*, which are protocols that enable swapping of crypto assets. 20% are yield farming protocols,

Yield, which are protocols that provide depositors with rewards on crypto asset deposits that can be used for lending and liquidity provision. 19% are lending protocols, *Lending*, which facilitate collateralized and uncollateralized (instantaneous, "flash") lending and borrowing of crypto assets.

A quarter of protocols employ oracles, *Oracle*. Because a blockchain cannot access external (often referred to as off-chain) data, oracles are used to provide external data necessary to execute smart contracts (e.g., Cong et al. (2023)).[19] If an oracle is compromised or manipulated, it can deliver biased data, causing smart contracts to execute incorrectly. Thus, the use of oracles can be a significant source of smart contract risk (e.g., Harvey and Rabetti (2024)). Smart contracts are deployed on public blockchains and are, therefore, by definition open-source. However, protocols can also make their off-chain code (e.g., various off-chain optimizations) open-source, *Open Source*, thereby raising their degree of transparency (e.g., Gefen, Rabetti, Sun, and Zhang (2024)), but also potentially exposing them to hacking or manipulation by bad actors. 9% of protocols are open-source.

Projects developing DeFi protocols can raise funds from external investors before launch, *Raised* is an indicator variable that equals one if a protocol raised external funds prior to launch. 35% of all protocols in our sample raised funds from external investors before protocol launch. Conditional on raising funds, the median (mean) amount raised is $3.5M ($9.63M).

The median number of blockchains on which smart contract protocols are deployed, *#Chains*, is one, the mean is 1.58, and the maximum is 25. The median (mean) number of audits per smart contract protocol before launch, *#Audits*, is 2 (1.16), although 43% of launched protocols are never audited. 7% of all launched protocols experienced a security breach, *Hack*, within six months of launch.

3.2.2 Outcomes at Launch

Our main outcome variable of interest is the total value locked, *TVL*—the total value of funds (in $) deposited into a protocol, which is widely used as a proxy for economic activity in the DeFi market (e.g., Cong et al. (2023), Campello, Jin, Rabetti, and Saleh (2024), and DeSimone et al. (2025)). When users deposit assets into a protocol, they become temporarily "locked" in it. *TVL* is roughly equivalent to the total value of deposits into a traditional financial institution.

We also employ alternative measures of post-launch protocol outcomes. One measure is the market capitalization of the protocol's governance tokens, used to raise funds, incentivize liquidity provision, and vote on protocol decisions, *Market capitalization*. *Market capitalization* is the product of protocol governance token price and the number of tokens outstanding (e.g., Lyandres et al. (2022), Bourveau, Brendel, and Schoenfeld (2024), and Bhambhwani and Huang (2024)). Another post-launch outcome is the number of holders of the protocol's governance

[19] Such data can include exchange rates, interest rates, weather data or even outcomes of particular events.

tokens, *Holders*, which tends to be correlated with the number of protocol users. We measure *Holders* as the natural logarithm of the number of distinct wallets with a positive amount of the protocol governance tokens at various post-launch horizons.[20] Although both these alternative measures provide complementary insights, they are limited in coverage because less than a quarter of the protocols have their governance tokens listed on an exchange, and because on-chain information is only available only for EVM-compatible blockchains.

3.2.3 Auditor Characteristics

Our three measures of auditor quality are *Auditor Market Share*, *Auditor Launch Rate*, and *Auditor Hack Rate*. The first measure, *Auditor Market Share*, represents the fraction of all audit reports produced by a specific auditor out of all audit reports within the previous six months. This measure is intended to reflect the size of the auditor. On average, protocols in our sample are audited by an auditor with a market share of 30% at the time the protocol is launched.

The second measure, *Auditor Launch Rate*, is defined as the ratio of protocols audited by the auditor that subsequently launched and achieved at least $1 million in *TVL* within the last six months, relative to all audits performed by the auditor in the preceding six months. This measure is designed to reflect the rate of successful launches by an auditor. On average, protocols in our sample are audited by firms for which approximately one out of four previously audited protocols successfully generated meaningful economic activity post-launch.

The third measure, *Auditor Hack Rate*, is one minus the percentage of all audits performed by an auditor in the previous six months in which a hack was detected. This measure aims to evaluate the auditor's effectiveness in preventing future security breaches. Protocols in our sample are typically audited by an auditor with a hack rate of 2%.[21]

3.3 Audit Reports

Figure 2 presents the distribution of audit reports with various numbers of vulnerabilities detected. The figure reveals that approximately 35% of audits do not detect any vulnerabilities, and over 70% of reports detect two or fewer vulnerabilities. Additional statistics—in Appendix A3—reveal that the mean length of an audit report is 15 pages, and that, on average, auditors deem only 7% of the detected vulnerabilities as critical, and 41% as major. Additionally, less than half of detected vulnerabilities end up being resolved by the protocol's development team before

[20] Note that we are only able to measure the number of distinct wallets holding protocol tokens outside CEXes and DEXes. It is reasonable to assume that token owners who hold the tokens in their wallets and not on exchanges do this to interact with (i.e., use) the protocol.

[21] For ease of interpretation, we define *Auditor Hack Rate* such that auditor quality is increasing in the variable, which is consistent with *Auditor Market Share* and *Auditor Launch Rate*.

the final audit report is published. Decentralized auditors detect a much larger fraction of major vulnerabilities detected by bounty hunters, 87%, in comparison with centralized auditors, 41%.

[Figure 2 here]

4 Factors Associated with Smart Contract Auditing

We proceed to investigate our first research question: what factors do protocol developers consider when deciding whether to have their smart contracts audited? Table 2 reports estimates of logistic regressions in which the dependent variable is an indicator that equals one if a smart contract protocol has undergone at least one audit before its launch:

$$\mathbb{I}(Audit) = \alpha + \overline{\beta}\Theta + \Lambda + \epsilon. \tag{1}$$

$\mathbb{I}(Audit)$ is the audit indicator, Θ is a vector of protocol characteristics described in Table 1 and Λ is a vector of time, blockchain, and protocol category fixed effects. See Appendix A2 for a detailed description of the blockchain, and protocol fixed effects categories.

Panel A focuses on audits by centralized auditors, whereas Panel B focuses on decentralized auditors (bounty hunters). In both panels, the four columns correspond to estimations that employ different fixed effect structures. In the specification that does not include time-fixed effects, we also include the natural logarithm of the market capitalization of ETH at the time of protocol launch ($\log(ETH\ Mcap)$), as a control for the time-varying level of the DeFi market activity.[22]

[Table 2 here]

In Panel A of Table 2, the coefficient on $\log(ETH\ Mcap)$ is significantly negative, which indicates that the likelihood of a protocol audit by a centralized auditor is negatively associated with the state of the blockchain market. This finding possibly reflects the inability of the supply of auditing services to keep up with demand, particularly during the period of high growth in the beginning of our sample period.

Ethereum Virtual Machine (EVM) coefficients are significantly positive; protocols deployed on EVM chains are substantially (67%-73%) more likely to undergo audits. The likely reason is that there is a larger supply of audit professionals skilled in Solidity, the main programming language of EVM chains. Similarly, significantly positive

[22] We exclude various independent variables from specifications when their variation is subsumed by included fixed effects.

coefficients for *DEX*, *Yield*, and *Lending*, indicate that smart contract protocols belonging to the three most populous categories are substantially (43%-135%) more likely to undergo audits than protocols belonging to less common categories, likely for a similar reason: auditors are more familiar with such protocols.

Significantly positive coefficients on *Raised* indicate that protocols that raise funds are 26%-33% more likely to be audited before launch. This finding suggests that protocols that face financial constraints are less likely to hire an auditor. In addition, the significantly positive coefficients on *Oracle* indicate that smart contracts that employ oracles are substantially (38%-61%) more likely to undergo an audit, consistent with oracles presenting an additional source of risk, which protocols attempt to mitigate via audits. The coefficients for *Open Source* are positive across all specifications, although significantly so for only the first two, suggesting that protocols that are generally transparent are also more likely to undergo audits.

Panel B focuses on factors associated with the likelihood of an audit by decentralized auditors. The results indicate that some of the market, industry (i.e., type of service provided by a protocol), and protocol characteristics associated with the choice of hiring centralized auditors also explain the choice of decentralized auditors. These include log(*ETH Mcap*), *EVM*, *Lending*, and *Oracle*. Interestingly, in contrast to the decision to hire a centralized auditor, the likelihood of being audited by bounty hunters is not associated with whether a protocol had previous funding round(s), consistent with the incentive-based compensation structure of decentralized auditors. The coefficients on *Oracle* are larger in magnitude than in Panel A, and all of the *Open Source* coefficients are significant.

Next, we examine factors associated with a protocol's decision to hire a high-quality auditor, conditional on having its smart contracts audited.[23] Table 3 presents estimates of OLS and Tobit regressions, in which the dependent variables are auditor characteristics that are related to auditor quality: *Auditor Market Share* (in Panel A), *Auditor Launch Rate* (in Panel B), and Auditor Hack Rate (in Panel C). The independent variables are the same as those in Table 2. In Tobit regressions, we also include the inverse Mills ratio as a correction for a protocol developer's decision to obtain an audit we include a correction for self-selection (Heckman 1979).[24]

$$\textit{Auditor Quality} = \alpha + \bar{\beta}\Theta + \Lambda + \epsilon, \tag{2}$$

[Table 3 here]

[23] In this exercise, we focus on an auditor performing the last audit prior to smart contract protocol launch—or the last audit in cases in which a protocol was never deployed on a blockchain. We focus on the last audit because it is widely perceived to be the most important one in light of frequent changes to smart contracts prior to their deployment and the impossibility of making further changes once smart contracts are deployed.

[24] In OLS and Tobit regressions in which we include fixed effects, we exclude variables that are subsumed by included fixed effects. In particular, *log(ETHMcap)* is subsumed by time fixed effects, *EVM* is subsumed by blockchain fixed effects, and *DEX*, *Yield* and *Lending* are subsumed by industry fixed effects. Industry reflects 11 categories including *DEX*, *Yield*, and *Lending*.

In *Auditor Market Share* regressions, the coefficients on log(*ETH Mcap*) are significantly positive, indicating that conditional on choosing to be audited, protocols launching in periods of high growth tend to choose larger auditors, which is consistent with larger auditors having greater flexibility in meeting demand for auditing services. Significantly positive *EVM* coefficients indicate that protocols deploying on EVM-compatible chains tend to choose larger auditors, as these auditors are more likely to have experts in Solidity. Protocols belonging to two of the three main categories, *DEX* and *Lending*, tend to choose larger auditors. *Oracle* coefficients are significantly positive, consistent with additional risk associated with oracles, which protocols attempt to mitigate via audits by a larger auditor. Inferences from Tobit regressions are similar to those based on OLS specifications. Although this alternative specification is well-specified (e.g., no Hauck-Donner effect), λ is not statistically significant, suggesting that selection bias is not a concern in the model. In other words, the coefficients from a standard OLS regression on the main equation (without the Heckman correction) likely yield unbiased estimates. Therefore, we use OLS in all regressions henceforth.

The results for *Auditor Launch Rate* in Panel B are broadly consistent with those for *Auditor Market Share* in Panel A. In particular, the coefficients on *EVM*, *DEX*, *Lender*, and *Oracle* are significantly positive across all specifications. A notable exception is the coefficient on log(*ETH Mcap*), which is significantly negative in *Auditor Launch Rate* regressions, consistent with auditors with high launch rates exhibiting lower flexibility in meeting demand for auditing services during periods of high growth in the smart contract market. The *Auditor Hack Rate* regression results in Panel C are broadly consistent with those in Panels A and B. In particular, the coefficients on *EVM*, *DEX*, *Lender*, and *Oracle* are significantly positive across all specifications.

Overall, the results in Tables 2 and 3 suggest that protocols' decisions to undergo an audit, as well as the decision to hire a high-quality auditor, are associated with several factors, including overall smart contract market activity, blockchain(s) on which a protocol is deployed, the type of service the protocol provides, and smart contract risk.

