NBER WORKING PAPER SERIES

DISTRIBUTED LEDGERS AND SECURE MULTI-PARTY COMPUTATION FOR FINANCIAL REPORTING AND AUDITING

Sean S. Cao
Lin William Cong
Baozhong Yang

Working Paper 32763
http://www.nber.org/papers/w32763

NATIONAL BUREAU OF ECONOMIC RESEARCH
1050 Massachusetts Avenue
Cambridge, MA 02138
August 2024

The authors thank the Editor, an anonymous Associate Editor, several anonymous referees, Alex Chinco, Pingyang Gao, Jiasun Li (Discussant), Bob McDonald (Discussant), Venky Nagar (Discussant), Fahad Saleh (Discussant), Haresh Sapra, Gerry Tsoukalas, and Larry Wall (Discussant) for detailed feedback and discussion. They also thank Vikas Agarwal, Kwan Chen, Mark Chen, Alisa DiCaprio, Matthew DeAngelis, John Hameling, Dalida Kadyrzhanova, Yongtae Kim, W. Robert Knechel, Anya Kleymenova, Clive Lennox, Pierre Liang, Roni Michaely, James ("Robbie") Moon, Jr., Curtis Mullis, Mark Peecher, Lin Peng, Shivaram Rajgopal, Ajay Subramanian, Lawrence J. White, Baohua Xin, Mao Ye, Shuhuai Zhang, Hongda Zhong, and participants at NBER Conference on Blockchains, Distributed Ledgers, and Financial Contracting, SFS Cavalcade Conference at Carnegie Mellon University, PCAOB/JAR Conference on Auditing and Capital Markets, Federal Reserve Bank of Atlanta Conference on New Technologies and Financial Stability, Ant Financial Workshop, Baidu Du Xiaoman Financial, Blackrock, DataYes & ACM KDD China FinTech×AI Workshop, Eastern Finance Association Meeting, Geneva Finance Research Institute, Georgia State University Workshops at the Departments of Accountancy, Computer Science and Finance, JD.com JDD (Financial Arm), and University of Minnesota for constructive comments. The authors gratefully acknowledge research support from the FinTech Lab at J. Mack Robinson College of Business at Georgia State University, the Center for Research in Security Prices at the University of Chicago, the Ripple University Blockchain Research Initiative (UBRI), and the Smith AI Initiative for Capital Market Research at the University of Maryland. The views expressed herein are those of the authors and do not necessarily reflect the views of the National Bureau of Economic Research.

NBER working papers are circulated for discussion and comment purposes. They have not been peer-reviewed or been subject to the review by the NBER Board of Directors that accompanies official NBER publications.

© 2024 by Sean S. Cao, Lin William Cong, and Baozhong Yang. All rights reserved. Short sections of text, not to exceed two paragraphs, may be quoted without explicit permission provided that full credit, including © notice, is given to the source.

Distributed Ledgers and Secure Multi-Party Computation for Financial Reporting and Auditing
Sean S. Cao, Lin William Cong, and Baozhong Yang
NBER Working Paper No. 32763
August 2024
JEL No. D21,D40,G32,G34,M42,M48

ABSTRACT

To understand the disruption and implications of distributed ledger technologies for financial reporting and auditing, we analyze firm misreporting, auditor monitoring and competition, and regulatory policy in a unified model. A federated blockchain for financial reporting and auditing can improve verification efficiency not only for transactions in private databases, but also for cross-chain verifications through privacy-preserving computation protocols. Despite the potential benefit of blockchains, private incentives for firms and first-mover advantages for auditors can create inefficient under-adoption or partial adoption that favors larger auditors. Although a regulator can help coordinate the adoption of technology, endogenous choice of transaction partners by firms can still lead to adoption failure. Our model also provides an initial framework for further studies of the costs and implications of the use of distributed ledgers and secure multi-party computation in financial reporting, including the positive spillover to discretionary auditing and who should bear the cost of adoption.

Sean S. Cao
University of Maryland
scao824@umd.edu

Lin William Cong
SC Johnson College of Business
Cornell University
Sage Hall
Ithaca, NY 14853
and NBER
will.cong@cornell.edu

Baozhong Yang
J. Mack Robinson College of Business
35 Broad Street, Suite 1243
Atlanta, GA 30303
bzyang@gsu.edu

An online appendix is available at http://www.nber.org/data-appendix/w32763

1. Introduction

Unbiased financial reporting is crucial in financial markets and regulatory agencies have constantly sought ways to improve reporting integrity. Because firms can potentially misreport, one main cost in ensuring quality reporting comes from auditors' verification of clients' transactions. Auditing firms traditionally operate separately because it is not customary to share proprietary information among auditors. It is challenging to find a trusted third party to facilitate timely and secure communications, not to mention clients' reluctance to reveal information to other auditors and legal issues concerning data privacy. In practice, auditors contact transaction counterparties for verification either manually or through a third party with potential agency frictions. The labor-intensive and mechanical nature of cross-firm verification leads to insufficient auditing effort and, consequently, errors and manipulations.[1]

Meanwhile, decentralized ledger/database technology has grabbed the world's attention, with the potential to allow industry-wide collaboration and disrupt corporate governance, industrial organization, payments, and entrepreneurial finance.[2] Among the various advances, "one theoretical application of blockchain is in financial reporting, and this is exactly the point in time to discuss advantages and disadvantages" (Harvey, 2016; FEI, 2018). Both the media and industry leaders are also increasingly paying attention to blockchain applications in financial reporting and auditing. For example, all Big 4 audit firms—Deloitte, Ernst & Young (EY), KPMG, and PwC—have devoted significant resources to establishing research labs and providing blockchain services (e.g., Bajpai, 2017; Vetter, 2018). However, questions remain concerning how blockchains should be designed for financial reporting and auditing to foster information sharing while preserving privacy as well as how they alter clients', auditors', and regulators' incentives and reshape auditor competition.

We take an initial step towards understanding these issues by examining how permis-

[1]For example, Luckin Coffee Inc. was found in 2020 to have fabricated transactions representing 150 to 310 million U.S. dollar worth of revenue over multiple years. The scandal crashed Luckin's prices, leading to its delisting from Nasdaq and huge costs for investors. See "Behind the Fall of China's Luckin Coffee: a Network of Fake Buyers and a Fictitious Employee," *Wall Stree Journal*, Jing Yang, May 28, 2020.

[2]See, for example, Yermack (2017) and Cong and He (2019) for discussions. Several consortiums, including Hyperledger, R3, and Ethereum Enterprise Alliance have accelerated the collaboration on blockchain development and deployment among various industries.

sioned blockchains disrupt traditional financial reporting and auditing processes and enable collaboration without sacrificing client data privacy.[3] In particular, we analyze two important aspects of financial reporting: firms' endogenous misstatements and auditors' monitoring/inspection of financial reports. To this end, we consider a collaborative, automated reporting and auditing process that capitalizes on distributed ledger and secure multi-party computation (MPC) technologies. We characterize the equilibrium outcomes allowing firms' endogenous misstatements, auditor heterogeneity and competition, blockchain adoption, and regulatory policy in a unified framework. We recognize the potential costs of blockchain and show how private incentives for firms and first-mover advantages for auditors can