5 Smart Contract Audits and Economic Outcomes

This section investigates our second research question: is having an audit associated with better real outcomes post-protocol launch, such as a protocol's increased ability to attract funds from depositors and reduced likelihood of future security breaches, and do these outcomes vary across various measures of quality of auditors, such as an auditor's track record of hacks associated with prior audits?

5.1 Association between Post-Launch Outcomes and Audits

We begin by estimating OLS regressions in which the dependent variable is the natural logarithm of *TVL* at various horizons–starting from the day of protocol launch and until three months post-launch, and the main independent variable, *Audit*, is an indicator that equals one for protocols with at least one pre-launch audit. The regressions, whose results are reported in Panel A of Table 4, include the same controls for protocol characteristics as in Tables 2 and 3. In addition, because the regression incorporates post-launch windows, we include *Staking*, as a control for the effects of staking programs on TVL.[25] The resulting regression is:

$$TVL = \alpha + \gamma \mathbb{I}(Audit) + \overline{\beta}\Theta + \Lambda + \epsilon. \tag{3}$$

The key finding from the TVL regressions is that the *Audit* coefficient is significantly positive across all specifications, ranging from 0.03, in the specification in which *TVL* is measured one day after launch, to 0.07, in the specification in which *TVL* is measured one quarter after launch. In dollar terms, these coefficients indicate that audited protocols, on average, have between \$0.5M and \$1M greater *TVL* than those without audits.[26] These dollar amounts are economically meaningful in comparison to the mean TVL value of \$14.24M.

[Table 4 here]

We also estimate (3) using two alternative post-launch outcomes, *Market Capitalization* and *Token Holders* in Panels B and C of 4, respectively. Data availability limits the samples of alternative post-launch performance measures to a maximum of 450 and 312 observations. The value of a protocol's governance tokens is significantly positively associated with the presence of pre-launch audit(s). The number of wallets holding a project's governance tokens is significantly positively related to the presence of pre-launch audi(t) for longer post-launch windows. Taken together, the findings in Table 5 suggest that having a security audit is generally associated with better post-launch outcomes.

5.2 Effect of the Terra-Luna Crash and FTX Collapse on Audited Smart Contracts

We next examine whether the relation between audits and post-launch outcomes changes following two plausibly exogenous shocks to the level of market participants' trust in protocols' and smart contracts' security (e.g., Cong et al. (2023)). The first shock is the Terra-Luna crash in May of 2022, which started with a significant depeg

[25] When a user stakes her cryptocurrency in a smart contract, she helps support the protocol, and in return, she earns rewards (such as interest), often in the form of protocol's governance tokens. As a result, TVL can be mechanically higher for protocols allowing staking.

[26] These dollar amounts are calculated as the product of the coefficient in percent for the first day (quarter) and the mean TVL at launch ($0.03 \times 14.24 = \$0.4272$ million and $0.07 \times 14.24 = \$0.9968$ million).

of UST—Terra blockchain's main stablecoin—from $US on May 7, 2022. The collapse of the Terra ecosystem led to a contagious effect on the crypto market as a whole, resulting in a total loss in value exceeding one trillion USD.[27] The second event is the collapse in November of 2022 of FTX, the second largest centralized crypto exchange, which sent market valuations of cryptocurrencies to their lowest values since 2020 and solidified the "crypto winter."[28] Figure 1 shows the evolution of combined on *TVL* of all protocols around both shocks.

Since one of the important roles of smart contract audits is to assure market participants that the audited smart contracts would operate as intended and would be less susceptible to security concerns, we expect the negative impact of these shocks on protocols' *TVL* to be lower for audited protocols than for non-audited ones. To test this conjecture, we estimate difference-in-differences (DiD) regressions around these two events. We construct a matched sample of audited and similar non-audited protocols using propensity score matching (PSM) based on the nearest neighborhood of the protocol characteristics from Table 2, which are associated with the choice for undergoing an audit.[29] Table in Appendix B presents the results of the matching procedure. The table indicates that matching achieves covariate balance for each of the matching variables, with all differences in means between the two groups insignificantly different from zero.

The dependent variable in the DiD regressions is *TVL*, measured four weeks before and four weeks after the two exogenous shocks. The key independent variables are *Audit* and *Post*, which is an indicator variable that equals one for post-shock observations, and the interaction between *Audit* and *Post*. We also control for the protocol characteristics as in Table 4 as well as industry and blockchain fixed effects. The resulting regression equation is:

$$TVL = \alpha + \gamma_1 \mathbb{I}(Audit) \times \mathbb{I}(Post) + \gamma_2 \mathbb{I}(Audit) + \gamma_3 \mathbb{I}(Post) + \bar{\beta}\Theta + \Lambda + \epsilon. \tag{4}$$

[Table 5 here]

Panels A and B of Table 5 present estimates for the Terra-Luna and FTX shocks, respectively.[30] Panel A reveals that *Post* coefficients are significantly negative across all three specifications. They are also economically large. For

[27] See https://www.coindesk.com/learn/the-fall-of-terra-a-timeline-of-the-meteoric-rise-and-crash-of-ust-and-luna/ and https://decrypt.co/101074/terra-crashed-spectacularly-heres-how-it-launched for discussions of the Terra-Luna crash.

[28] See https://www.foxbusiness.com/markets/inside-collapse-crypto-exchange-ftx-everything-you-need-know. for a description of FTX collapse.

[29] In addition, we control for *Staking*, as it mechanically affects TVL and for Fully Diluted Valuation (*FDV*), a measure in dollars of the total value of tokens available for issuance as a proxy for protocol size. *EVM* and *DEX* are subsumed by fixed effects and, therefore, are not included.

[30] We do not estimate Equation (4) and subsequent equations using the two alternative outcome variables, *Market Capitalization* and *Holders*, because of their relatively small sample sizes and the use of these variables as matching variables for the event study analysis. However, untabulated findings from estimations in which each is used as an outcome variable but excluded from the matching procedure yield qualitatively similar results.

example, *Post* coefficient of -0.23 in column (I), corresponds to a 20.5% reduction in TVL in the post-shock period.[31] Most importantly, the coefficients on our variable of interest–the interaction between *Audit* and *Post*–are significantly positive across all three specifications. The 0.09 interaction coefficient in column (1) indicates that the negative response for audited protocols to the Terra-Luna shock was approximately 36% smaller in magnitude than for non-audited protocols.[32] These findings suggest that audited smart contract protocols tended to be more resilient in the face of the Terra-Luna shock.

The findings in Panel B, focusing on the FTX collapse, yield similar inferences. In particular, across the three specifications, *Post* coefficients are significantly negative, and the interaction term coefficients are significantly positive. Comparing the coefficient of 0.06 on *Audit* × *Post* with the −0.11 *Post* coefficient in column (I) indicates that the negative response for audited protocols to the FTX shock was approximately 55% weaker than the negative response for non-audited protocols.

The key identification assumption underlying our DiD regressions is the absence of a differential trend in TVL between audited and non-audited smart contract protocols before the Terra-Luna and FTX shocks. We assess this parallel trends assumption by replacing *Post* with weekly indicator variables beginning six weeks before each shock and ending thirteen weeks after each shock. We then re-estimate (4) with interactions between *Audit* and the weekly indicators.[33] We omit the indicator for the shock week, which serves as the benchmark week. Panels A and B of Figure 3 plot the coefficients on the interaction terms and their associated 10% confidence intervals for the two shocks. The plots indicate that the differences between the pre-shock coefficients for audited and non-audited protocols are insignificant, which is consistent with the parallel trends assumption. In contrast, the differences in the post-shock coefficients between treatment and control firms are significantly positive, which indicates that the greater resiliency of audited smart contracts to shocks persisted through the post-shock period.

Taken together, the findings in Table 6 and Figure 3 suggest that audits provide market participants and protocol users with some assurance that audited smart contracts would operate as intended and are, therefore, would be less susceptible to security concerns.

5.3 Auditor Quality and TVL

The findings in Tables 4and Table 5 indicate a positive association between pre-launch smart contract audits and post-launch protocol outcomes. In this section, we examine, conditional on having an audit, whether the relation between audit and arguably the most important post-launch outcome—*TVL*—varies with auditor quality.

[31] $-0.205 = e^{-0.23} - 1$.

[32] The sum of the *Post* and *Audit* × *Post* is -0.14, which implies a 13.1% reduction in TVL for audited protocols in the post-event period.

[33] For ease of interpretability, we estimate these regressions using weekly rather than daily data.

To conduct this analysis we use the same three measures of auditor quality as in Table 4, *Auditor Market Share*, *Auditor Launch Rate*, and *Low Auditor Hack Rate*, as well as *Decentralized Auditor* indicators.

In our empirical specification, we regress *TVL* 90 days after protocol launch on the four measures of auditor quality.[34] The regressions include the same control variables as those in Table 4, and time, blockchain, and industry fixed effects. The resulting model is given by (5):

$$\begin{aligned} TVL = \alpha + \gamma_1(Auditor\ Market\ Share) + \gamma_2(Auditor\ Launch\ Rate) \\ + \gamma_3(Auditor\ Hack\ Rate) + \gamma_4\mathbb{I}(Bounty\ Hunters) + \bar{\beta}\Theta + \Lambda + \epsilon. \end{aligned} \tag{5}$$

[Table 6 here]

Columns (I) through (IV) of Table 6, in which the four auditor quality dimensions are examined separately, reveal that *Auditor Launch Rate* and *Auditor Hack Rate* are positively associated with *TVL* 90 days after protocol launch, and that protocols audited by decentralized auditors also have higher *TVL*. Surprisingly, *Auditor Market Share* has a significantly negative association with *TVL*. The findings in Column (V), which includes all four measures of auditor quality, confirm the result in individual specifications. The coefficients are economically meaningful. A one-standard-deviation increase in an auditor's launch rate is associated with 3% increase in *TVL*. A one-standard-deviation decrease in past hack rate is associated with 1.5% higher *TVL*. Protocols audited by decentralized auditors attract 14% higher *TVL* ceteris paribus.

6 Post-launch Security Breaches and Auditor Replacement

6.1 Post-launch Security Breaches

The findings in the previous section suggest that having an audit, particularly by higher-quality auditors as well as by decentralized ones, provides protocol users and market participants with increased confidence that their smart contracts would work as intended and be less vulnerable to security breaches. In this section we examine whether this increased confidence is warranted. Addressing this question poses several challenges. First, because audits are not randomly assigned but are the result of choices made by smart contract developers, it is difficult to rule out the possibility of reverse causality. For example, protocols that are more likely to have vulnerabilities may be more likely to have their smart contracts audited. Second, data regarding protocol hacks are incomplete and in some cases are subject to voluntary disclosure by protocols.

[34] Untabulated findings using other post-launch horizons generally yield similar inferences.

Subject to these limitations, we pose two related questions. First, is there an association between having a smart contract audit and the likelihood of future security breaches? Second, conditional on a smart contract audit, is the likelihood of future security breaches lower for contracts audited by auditors of higher perceived quality?

We address the first question by estimating logistic regressions in which the dependent variable is an indicator that equals one if a protocol experienced a security breach within six months of launch. The main independent variable is an indicator that equals one if a protocol has undergone at least one audit prior to launch:

$$\mathbb{I}(Hack) = \alpha + \gamma \mathbb{I}(Audit) + \overline{\beta}\Theta + \Lambda + \epsilon. \tag{6}$$

[Table 7 here]

The results are reported in Panel A of Table 7. Perhaps surprisingly, the coefficient on *Audit*, which ranges from 1.16 to 1.29, is significantly positive across all specifications, which indicates that the relation between having an audit and the likelihood of a post-launch hack is positive. A possible explanation for this result is that protocol developers may choose to have audits if they believe their protocols are more likely to be subject to future hacks.

We address the second question by focusing on the subset of smart contract protocols that elected to have audits. We estimate logistic regressions in which the dependent variable is again an indicator that equals one if a protocol experienced a security breach within six months of launch. The main independent variables are the three measures of auditor quality, *Auditor Market Share*, *Auditor Launch Rate*, and Auditor Hack Rate, and an indicator for whether a protocol is audited by *Decentralized Auditors*:

$$\begin{aligned}\mathbb{I}(Hack) = \alpha &+ \gamma_1(Auditor\ Market\ Share) + \gamma_2(Auditor\ Launch\ Rate) \\ &+ \gamma_3(Auditor\ Hack\ Rate) + \gamma_4 \mathbb{I}(Bounty\ Hunters) + \overline{\beta}\Theta + \Lambda + \epsilon.\end{aligned} \tag{7}$$

The findings in columns (I) and (II) of Panel B of Table 7 indicate that the likelihood of future security breaches is increasing in the auditor's market share and launch rate. The findings in column (III) indicate that the likelihood of future security breaches is decreasing in the auditor's prior hack rate. The findings in column (IV) indicate that the use of bounty hunters is not significantly associated with the likelihood of future security breaches. These findings generalize to including all four auditor characteristics in the estimation, with the exception that the positive association for auditor launch rate is no longer significant.

Taken together, the findings in Panels A and B of Table 7 suggest an audit of a smart contract is not associated with a decreased likelihood of future security breaches, except for when the audit is performed by an auditor with a history of lower hack incidence.

6.2 Auditor Replacements

The final question we address is whether protocol developers change auditors following security breaches. An auditor's failure to spot vulnerabilities that have led to a security breach may raise doubts about its effectiveness. Additionally, after a breach, stakeholders—investors, users, developers—are likely to scrutinize auditors more closely. Thus, protocols may decide to switch auditors to restore trust and avoid reputational damage. By switching auditors after a breach, protocols may aim to demonstrate commitment to security and transparency.

We examine whether characteristics of the incumbent auditor before a security breach are associated with likelihood that they will be replaced following the breach. We do this by estimating logistic regressions in which the dependent variable, *Replacement*, is an indicator that equals one if a protocol replaces its auditor within six months of protocol launch or within six months of a security breach. The main independent variable, *Post*, equals one if a smart contract protocol is breached within six months of launch. The regression also includes the three auditor quality measures and an indicator for *Decentralized Auditors*. We also include interactions of the quality measures and *Post* to examine differential effects of incumbent auditor quality on the likelihood of replacement conditional on a security event. Additional explanatory variables include protocol characteristics used in prior tables, and controls for time, blockchain, and industry-fixed effects:

$$\begin{aligned}\mathbb{I}(Replacement) = \alpha &+ \gamma_1 \mathbb{I}(Post) \times (Auditor\ Market\ Share) + \gamma_2 \mathbb{I}(Post) \times (Auditor\ Launch\ Rate) \\ &+ \gamma_3 \mathbb{I}(Post) \times (Auditor\ Hack\ Rate) + \gamma_4 \mathbb{I}(Post) \times (Bounty\ Hunter) + \gamma_5 \mathbb{I}(Post) \\ &+ \gamma_6 (Auditor\ Market\ Share) + \gamma_7 (Auditor\ Launch\ Rate) + \gamma_8 (Auditor\ Hack\ Rate) \\ &+ \gamma_9 (Bounty\ Hunter) + \overline{\beta}\Theta + \Lambda + \epsilon.\end{aligned} \tag{8}$$

Table 8 presents the results of estimating equation (8) . The first column reports results for the full sample. Protocols are more likely to replace auditors following a hack episode, as evident from the positive coefficient, 0.23, on the *Post* indicator. Protocols audited by the auditor with the highest *Auditor Market Share*, and those audited by the auditor with the highest *Auditor Launch Rate* are more likely than other auditors to be replaced after a security breach (but not during routine post-launch audits). In contrast, auditors with historically low hack rates and decentralized auditors are not more likely to be replaced than other auditors following a security breach, suggesting that protocols do not rush to update their priors on auditors' skills following a breach.[35]

[35] While the sample of auditor replacements following security breaches is too small for a meaningful empirical analysis, small-sample evidence suggests that auditors with high market shares and high launch rates are less likely to be hired as replacement auditors following a security breach, whereas auditors' with low past hack rates and decentralized auditors are the preferred choices of protocols replacing their incumbent auditors following hacks.

[Table 8 here]

Although the staggered nature of security breaches at the smart contract protocol level provides a quasi-natural experiment involving a protocol's response to an update of its assessment of its auditor's quality, we further strengthen the case for a causal relation by estimating equation (8) for the period before and after the largest hack episode in history —the Poly Network's exploit in August 2021, which reportedly led to $600 million in losses across multiple protocols across several blockchains.[36]

The Poly Network shock was plausibly exogenous at the protocol level. The event caught the attention of regulators and highlighted the importance of auditing work in the DeFi space. For instance, the SEC began to investigate executives behind DeFi applications and raised users' awareness of the relevance of auditing in preventing security breaches and exploits.[37] Therefore, we expect smart contract protocol developers to be more likely to switch auditors in response to security breaches following Poly Network's massive exploit.

In columns (II) and (III) of Table 8, we present findings from estimating equation (8) separately using observations before and after the Poly Network exploit. The findings suggest that protocols are more likely to switch auditors in response to a security breach, as indicated by the positive and statistically significant difference of 0.11 between *Post* coefficients after and before the Poly Network hack. The table also reveals that the propensity to switch auditors after a hack is increasing in *Auditor Market Share* and *Auditor Launch Rate*. These findings are consistent with higher market share and launch rate face larger loss of credibility following security breaches of their audited protocols after the Poly Network hack.

7 Conclusions

This study addresses two fundamental questions about the market for smart contract audits. First, what factors do protocols consider when deciding whether to have their smart contracts audited and what types of auditors to engage? Second, is having an audit associated with real outcomes post-protocol launch, and do these outcomes vary across auditors of varying quality?

Regarding the first question, we find that smart contracts are more likely to undergo an audit when they run on a popular blockchain, such as Ethereum, when protocols raise external funds before launch, when protocols offer relatively common financial services, and when smart contracts are relatively complex/risky. Conditional on having a protocol's smart contracts audited, the choice of a high-quality auditor is largely driven by the same factors.

[36] Poly Network is a cross-chain protocol that focuses on interoperability, allowing users to move digital assets from one blockchain to another. See https://cointelegraph.com/news/hackers-stole-at-least-600m-in-poly-exploit-across-three-chains for a discussion of the hack.

[37] See https://www.sec.gov/news/press-release/2021-145 and https://www.ic3.gov/Media/Y2022/PSA220829.

Regarding the second question, we find that protocols, especially those audited by auditors with larger market share, high past launch rates, and low past hack rates, as well as those audited by decentralized auditors tend to exhibit better post-launch outcomes and are less severely affected by adverse exogenous shocks to the DeFi market. However, we find little evidence that protocols whose smart contracts are audited exhibit lower likelihood of security breaches.

Our study is among first to examine the role auditing plays in the burgeoning decentralized finance markets. To date, the DeFi market has been characterized by low regulation and high risk. Understanding how smart contract audit market impacts real outcomes provides insights to policy makers regarding whether and how to adapt the auditing regulatory apparatus to the DeFi market.[38] Our study also connects the DeFi literature with the accounting and auditing literature by examining the effectiveness of voluntary auditing and by building upon the literature in archival auditing that studies the determinants of auditing quality.

[38] Similar challenges arise in other areas, such as taxation (Cong, Landsman, Maydew, and Rabetti (2023)).

References

Allee, K. D. and T. L. Yohn (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), 1–25.

Amiram, D., B. N. Jørgensen, and D. Rabetti (2022). Coins for bombs: The predictability of on-chain transfers for terrorist attacks. *Journal of Accounting Research 60*(2), 427–466.

Amiram, D., E. Lyandres, and D. Rabetti (2024). Trading volume manipulation and competition among centralized crypto exchanges. Forthcoming. *Management Science* (https://doi.org/10.1287/mnsc.2021.02903).

Antle, R. and B. Nalebuff (1991). Conservatism and auditor-client negotiations. *Journal of Accounting Research 29*, 31–54.

Ashraf, M., P. N. Michas, and D. Russomanno (2020). The impact of audit committee information technology expertise on the reliability and timeliness of financial reporting. *The Accounting Review 95*(5), 23–56.

Bhambhwani, S. and A. H. Huang (2024). Auditing decentralized finance. *British Accounting Review 56*(2), 101270.

Blacconiere, W. and M. DeFond (1997). An investigation of audit opinions and subsequent auditor litigation of publicly-traded failed savings and loans. *Journal of Accounting and Public Policy 16*, 415–454.

Bourveau, T., J. Brendel, and J. Schoenfeld (2024). Decentralized finance (DeFi) assurance: Early evidence. *Review of Accounting Studies 29*, 2209–2253.

Bourveau, T., M. Breuer, J. Koenraadt, and R. Stoumbos (2023). Public company auditing around the securities exchange act. Working Paper. (http://dx.doi.org/10.2139/ssrn.3837593).

Campello, M., P. Jin, D. Rabetti, and F. Saleh (2024). The market for crypto zombies: Under-collateralization in DeFi lending. Working Paper. (https://tinyurl.com/3zfm9a8m).

Clarkson, P. and D. Simunic (1994). Auditor industry specialist research design. *Journal of Accounting and Economics 17*, 207–228.

Cong, L., C. R. Harvey, D. Rabetti, and Z.-Y. Wu (2024). An anatomy of crypto-enabled cybercrimes. Forthcoming. *Management Science* (https://www.nber.org/papers/w30834).

Cong, L. W., K. Grauer, D. Rabetti, and H. Updegrave (2023). Blockchain forensics and crypto-related cybercrimes. Book chapters. (http://dx.doi.org/10.2139/ssrn.4358561).

Cong, L. W., W. R. Landsman, E. L. Maydew, and D. Rabetti (2023). Tax-loss harvesting with cryptocurrencies. *Journal of Accounting and Economics 76*(2–3), 101607.

Cong, L. W., E. Prasad, and D. Rabetti (2023). Financial and informational integration through decentralized oracle networks. Working paper. (https://dx.doi.org/10.2139/ssrn.4495514).

DeFond, M., D. H. Erkens, and J. Zhang (2017). Do client characteristics really drive the big n audit quality effect? new evidence from propensity score matching. *Management Science 63*(11), 3628–3649.

DeFond, M. and K. Subramanyam (1998). Auditor changes and discretionary accruals. *Journal of Accounting and Economics 25*, 35–67.

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

Deng, M., T. Lu, D. A. Simunic, and M. Ye (2014). Do joint audits improve or impair audit quality? *Journal of Accounting Research 52*(5), 1029–1060.

DeSimone, L., P. Jin, and D. Rabetti (2025). Tax planning, illiquidity, and credit risks: Evidence from DeFi lending. (http://dx.doi.org/10.13140/RG.2.2.32320.85760).

Du, K. and S. Wang (2023). In code we trust? the role of blockchain audits in cryptocurrency markets. Working paper. (https://ssrn.com/abstract=4560339).

Duguay, R., M. Minnis, and A. Sutherland (2020). Regulatory spillovers in common audit markets. *Management Science 66*, 3389–3411.

Dye, R. (1991). Informationally motivated auditor replacement. *Journal of Accounting and Economics 14*(2), 347–374.

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

Feng, D., R. Hitsch, K. Qin, A. Gervais, R. Wattenhofer, Y. Yao, and Y. Wang (2023). DeFi auditing: Mechanisms, effectiveness, and user perceptions. *Cryptology ePrint Archive, Paper 2023/1207*.

Francis, J., E. Maydew, and H. Sparks (1999). The role of big 6 auditors in the credible reporting of accruals. *Auditing: A Journal of Practice & Theory 18*(2), 17–34.

Frishkoff, P. (1989). Some observations on the extent of bank audits in america: 1800-1863. Article 19. *Accounting Historians Notebook 12*(1), 41–47.

Gefen, O., D. Rabetti, Y. Sun, and C. Zhang (2024). Code-washing: Evidence from open-source blockchain startups. Working paper. (https://ssrn.com/abstract=5068292).

Gul, F., S. Fung, and B. Jaggi (2009). Earnings quality: Some evidence on the role of auditor tenure and auditors' industry expertise. *Journal of Accounting and Economics 47*, 265–287.

Harvey, C., A. Ramachandran, and J. Santoro (2021). DeFi and the Future of Finance. Hoboken, New Jersey: Wiley.

Harvey, C. R. and D. Rabetti (2024). International business and decentralized finance. *Journal of International Business Studies 55*, 840–863.

Heckman, J. (1979). Sample selection bias as a specification error. *Econometrica 47*(1), 153–161.

Heckman, J. (1990). Varieties of selection bias. *The American Economic Review 80*(2), 313–318.

John, K., L. Kogan, and F. Saleh (2023). Smart contracts and decentralized finance. *Annual Review of Financial Economics 15*, 523–542.

Kaplan, S. and D. Williams (2013). Do going concern audit reports protect auditors from litigation? A simultaneous equations approach. *The Accounting Review 88*, 199–232.

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

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

Lee, S. W., J. Pinto, D. Rabetti, and G. Sadka (2024). Blockchain-induced supply chain transparency and firm performance: The role of capacity utilization. (https://ssrn.com/abstract=4921795).

Lennox, C. and J. Pittman (2010). Big five audits and accounting fraud. *Contemporary Accounting Research 27*(1), 209–247.

Lennox, C., J. Schmidt, and A. Thompson (2023). Why are expanded audit reports not informative to investors? Evidence from the united kingdom. *Review of Accounting Studies 28*, 497–532.

Lennox, C. S. and J. A. Pittman (2011). Voluntary audits versus mandatory audits. *The Accounting Review 86*(5), 1655–1678.

Lisowsky, P. and M. Minnis (2020). The silent majority: Private U.S. firms and financial reporting choices. *Journal of Accounting Research 58*(3), 547–588.

Lobo, G. J., L. Paugam, D. Zhang, and J.-F. Casta (2017). The effect of joint auditor pair composition on audit quality: Evidence from impairment tests. *Contemporary Accounting Research 34*(1), 118–153.

Luo, M., D. Rabetti, and S. Yu (2024). Blockchain adoption and audit quality. Working paper. (https://ssrn.com/abstract=5074602).

Lyandres, E., B. Palazzo, and D. Rabetti (2022). ICO success and post-ICO performance. *Management Science 68*(12), 8658–8679.

Magee, R. and M. Tseng (1990). Audit pricing and independence. *The Accounting Review 65*(2), 315–336.

Makarov, I. and A. Schoar (2022). Cryptocurrencies and decentralized finance (DeFi). Working Paper. (http://www.nber.org/papers/w30006).

Minnis, M. (2011). The value of financial statement verification in debt financing: Evidence from private U.S. firms. *Journal of Accounting Research 49*(2), 457–506.

Minnis, M. and N. Shroff (2017). Why regulate private firm disclosure and auditing? *Accounting and Business Research 47*, 473–502.

Mutchler, J.F., H. W. and J. McKeown (1997). The influence of contrary information and mitigating factors on audit opinion decisions on bankrupt companies. *Journal of Accounting Research 35*(2), 295–310.

Parlour, C. A. (2023). How safe is DeFi? Systemic risk and fragility. *Key Note Talk at the 2023 Global AI Finance Research Conference*.

Reichelt, K. and D. Wang (2010). National and office-specific measures of auditor industry expertise and effects on audit quality. *Journal of Accounting Research 48*(3), 647–686.

Schoenfeld, J. (2024). Cyber risk and voluntary service organization control (SOC) audits. *Review of Accounting Studies 29*, 580–620.

Sheen, L. (2021). The Cryptopians: Idealism, Greed, Lies, and the Making of the First Big Cryptocurrency Craze. New York, New York: Hachette .

Simunic, D. (1980). The pricing of audit services: Theory and evidence. *Journal of Accounting Research 18*(1), 161–190.

Watts, R. and J. Zimmerman (1983). Agency problems, auditing, and the theory of the firm: Some evidence. *Journal of Law and Economics 26*(3), 613–633.

Yuyama, T., K. Katayama, and P. Brigner (2023). Proposal of principles of DeFi disclosure and regulation. *Financial Cryptography and Data Security. 13953*.

Figure 1. Total Value Locked and Smart Contract Audits. This figure depicts monthly Total Value Locked *(TVL)* and the monthly number of audit reports across all protocols. The audit report (TVL) scale is on the left (right) side of the figure. TVL is plotted in dashed red. The number of audit reports is plotted in solid blue. The sample period is from January 2020 to October 2023. The shaded area indicates that auditing reports for this period are still in formation.

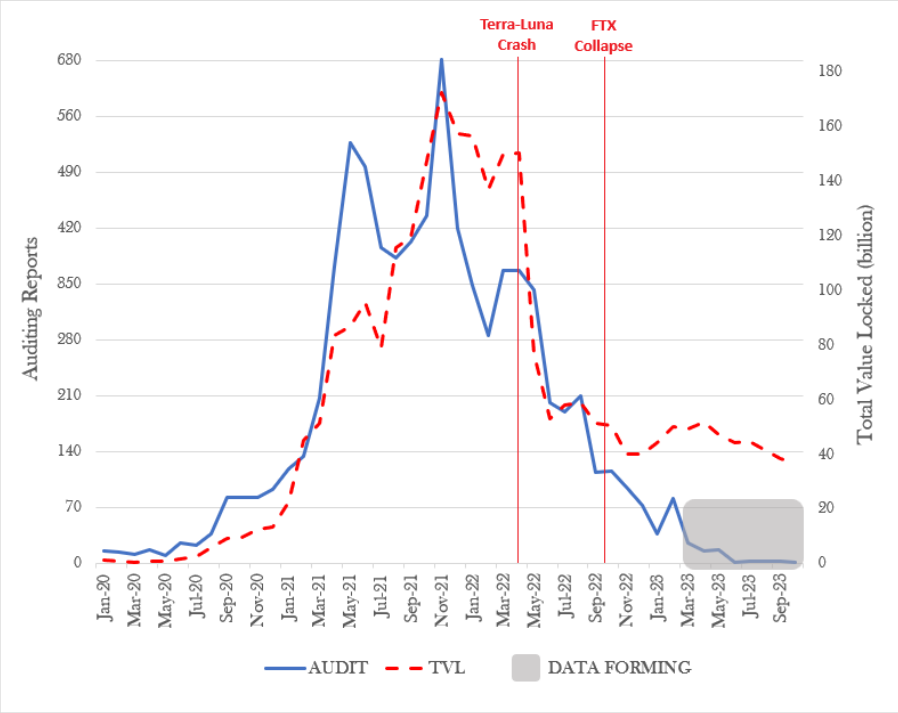


Figure 2. Distribution of Vulnerabilities in Audit Reports. This figure depicts the proportion of vulnerabilities detected across the sample of audit reports.

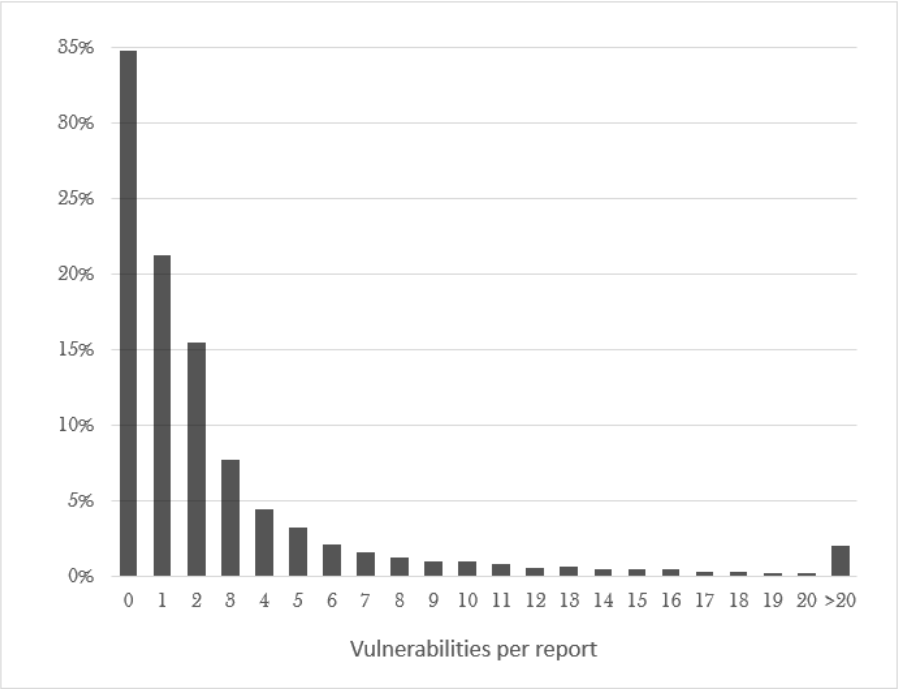


Figure 3. TVL around Terra-Luna and FTX Shocks: This figure depicts daily standardized *TVL* coefficients for audited DeFi protocols (*Treatment group*, in light blue) and non-audited protocols (*Control group*, in orange) is responses to exogenous shocks. Panel A depicts weekly coefficients around the Terra-Luna crash. Panel B depicts the daily coefficients around the FTX collapse. All continuous predictors are mean-centered and scaled by one standard deviation. Standard errors (reported in confidence intervals) are heteroskedasticity consistent and clustered at the category × blockchain. Vertical lines depict 10% confidence intervals around coefficient estimates.

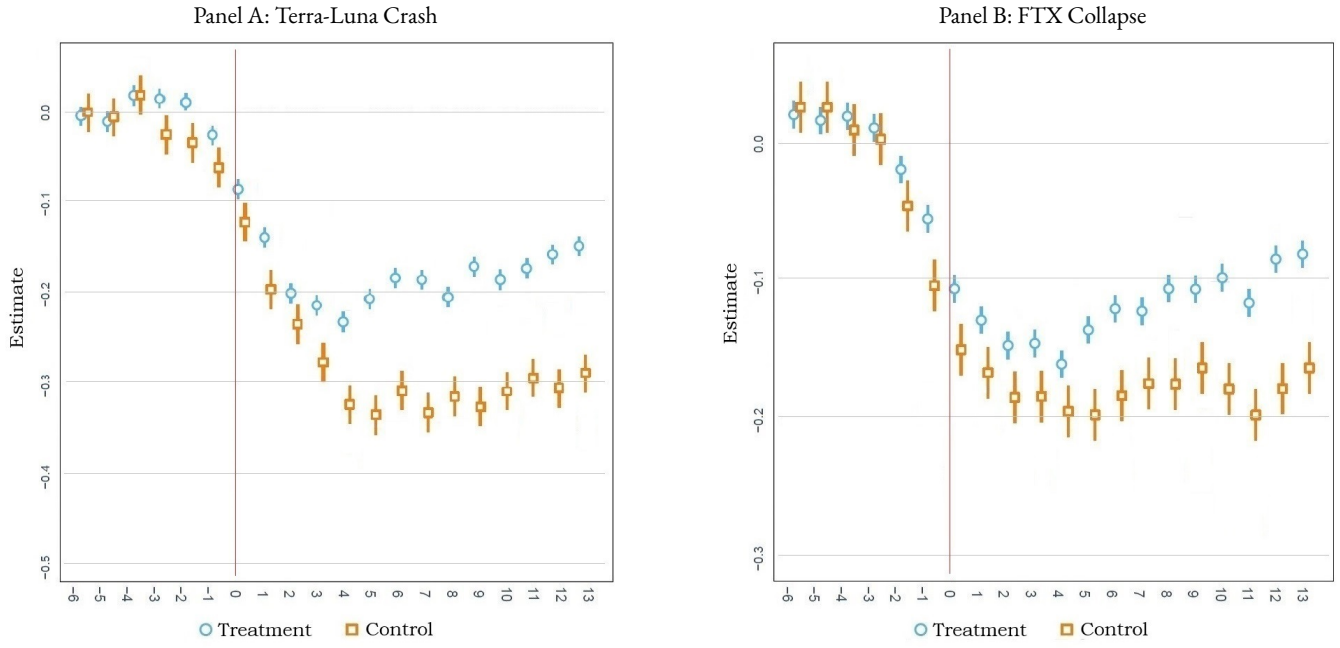


Table 1. Summary Statistics: Auditor and Protocol Characteristics and Outcomes. This table presents summary statistics of variables used in the empirical analysis: protocol characteristics, post-launch outcomes, and auditor characteristics. *Ethereum* is an indicator variable that equals one if a protocol has been deployed on Ethereum (possibly among several blockchains). *EVM* is an an indicator variable that equals one if a protocol has been deployed on at least one Ethereum Virtual Machine (*EVM*) compatible chain. *DEX* (*Yield*, *Lending*) is an indicator variable that equals one if a protocol's main activity is the operation of Decentralized exchange (Yield farming service, Collateralized or flash lending/borrowing platform). *Oracle* is indicator variable that equals one if a protocol uses external inputs from other protocols or outside the blockchain. *Open Source* is an indicator variable that equals one if parts of a protocol's code transcending smart contracts are available on Github. *Raised* is an indicator variable that equals one if the entity developing a protocol has raised external funds. *Raised amount* is the amount of external funds raised (in $M), conditional on raising a positive amount. *# Chains* is the number of blockchains on which a protocol's smart contracts are deployed. *Audited Protocols* is an indicator variable that equals one if a protocol's smart contracts have been audited by at least one auditor. *# Audits* is the number of auditors that produced reports for a protocol's smart contracts. Post-audit security breach (*Hack*) is an indicator variable that equals one if the protocol has been hacked within six months of launch. Total value locked (*TVL*) at launch equals the amount of funds deposited into the protocol at the end of the first week following protocol deployment. Market capitalization (*MCap*) at launch equals the product of protocol's governance token price at the end of the first week following deployment and the number of tokens outstanding at the end of that week. The number of token holders (*Holders*) at launch equals the number of distinct wallets with a positive amount of the protocol's governance tokens at the end of the first post-launch week. *Auditor Market Share* is the fraction of all audit reports produced by the auditor out of all audit reports within the last six months. *Auditor Launch Rate* is the ratio of protocols audited by the auditor launching and achieving at least $1M in TVL in the last six months relative to all audits by the auditor in the preceding six months. *Auditor Hack Rate* is the percentage of all audits performed by an auditor in the previous six months in which a hack was detected.

Auditor and Protocol Characteristics and Outcomes						
	Min.	**Median**	**Mean**	**Max.**	**Sd.**	**Obs.**
	(I)	(II)	(III)	(IV)	(V)	(VI)
Protocol Characteristics:						
Ethereum	0.00	0.00	0.37	1.00	0.48	1,575
EVM	0.00	1.00	0.74	1.00	0.44	1,575
DEX	0.00	0.00	0.28	1.00	0.45	1,575
Yield	0.00	0.00	0.20	1.00	0.40	1,575
Lending	0.00	0.00	0.19	1.00	0.29	1,575
Oracle	0.00	0.00	0.25	1.00	0.43	1,575
Open Source	0.00	0.00	0.09	1.00	0.10	1,575
Raised	0.00	0.00	0.35	1.00	0.48	1,575
Raised amount ($M)	0.05	3.50	9.63	153.00	7.06	552
# Chains	1.00	1.00	1.58	25.00	1.81	1,575
Audited Protocol	0.00	1.00	0.57	1.00	0.49	1,575
# Audits	0.00	2.00	1.16	4.00	1.02	1,575
Post-Audit Security Breach (*Hack*)	0.00	0.00	0.07	1.00	0.22	1,575
Outcomes (at launch):						
Total value locked (*TVL ($M)*)	1.00	4.69	14.24	177.68	92.65	1,575
Market capitalization (*MCap ($M)*)	7.96	6.31	41.27	293.58	139.89	450
Number of token holders (*Holders (#)*)	12.52	69.31	71.35	207.94	105.32	312
Auditor Characteristics:						
Auditor Market Share	0.01	0.11	0.30	1.00	0.38	902
Auditor Launch Rate	0.00	0.23	0.27	0.75	0.27	902
Auditor Hack Rate	0.00	0.00	0.02	1.00	0.10	902

Table 2. Audit Presence. This table presents results of estimating logistic regressions in which the dependent variable is an indicator variable that equals one if a protocol has undergone at least one audit by a centralized auditor (in Panel A) and by a decentralized auditor (in Panel B). The independent variables are protocol characteristics described in Table 1. log*(ETH Mcap)* is the natural logarithm of lagged market capitalization of ETH at the time of protocol launch. Standard errors are heteroskedasticity robust and clustered at category × blockchain. *** p < 0.01; ** p < 0.05; * p < 0.1.

	Panel A: Centralized Auditors				*Panel B: Decentralized Auditors*			
	(I)	(II)	(III)	(IV)	(V)	(VI)	(VII)	(VIII)
log(ETH Mcap)	−0.63 ***				−0.72 ***			
	(0.13)				(0.26)			
EVM	0.73 ***	0.67 ***			1.75 **	1.76 **		
	(0.13)	(0.13)			(0.74)	(0.87)		
DEX	0.60 ***	0.49 ***	0.43 ***		0.61	0.65	0.69	
	(0.14)	(0.14)	(0.14)		(0.94)	(0.95)	(0.95)	
Yield	0.77 ***	0.65 ***	0.71 ***		0.23	0.22	0.16	
	(0.15)	(0.15)	(0.16)		(1.18)	(1.18)	(1.18)	
Lending	1.35 ***	1.28 ***	1.28 ***		1.78 **	1.75 **	1.75 **	
	(0.23)	(0.23)	(0.24)		(0.87)	(0.88)	(0.88)	
Raised	0.29 **	0.33 ***	0.28 **	0.26 **	0.57	0.51	0.63	0.96
	(0.12)	(0.12)	(0.12)	(0.13)	(0.84)	(0.82)	(0.82)	(0.83)
Oracle	0.61 ***	0.60 ***	0.51 ***	0.38 ***	2.31 ***	2.36 ***	2.36 ***	2.44 ***
	(0.13)	(0.13)	(0.14)	(0.15)	(0.77)	(0.77)	(0.77)	(0.79)
Open Source	2.86 ***	2.73 ***	1.46	1.17	0.41 ***	0.42 ***	0.42 ***	0.40 **
	(1.06)	(1.05)	(1.17)	(1.18)	(0.14)	(0.15)	(0.15)	(0.16)
Time FE	No	Yes	Yes	Yes	No	Yes	Yes	Yes
Blockchain FE	No	No	Yes	Yes	No	No	Yes	Yes
Category FE	No	No	No	Yes	No	No	No	Yes
Obs.	1,575	1,575	1,575	1,575	1,575	1,575	1,575	1,575
Pseudo.r.^{2}	0.15	0.16	0.23	0.28	0.16	0.17	0.17	0.19

Table 3. Auditor Quality Choice. This table presents results of estimating OLS and Tobit regressions in which the dependent variables are proxies for audit quality of the last auditor performing protocol audit before its launch. The regressions are estimated using a sample of protocols with at least one audit. In Panel A, the dependent variable is *Auditor Market Share*. In Panel B, the dependent variable is *Auditor Launch Rate*. In Panel C, the dependent variable is *Auditor Hack Rate*. Tobit regressions include Heckman's correction (e.g., Heckman, 1979, 1990), λ (see Appendix C for first-stage regressions). See Table 1 for definitions of the dependent and independent variables reported in this table. Standard errors are heteroskedasticity robust and clustered at category × blockchain. *** p < 0.01; ** p < 0.05; * p < 0.1.

	Panel A: Auditor Market Share				*Panel B: Auditor Launch Rate*				*Panel C: Auditor Hack Rate*			
	OLS		*Tobit*		*OLS*		*Tobit*		*OLS*		*Tobit*	
	(I)	(II)	(III)	(IV)	(V)	(VI)	(VII)	(VIII)	(IX)	(X)	(XI)	(XII)
log(ETH Mcap)	0.05 ***		0.03 *		—0.04 ***		—0.08 ***		—0.02		—0.06 *	
	(0.02)		(0.02)		(0.01)		(0.02)		(0.01)		(0.03)	
EVM	0.16 ***		0.53 ***		0.09 ***		0.23 ***		0.09 ***		0.23 ***	
	(0.02)		(0.07)		(0.01)		(0.03)		(0.01)		(0.03)	
DEX	0.07 ***		0.20 ***		0.03 **		0.08 **		0.03 *		0.08 *	
	(0.02)		(0.07)		(0.02)		(0.03)		(0.01)		(0.04)	
Yield	0.02		0.06		0.00		0.01		0.02		0.06	
	(0.02)		(0.07)		(0.02)		(0.04)		(0.02)		(0.05)	
Lending	0.09 ***		0.30 ***		0.10 ***		0.19 ***		0.05 **		0.16 **	
	(0.03)		(0.10)		(0.02)		(0.05)		(0.02)		(0.06)	
Raised	0.00	—0.02	0.03	—0.03	0.02	0.00	0.03	—0.01	0.00	-0.01	0.01	—0.03
	(0.02)	(0.02)	(0.06)	(0.06)	(0.01)	(0.01)	(0.03)	(0.03)	(0.01)	(0.01)	(0.04)	(0.04)
Oracle	0.09 ***	0.06 ***	0.30 ***	0.22 ***	0.08 ***	0.06 ***	0.17 ***	0.13 ***	0.06 ***	0.04 ***	0.18 ***	0.13 ***
	(0.02)	(0.02)	(0.06)	(0.06)	(0.01)	(0.01)	(0.03)	(0.03)	(0.01)	(0.01)	(0.04)	(0.04)
Open Source	—0.04	—0.05	—0.28	—0.27	0.03	0.03	0.21	0.22	0.22 ***	0.24 ***	0.56 ***	0.61 **
	(0.09)	(0.11)	(0.28)	(0.36)	(0.06)	(0.08)	(0.13)	(0.17)	(0.06)	(0.08)	(0.17)	(0.23)
λ			—0.47	—0.14			—0.14	—0.24			—0.13	—0.18
			(0.33)	(0.16)			(0.20)	(0.17)			(0.24)	(0.14)
Time FE	No	Yes	No	Yes	No	Yes	No	Yes	No	Yes	No	Yes
Blockchain FE	No	Yes	No	Yes	No	Yes	No	Yes	No	Yes	No	Yes
Category FE	No	Yes	No	Yes	No	Yes	No	Yes	No	Yes	No	Yes
Obs.	902	902	902	902	902	902	902	902	902	902	902	902
Adj.r.^{2} / log-likelihood	0.05	0.08	1,406	1,365	0.08	0.12	1,008	960	0.08	0.12	1,008	960

Table 4. Post-launch Outcomes. This table presents results of estimating the effects of auditing on several post-launch outcomes at various horizons post-launch (the end of the launch day, seven days post-launch, one-month post-launch, and three months post-launch). The dependent variable is as follows. In Panel A, Total Value Locked (*TVL*) equals the natural logarithm of the funds deposited into the protocol (in $M). In Panel B, Market Capitalization *(MCap)* is the natural logarithm of the product of the protocol's governance token price and the number of tokens outstanding (in $M). In Panel C, the Number of Token Holders (*Holders*) is the natural logarithm of the number of wallets with a positive amount of the protocol's governance tokens. For all specifications, the main independent variable, *Audit*, is an indicator variable that equals one if there was at least one protocol audit. Standard errors are heteroskedasticity robust and clustered at category × blockchain. *** p < 0.01; ** p < 0.05; * p < 0.1.

	Baseline Specification				*Alternative Specifications*							
	Panel A: Total Value Locked				*Panel B: Market Capitalization*				*Panel C: Holders*			
	Day	*Week*	*Month*	*Quarter*	*Day*	*Week*	*Month*	*Quarter*	*Day*	*Week*	*Month*	*Quarter*
	(I)	(II)	(III)	(IV)	(V)	(VI)	(VII)	(VIII)	(IX)	(X)	(XI)	(XII)
Audit	0.03 *	0.05 ***	0.06 ***	0.07 ***	0.02 **	0.03 ***	0.04 ***	0.04 ***	0.03	0.08	0.10 *	0.17 ***
	(0.02)	(0.01)	(0.02)	(0.02)	(0.01)	(0.01)	(0.01)	(0.02)	(0.06)	(0.05)	(0.05)	(0.06)
log(ETH Mcap)	0.01	0.02	0.10 ***	0.16 ***	0.06 ***	0.05 ***	0.08 ***	0.09 ***	0.01 ***	0.02 ***	0.03 ***	0.06 ***
	(0.03)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.02)	(0.00)	(0.00)	(0.01)	(0.02)
Staking	0.00 **	0.00 **	0.01 ***	0.01 ***	0.00 ***	0.00 ***	0.00 ***	0.00 ***	0.01 **	0.01 **	0.01 **	0.01 **
	(0.00)	(0.00)	(0.00)	(0.00)	(0.00)	(0.00)	(0.00)	(0.00)	(0.00)	(0.00)	(0.00)	(0.00)
Raised	0.01	0.02 *	0.02	0.01	0.02 *	0.02 **	0.03 ***	0.04 ***	0.08	0.04	0.10 **	0.09 *
	(0.02)	(0.01)	(0.01)	(0.02)	(0.01)	(0.01)	(0.01)	(0.01)	(0.05)	(0.05)	(0.05)	(0.05)
Oracle	0.04 *	0.03 **	0.05 ***	0.05 ***	0.01	0.02	0.01	0.02	0.05	0.09 *	0.10 **	0.11 **
	(0.02)	(0.02)	(0.02)	(0.02)	(0.01)	(0.01)	(0.01)	(0.01)	(0.06)	(0.05)	(0.05)	(0.05)
Open Source	0.17 **	0.16 **	0.16 **	0.19 *	0.15 **	0.15 **	0.14 **	0.17 *	0.47	0.43	0.59	0.41
	(0.08)	(0.08)	(0.08)	(0.10)	(0.07)	(0.07)	(0.07)	(0.09)	(0.43)	(0.37)	(0.42)	(0.41)
Time FE	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Blockchain FE	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Category FE	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Obs.	1,383	1,365	1,297	1,067	450	449	441	394	312	312	311	282
Adj.r.^{2}	0.06	0.11	0.23	0.29	0.16	0.18	0.22	0.26	0.11	0.16	0.17	0.21

Table 5. Audits and TVL: Exogenous Shocks. This table reports estimates of OLS regressions in which the dependent variable is protocol's Total Value Locked (*TVL*) around exogenous shocks to the blockchain ecosystem. In Panel A, the sample included all protocols operating 4 weeks before and 4 weeks after the Terra-Luna crash on May 7, 2022. In Panel B, the sample includes all protocols operating 4 weeks before and 4 weeks after the FTX bankruptcy filing on November 11, 2022. The regressions are estimated on matched samples, constructed using the matching procedure summarized in Appendix B. The main independent variables of interest are: *Audit*—an indicator variable that equals one if a protocol has been audited at least once, *Post*—indicator variable that equals one for observations occurring after the event in question, and *Audit* × *Post*—the product of the two indicators. All the other independent variables are as in Table 4. Standard errors are heteroskedasticity robust and clustered at the category × blockchain. *** p < 0.01; ** p < 0.05; * p < 0.1.

Panel A: Terra-Luna Crash

	(I)	(II)	(III)
Audit	0.04	0.04	0.03
	(0.03)	(0.03)	(0.02)
Post	−0.23 ***	−0.22 ***	−0.22 ***
	(0.03)	(0.03)	(0.03)
Audit × *Post*	0.09 ***	0.09 ***	0.08 **
	(0.03)	(0.03)	(0.03)
Controls	Yes	Yes	Yes
Category FE	No	Yes	Yes
Blockchain FE	No	No	Yes
Obs.	37,296	37,296	37,296
Pseudo.r.^{2}	0.22	0.24	0.27

Panel B: FTX Collapse

	(I)	(II)	(III)
Audit	0.02	0.02	0.02
	(0.01)	(0.01)	(0.01)
Post	−0.11 ***	−0.09 ***	−0.09 ***
	(0.03)	(0.03)	(0.03)
Audit × *Post*	0.06 ***	0.05 ***	0.05 **
	(0.02)	(0.02)	(0.02)
Controls	Yes	Yes	Yes
Category FE	No	Yes	Yes
Blockchain FE	No	No	Yes
Obs.	37,296	37,296	37,296
Pseudo.r.^{2}	0.19	0.20	0.22

Table 6. Auditor Quality and TVL. This table reports estimates of OLS regressions in which the dependent variable is protocol's Total Value Locked (*TVL*) 90 days post-protocol launch. The main independent variables are measures of auditor quality: *Auditor Market Share*, *Auditor Launch Rate*, *Auditor Hack Rate*, and, *Bounty Hunter* indicator. See Table 1 for definitions of dependent variables. The remaining independent variables (controls; not reported) are as in Table 2. The sample includes all launched protocols with at least $1M of TVL within the first week from launch. All regressions include industry, blockchain, and time fixed effects. Standard errors are heteroskedasticity robust and clustered at category × blockchain. *** p < 0.01; ** p < 0.05; * p < 0.1.

Effects of Auditor Reputation on TVL					
	(I)	(II)	(III)	(IV)	(V)
Centralized Auditors:					
Auditor Market Share	−0.04 **				−0.03
	(0.02)				(0.03)
Auditor Launch Rate		0.09 **			0.11 **
		(0.04)			(0.05)
Auditor Hack Rate			0.11 ***		0.13 ***
			(0.03)		(0.04)
Decentralized Auditors:					
Bounty Hunter				0.11 ***	0.14 ***
				(0.03)	(0.04)
Controls	Yes	Yes	Yes	Yes	Yes
Time FE	Yes	Yes	Yes	Yes	Yes
Blockchain FE	Yes	Yes	Yes	Yes	Yes
Category FE	Yes	Yes	Yes	Yes	Yes
Obs.	809	809	809	809	809
Adj.r^2	0.18	0.18	0.18	0.20	0.21

Table 7. Audit Presence, Auditor Quality, and Security Breaches. This table reports estimates of logistic regressions in which the dependent variable is an indicator variable that equals one for protocol that had a security breach (hack) within six months of launch. In Panel A, the main independent variable is an indicator variable that equals one for protocols that has undergone at least one audit prior to launch. In Panel B, the main independent variables are measures of auditor quality: *Auditor Market Share*, *Auditor Launch Rate*, *Auditor Hack Rate*, and, *Bounty Hunter* indicator. See Table 1 for definitions of dependent variables. The remaining independent variables (controls; not reported) are as in Table 2. In Panels A, the sample includes all launched protocols. In Panel B, the sample includes all launched protocol that have been audited at least once prior to launch. All regressions include industry, blockchain, and time fixed effects. In Panel B, we also include Heckman's correction for self-selection. Standard errors are heteroskedasticity robust and clustered at category × blockchain. *** p < 0.01; ** p < 0.05; * p < 0.1.

Panel A: Effect of Audit Presence on Security Breaches

	(I)	(II)	(III)	(IV)
Audit	1.29 ***	1.16 ***	1.17 ***	1.20 ***
	(0.42)	(0.42)	(0.45)	(0.44)
Controls	Yes	Yes	Yes	Yes
Time FE	No	Yes	Yes	Yes
Blockchain FE	No	No	Yes	Yes
Category FE	No	No	No	Yes
Obs.	1,575	1,575	1,575	1,575
Pseudo.r.^{2}	0.13	0.16	0.18	0.18

Panel B: Effect of Auditor Characteristics on Security Breaches

	(I)	(II)	(III)	(IV)	(V)
Centralized Auditors:					
Auditor Market Share	0.11 *				0.16 *
	(0.06)				(0.10)
Auditor Launch Rate		1.23 *			1.14
		(0.72)			(1.08)
Auditor Hack Rate			−0.29 **		−0.31 **
			(0.10)		(0.14)
Decentralized Auditors:					
Bounty Hunters				−1.19	−1.37
				(0.96)	(0.94)
Controls	Yes	Yes	Yes	Yes	Yes
Time FE	Yes	Yes	Yes	Yes	Yes
Blockchain FE	Yes	Yes	Yes	Yes	Yes
Category FE	Yes	Yes	Yes	Yes	Yes
Obs.	902	902	902	902	902
Pseudo.r.^{2}	0.16	0.16	0.19	0.15	0.18

Table 8. Security Breaches and Replaced Auditors. This table reports estimates of logistic regressions in which the dependent variable is an indicator variable that equals one for protocols that replaced their auditor. The main independent variable, *Post*, equals one if a smart contract protocol is breached within six months of launch. The other independent variables are measures of auditor quality: *Auditor Market Share*, *Auditor Launch Rate*, *Auditor Hack Rate*, and, *Bounty Hunter* indicator. See Table 1 for definitions of dependent variables. Regressions also include interactions of the post-breach indicator with the four auditor indicators above. See Table 1 for the description of variables. The remaining independent variables (not reported) are as in Table 2. The first column reports results for the full sample. Columns (II)-(III) report regression results for the period before and after August 2021, respectively. Column (IV) reports the difference between the coefficients obtained within the before and after subsamples. All regressions include industry, blockchain, and time-fixed effects. Standard errors are heteroskedasticity robust and clustered at category × blockchain. *** p < 0.01; ** p < 0.05; * p < 0.1.

Characteristics of Replaced Auditors				
	Full Sample	*Poly Network Hack*		
		Before	*After*	*Diff*
	(I)	(II)	(III)	(IV)
Post	0.23 ***	0.15 ***	0.26 ***	0.11 ***
	(0.03)	(0.04)	(0.04)	(0.03)
Centralized Auditors:				
Auditor Market Share	0.00	0.00	0.00	0.00
	(0.01)	(0.03)	(0.02)	(0.02)
Auditor Launch Rate	0.00	0.00	0.00	0.00
	(0.02)	(0.03)	(0.02)	(0.02)
Auditor Hack Rate	0.00	0.00	0.00	0.00
	(0.00)	(0.00)	(0.00)	(0.00)
Post × *Auditor Market Share*	0.19 ***	0.10 **	0.23 ***	0.12 **
	(0.06)	(0.06)	(0.07)	(0.07)
Post × *Auditor Launch Rate*	0.07 *	0.05	0.11 **	0.06 *
	(0.04)	(0.04)	(0.05)	(0.04)
Post × *Auditor Hack Rate*	0.03	0.02	0.05	0.03
	(0.01)	(0.02)	(0.03)	(0.02)
Decentralized Auditors:				
Bounty Hunters	0.00	0.03	—0.02	—0.05
	(0.04)	(0.07)	(0.07)	(0.06)
Post × *Bounty Hunters*	—0.07	—0.07	—0.07	0.00
	(0.05)	(0.04)	(0.05)	(0.01)
Controls	Yes	Yes	Yes	Yes
Time FE	Yes	Yes	Yes	Yes
Blockchain FE	Yes	Yes	Yes	Yes
Category FE	Yes	Yes	Yes	Yes
Obs.	902	310	592	902
Adj.r.^{2}	0.27	0.16	0.35	0.32

Appendices for "Auditing Smart Contracts"

Wayne Landsman, Evgeny Lyandres, Edward Maydew, and Daniel Rabetti"

Appendix A1 — Example of an Audit Report

Binance zk-SNARKs Proof of Solvency
Independent Technical Assessment

Feb 14, 2023

Repositories:

https://github.com/binance/zkmerkle-proof-of-solvency

Commit:

c1884aae22cd17af023ac4424b4e6623eb0ea9dd

References:

- Announcement
- How to Verify Your Account Balance on Binance
- How zk-SNARKs Improve Binance's Proof of Reserves System
- Proof of solvency - technical specification
- Having a safe CEX: proof of solvency and beyond

Authors:

Luciano Ciattaglia (l.ciattaglia@hacken.io)
Bartosz Barwikowski (b.barwikowski@hacken.io)
Yaroslav Bratashchuk (y.bratashchuk@hacken.io)
Sofiane Akermoun (s.akermoun@hacken.io)

Example of Audit Report for Binance PoS tech assessment—Continuation. This figure depicts a sample from a smart contract auditing report for Binance Proof-of-Stake.

2 Project Summary

In the project we identified 1 critical issue which allows to fake the total debt amount in the zero knowledge proof circuit, 1 medium severity issue and 2 other low severity issues. The critical and medium severity issues have been already fixed. However, any proof generated before those issues were fixed cannot be verified to be valid, as the critical one allowed for the total debt amount to be tampered. Although the proofs may appear to be valid, it is not possible to ensure that they were not modified due to the vulnerability. The other low severity issues are very unlikely to be abused and do not need to be addressed immediately.

The project has 1157 dependencies, all of them with checksum verification. There were found 42 vulnerabilities within all dependencies, with 16 of them having public exploits available. 22 with high severity and 20 with medium. None of the vulnerable functions are currently being used in the project.

It uses a forked version of gnark made on Sep 2022 for the circuits and Poseidon with BN254 hash function to hash the user information and the Sparse Merkle Tree (SMT) data structure to store the hashes. The SMT is implemented using the BSMT library, and its maximum depth is set to be 28, which means that this Proof Of Solvency approach may be used for more than 250M users.

The code quality is clean and organized.

The README.md contains instructions on how to run tools one by one, and motivation behind the circuits is also detailed.

The Panic is used for main function error handling, so all the tools crash with a stack trace in case of an error.

The sample user data (balance sheets) is provided in order to test tools manually. There is a way to fetch (probably production) Postgres configuration from the AWS storage if the remote_password_config flag is provided to the tools that use Postgres.

There was a function to generate fake accounts in the witness service, which was commented out but still left in the code (probably for manual testing purposes). EmptyAccounts are generated in the witness, and they are used in case the last account's batch size is less than 864.

Example of Audit Report for Binance PoS tech assessment—Continuation. This figure depicts a sample from a smart contract auditing report for Binance Proof-of-Stake.

The git history log has been modified several times, and as a result, the git metadata is mixed in some places.

3 Vulnerabilities

3.1 [Critical][Fixed] TotalDebt manipulation vulnerability caused by overflow of BasePrice

The code contains a critical error that enables it to create false user debt, reducing the number of assets needed. This occurs because there is a method to circumvent the assertion that checks if the user's debt exceeds their equity.

There is a bug in the system that allows for bypassing because the BasePrice parameter can be set to an extremely high value. This vulnerability exists because the parameter is not checked for value range, making it easy to manipulate. Although the BasePrice is publicly accessible, it would be simple to identify if it has been changed. However, there is a method to modify the BasePrice in a way that would be undetectable by other users, making it possible to exploit the vulnerability without being detected.

As an optimization, the code splits all the users into batches, each with 864 users. The batches are linked with each other by sharing information about assets and the cryptographic hashes. Each exchange asset is shared using three variables: TotalEquity, TotalDebt and BasePrice. The hash of asset is calculated from one big integer, which is calculated using the following formula:

$$TotalEquity * 2^{128} + TotalDebt * 2^{64} + BasePrice$$

The problem is, that in the code responsible for doing these calculations, only *TotalEquity* and *TotalDebt* are checked if they are greater or equal to 0 and lower than 2^{64}. The value of BasePrice is not being checked, which allows to set it to value higher than $2^{64} - 1$ which makes it possible to modify the value of *TotalDebt* and *TotalEquity*. Because of that, it is possible to generate the same value for different parameters, for example both *TotalDebt* = 2, *BasePrice* = 3 and *TotalDebt* = 1, *BasePrice* = $2^{64} + 3$ will have value of $2 * 2^{64} + 3$. The source code responsible for this calculations:

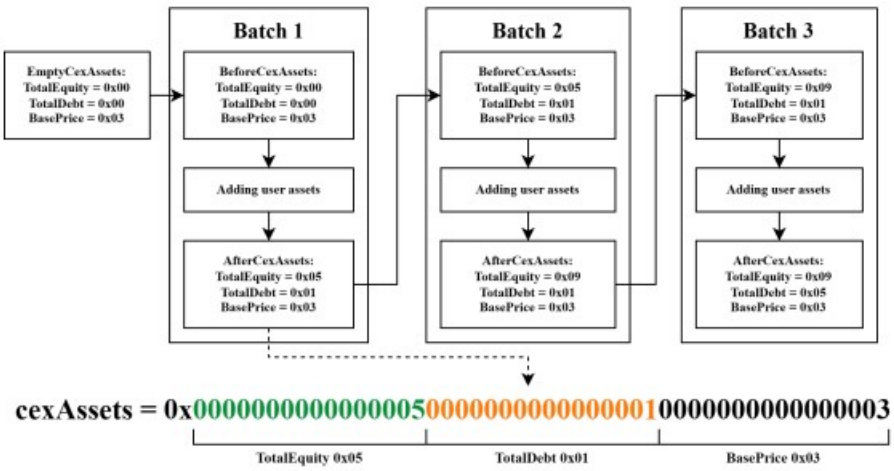
Example of Audit Report for Binance PoS tech assessment—Continuation. This figure depicts a sample from a smart contract auditing report for Binance Proof-of-Stake.

```
// verify whether beforeCexAssetsCommitment is computed correctly
for i := 0; i < len(b.BeforeCexAssets); i++ {
        CheckValueInRange(api, b.BeforeCexAssets[i].TotalEquity)
        CheckValueInRange(api, b.BeforeCexAssets[i].TotalDebt)
        cexAssets[i] = api.Add(api.Mul(b.BeforeCexAssets[i].TotalEquity, utils.Uint64MaxValueFrSquare),
                api.Mul(b.BeforeCexAssets[i].TotalDebt, utils.Uint64MaxValueFr), b.BeforeCexAssets[i].BasePrice)
        afterCexAssets[i] = b.BeforeCexAssets[i]
}
actualCexAssetsCommitment := poseidon.Poseidon(api, cexAssets...)
api.AssertIsEqual(b.BeforeCEXAssetsCommitment, actualCexAssetsCommitment)
```

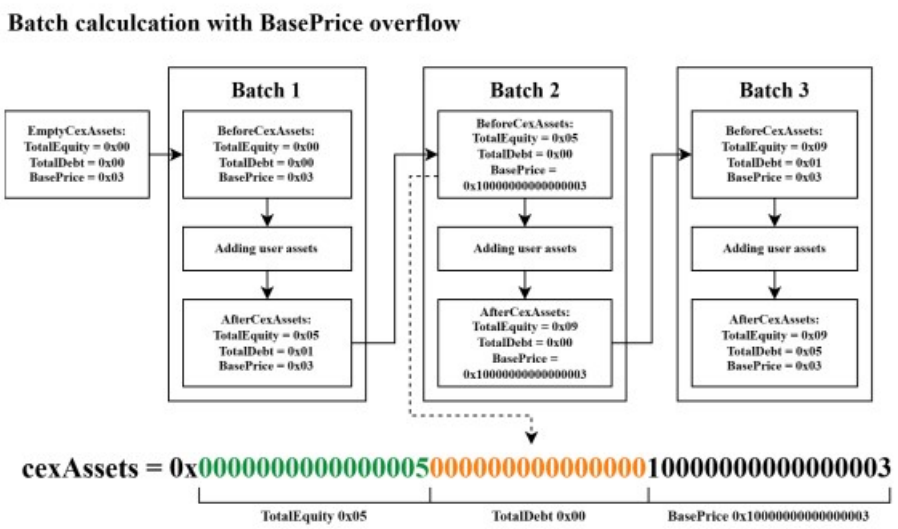
The lack of validation of *BasePrice* allows it to be modified between batches, by lowering the *TotalDebt* by 1, the *BasePrice* can be increased by 2^{64} and vice versa. Because of that, it is possible to generate almost unlimited debt. A user with 1 coin with *BaseValue* greater than 2^{64} (million of dollars) can have almost any debt, the assertion responsible for checking if users have lower debt than equity won't work correctly.

It is possible to generate the debt without anyone noticing it, it is possible by creating a batch of 864 fake users with huge debt but also with a single coin with modified *BaseValue*, which will cover the whole debt. The below diagrams demonstrate how the value of *BasePrice* can be modified in a single batch.

Correct batch calculation



Example of Audit Report for Binance PoS tech assessment—Continuation. This figure depicts a sample from a smart contract auditing report for Binance Proof-of-Stake.



Hacken team created a dedicated repository to prove the existence of this issue: https://github.com/hknio/zkmerkle-proof-of-solvency-debt-bug.

The issue with the fix proposal was reported to Binance Team which confirmed the issue and merged fix proposed by Hacken team: https://github.com/binance/zkmerkle-proof-of-solvency/pull/5.

3.2 [Medium][Fixed] TotalDebt value underflow caused by integer overflow

When *TotalEquity* and *TotalDebt* is calculated from user assets, it is possible that it becomes bigger than 2^{64}, an example case is when two users have both 2^{63} debt and equity, then the sum of their debt and equity will be equal to 2^{64}. The code responsible for the calculations:

```
for j := 0; j < len(userAssets); j++ {
        CheckValueInRange(api, userAssets[j].Debt)
        CheckValueInRange(api, userAssets[j].Equity)
        totalUserEquity = api.Add(totalUserEquity, api.Mul(userAssets[j].Equity, b.BeforeCexAssets[j].BasePrice))
        totalUserDebt = api.Add(totalUserDebt, api.Mul(userAssets[j].Debt, b.BeforeCexAssets[j].BasePrice))

        afterCexAssets[j].TotalEquity = api.Add(afterCexAssets[j].TotalEquity, userAssets[j].Equity)
        afterCexAssets[j].TotalDebt = api.Add(afterCexAssets[j].TotalDebt, userAssets[j].Debt)
}
```

Example of Audit Report for Binance PoS tech assessment—Continuation. This figure depicts a sample from a smart contract auditing report for Binance Proof-of-Stake.

When the value of *TotalEquity* or *TotalDebt* will become higher than 2^{64}, then the next part of code, responsible for calculating integer used by hash function (*tempAfterCexAssets)* will work incorrectly because of overflows:

```
for j := 0; j < len(tempAfterCexAssets); j++ {
        tempAfterCexAssets[j] = api.Add(api.Mul(afterCexAssets[j].TotalEquity, utils.Uint64MaxValueFrSquare),
                api.Mul(afterCexAssets[j].TotalDebt, utils.Uint64MaxValueFr), afterCexAssets[j].BasePrice)
}
```

When *TotalEquity* exceeds 2^{64} then the proof in the next batch will be incorrect, however when *TotalDebt* exceeds 2^{64}, then it will overflow into *TotalEquity*. For example, *TotalDebt* equal to exactly 2^{64} would be equivalent to *TotalEquity* equal 1 and *TotalDebt* equal 0. This allows to lower the value of *TotalDebt* in the similar way as it was done in the case of the first issue with *BasePrice*, however it would not be beneficial in any way so this issue is not critical.

We recommend adding additional *CheckValueInRange* for *TotalEquity* and *TotalDebt* when calculating *tempAfterCexAssets*.

The issue was addressed and fixed by Binance Team: https://github.com/binance/zkmerkle-proof-of-solvency/pull/6

3.3 [Low] Potential omission of users

The current system of verification lacks a mechanism to confirm the completeness of the provider's inclusion of their users in the Merkle Tree. It is uncertain whether the provider may have excluded some users, who they presume will either not perform a verification of the proof or whose objections, in the event that they do not receive a proof, will not be given due consideration.

In the current implementation, the prover knows which users do the verification process as they need to download the configuration files from their website. Simplifying the process of choosing which users should be included and which ones can be omitted.

While unlikely this would happen in practice, to address this issue, it is necessary a trusted third party, as they become more readily available to support crypto exchanges, must verify that all users were included in the Merkle Tree without any exclusions.

Example of Audit Report for Binance PoS tech assessment—Continuation. This figure depicts a sample from a smart contract auditing report for Binance Proof-of-Stake.

3.4 [Low] Merkle Root hash integrity

When users download the Merkle tree and each user config from the frontend, the Merkle root hash is included in the user_config.json file, but there is no way to check the integrity of this hash across all Binance users in order to be sure that this root hash wasn't tampered depending on the client IP or other parameters of the users.


```
{
  "AccountIndex": 9,
  "AccountIdHash": "0000041cb7323211d0b356c2fe6e79fdaf0c27d74b3bb1a4635942f9ae92145b",
  "Root": "29591ef3a9ed02605edd6ab14f5dd49e7dbe0d03e72a27383f929ef3efb7514f",
  "Assets": [{"Index":7,"Equity":123456000,"Debt":0}],
  "Proof": ["DrPpFsm4/5HntRTf8M3dbgpdrxq3Q8lZkB2ngysW2js=","G1WgD/CvmGApQgmIX0rE0BlSifkw6IfNwY
  "TotalEquity": 123456000,
  "TotalDebt": 0
}
```


To counteract this, the Merkle root should be signed by a trusted third-party auditor or be published on the blockchain as a public bulletin board, so users can easily verify the transaction's inclusion and the validity of the Merkle root hash they got from their user_config.json. It should be done in a single transaction, which will be easy to detect. It's also possible to address this issues by publishing the hash root in a social media that the proved doesn't control.

3.5 [Informational] Total amount of users inference

The user downloads a proof.csv file in the verification config containing the total amount of batches and their commitments. The current number of batches at the moment of this assessment is 49.789. If we multiply this by the number of users per batch (currently 864), we can infer that the total number of users is around 43.015.104, as one leaf is equal to one user in the current implementation. Still, this amount can also include a number of empty leaves, so it's only an approximation.
Randomizing the number of empty leaves in bigger numbers can solve this issue.

Appendix A2 — DeFi Category and Blockchain

Category

The vector *category* is based on the following 11 DeFi categories. *Algo-Stables* are protocols that manage algorithmic stablecoins; *CDP* are collateralized debt position platforms that enable users to lock collateral (e.g., crypto assets) to mint or borrow assets like stablecoins; *DEX* are decentralized exchanges that facilitate peer-to-peer trading of digital assets without intermediaries; *Lending* are platforms that allow users to lend or borrow cryptocurrencies; *Options* are protocols that enable the trading of crypto options; *Reserve Currency* are protocols that issue decentralized reserve assets intended to serve as stable or alternative currencies; *Services* are platforms that offer auxiliary services to other DeFi protocols, such as oracles, infrastructure, or analytics; *Staking* are protocols that support mechanisms that allow users to earn rewards by locking assets to secure networks or participate in governance; *Yield* are platforms that focus on generating passive income by optimizing returns on deposited assets through farming or staking strategies; *Yield Aggregators* are protocols that automate yield farming by reallocating funds across multiple platforms to maximize returns for users. *Other* are all other platforms.

Blockchain

The vector *blockchain* is based on the following 10 blockchain categories. *Avalanche* is a high-performance chain known for its fast transaction processing and scalability; *Binance Smart Chain* is a chain with low fees and high throughput on Binance; *Cronos* is a chain designed to bridge DeFi with the Cosmos ecosystem; *Ethereum* is the most widely used blockchain for DeFi; *Fantom* is a scalable blockchain platform focused on high-speed transactions and low costs; *Harmony* is designed to support decentralized applications and cross-chain finance; Polygon is a Layer 2 scaling solution for Ethereum; *Solana* is a high-performance blockchain that is widely used in DeFi and NFT markets; *Terra* is a blockchain focused on algorithmic stablecoins and DeFi solutions; *Other* are all other blockchains.

Appendix A3 — Audit Reports

Table A. Summary Statistics: Audit Reports This table reports characteristics of 8,195 audit reports submitted by 118 auditors between January 2020 and October 2023. We used a team of research assistants to analyze the audit reports and collect key information, including the number of vulnerabilities detected, the degree of severity of each vulnerability, and the resolution status of each vulnerability. *Centralized Auditors* includes all auditing firms, such as Certik, Haken, and Peckshield, contracted to conduct smart contract audit. See the full list of centralized auditors in Appendix E Table E. *Decentralized Auditors (bounty hunters)* are stand-alone self-appointed auditors who attempt to find protocol vulnerabilities in return for promised rewards ("bounties") paid by the protocols. *Pages* is mean number of pages in an audit report. *Critical* (*Major*, *Total*) is the mean proportion of vulnerabilities that are tagged as having critical (major, any) severity. *Resolved* is the percentage of vulnerabilities resolved by the protocol team prior to the final version of the report.

Audit Reports Characteristics						
	Reports		*Vulnerabilities Detected*			
Auditor	*#*	*Pages*	*Total*	*Critical*	*Major*	*Resolved*
	(I)	(II)	(III)	(IV)	(V)	(VI)
Centralized Auditors:						
Full Sample	8,060	15.14	6.64	7%	41%	44%
Decentralized Auditors:						
Bounty Hunters	135	-	18.43	-	87%	79%

Appendix B — Matching Samples

Table B. Construction of matched sample. This table reports the summary statistics of matched sample used in the analyses of the Terra-Luna and FTX exogenous shocks. We employ propensity score matching (PSM) based on the nearest neighborhood. For each of the 444 audited protocols, we match one non-audited protocol. The table reports the mean values for the characteristics of audited protocols, matched non-audited protocols, and their mean differences. The last column (*Percentage Improvement*) reports the percentage improvement of the matching procedure, defined as one minus the ratio of the absolute distance between mean characteristic of audited protocols and mean characteristic of matched non-audited protocols to the absolute distance between mean characteristic of audited protocols and mean characteristic of all (not necessarily matched) non-audited protocols.

Panel A: Matching Outcomes for Luna Crash

	Audited	**Non-Audited**	**Mean Diff**	**Perc. Improv.**
Staking ($M)	9.32	9.17	0.15	32.99%
FDV ($M)	39.22	37.74	1.48	94.02%
Raised ($M)	0.27	0.24	0.03	72.35%
Oracle	0.18	0.17	0.01	39.80%
Open Source	0.09	0.07	0.02	25.21%
Overall Distance	0.37	0.34	0.03	57.66%

Panel B: Matching Outcomes for FTX Collapse

	Audited	**Non-Audited**	**Mean Diff**	**Perc. Improv.**
Staking ($M)	8.26	8.03	0.23	72.18%
FDV ($M)	23.77	18.98	4.79	91.83%
Raised ($M)	0.27	0.25	0.02	69.50%
Oracle	0.21	0.19	0.02	57.09%
Open Source	0.10	0.09	0.01	44.24%
Overall Distance	0.41	0.36	0.05	69.35%

Appendix C — Selection Model

Table C. Selection Model. This table reports coefficient estimates for the first stage Heckman selection model reported in table 3. We employ Heckman correction for selection (e.g., Heckman, 1979, 1990) for the 902 DeFi protocols that decided to undergo auditing. The parameters used in the selection model are the same as in Table 3 and are described in Table 1.

Seclection Model: 1st Stage Heckman				
Parameter	**Estimate**	**Std. Error**	**t-value**	**Pr(>|t|)**
log(ETH Mcap)	−0.356	0.0693	−5.14	0.0000
EVM	0.452	0.080	5.69	0.0000
DEX	0.361	0.083	4.35	0.0000
Yield	0.476	0.090	5.27	0.0000
Lending	0.816	0.133	6.13	0.0000
Raised	0.178	0.072	2.47	0.0137
Oracle	0.364	0.081	4.50	0.0000
Open Source	1.520	0.487	3.12	0.0018
Full Sample	1,575			
Selected Sample	902			

Appendix D — Security Breaches

Table D. List of Security Breaches. This table reports the number of security breach events and the total amount lost to hackers in each year. Data retrieved from https://defillama.com/hacks.

Year	Amount lost (in millions)	Number of Attacks
2016	60.00	1
2017	157.70	2
2018	235.00	1
2020	183.75	16
2021	2,290.16	66
2022	3,280.77	59
2023	1,396.04	41
Total	7,603.42	186.00

Appendix E — Auditing Firms Dataset

Table E: This table lists all known auditors. *Auditor* is the name of the auditing firm. *Protocols* is the number of audited protocols per auditing firm. *Launched* is the number of audited protocols that succeeded in deploying their smart contracts and attracting at least $1M in *TVL* in the first week of going live *Auditor Launch Rate* is the proportion of protocols launched within six months of an audit to the total number of audited protocols by a given auditor.

Auditor	Protocols	Launched	Launch Rate	Auditor	Protocols	Launched	Launch Rate	Auditor	Protocols	Launched	Launch Rate
PeckShield	149	112	75.17%	BlockSec	8	1	12.50%	RED4SEC	7	0	0.00%
SlowMist	58	42	72.41%	Chainsulting	56	6	10.71%	BlockchainConsilium	6	0	0.00%
iosiro	10	7	70.00%	Solidified	180	19	10.56%	Somish	6	0	0.00%
DeFiSafety	88	60	68.18%	Tech Rate	706	74	10.48%	Anchain	5	0	0.00%
Quantstamp	58	35	60.34%	OXORIO	11	1	9.09%	BramahSystems	5	0	0.00%
Dedaub	18	10	55.56%	HashEx	107	9	8.41%	xGuard	5	0	0.00%
Certora	20	11	55.00%	Novos	26	2	7.69%	NCCGroup	4	0	0.00%
Certik	552	287	51.99%	Solidproof	217	14	6.45%	SCV	3	0	0.00%
Secbit	2	1	50.00%	RD AUDITORS	183	11	6.01%	ApeAudits	2	0	0.00%
Theori	2	1	50.00%	InterFi	109	6	5.50%	ChainsGuard	2	0	0.00%
Inspex	17	8	47.06%	Callisto	63	3	4.76%	SmartDec	2	0	0.00%
De.Fi(DEFIYIELD)	69	32	46.38%	Ether Authority	242	8	3.31%	TakaSecurity	2	0	0.00%
Trail of Bits	98	42	42.86%	QuillAudits	399	11	2.76%	ZKLabs	2	0	0.00%
Cure53	5	2	40.00%	Dessert Finance	115	3	2.61%	Arachnid	1	0	0.00%
CONSENSYS	51	20	39.22%	Contract Wolf	317	8	2.52%	Blockstream	1	0	0.00%
Obelisk	29	11	37.93%	Soken	165	2	1.21%	BTBLOCK	1	0	0.00%
Zokyo	40	15	37.50%	Tech Audit	186	2	1.08%	CintaInfinita	1	0	0.00%
OpenZeppelin	62	22	35.48%	Verichains	175	0	0.00%	CrypticLabs	1	0	0.00%
Oak Security	17	6	35.29%	ImmuneBytes	119	0	0.00%	CyberUnit.Tech	1	0	0.00%
RUNTIME	42	14	33.33%	CTDSec	74	0	0.00%	Dapp.org	1	0	0.00%
KUDELSKI	30	10	33.33%	BlockSAFU	53	0	0.00%	GOGROUP	1	0	0.00%
Arcadia	21	7	33.33%	eNebula	34	0	0.00%	HECO	1	0	0.00%
CryptoManiacs	3	1	33.33%	Coinspect	33	0	0.00%	IgorGulamov	1	0	0.00%
Paladin	189	61	32.28%	ShellBoxes	27	0	0.00%	Midgard	1	0	0.00%
CODE4RENA	137	44	32.12%	SafuAudit	21	0	0.00%	OWN AUDIT	1	0	0.00%
Halborn	102	32	31.37%	CoinBae	19	0	0.00%	PlatON	1	0	0.00%
ChainSecurity	24	7	29.17%	Knownsec	17	0	0.00%	ProvideTechnologies	1	0	0.00%
Beosin	45	13	28.89%	Coinscope	14	0	0.00%	RootB	1	0	0.00%
SigmaPrime	14	4	28.57%	Noneage	13	0	0.00%	RugBusters	1	0	0.00%
Pessimistic	82	19	23.17%	SolidGroup	13	0	0.00%	SaferICO	1	0	0.00%
Haechi	96	22	22.92%	Tech Audit USA	13	0	0.00%	SCATDAO	1	0	0.00%
Cryptonics	22	5	22.73%	Rugfreecoins	11	0	0.00%	ScottBigelow	1	0	0.00%
Hexens	15	3	20.00%	ViearrtheAuditor	11	0	0.00%	Sentnl	1	0	0.00%
MixBytes	101	19	18.81%	BlockChainLabs	10	0	0.00%	Sooho	1	0	0.00%
ABDK	92	16	17.39%	VitalBlock	10	0	0.00%	SpyWolf	1	0	0.00%
CoinFabrik	48	8	16.67%	FairyProof	7	0	0.00%	StaySAFU	1	0	0.00%
Armors	20	3	15.00%	Omniscia	7	0	0.00%	TEAM OMEGA	1	0	0.00%
Hacken	478	67	14.02%	RED4SEC	7	0	0.00%	TrustlookBlockchainlabs	1	0	0.00%
LeastAuthority	112	15	13.39%	Omniscia	7	0	0.00%	Zeropool	1	0	0.00%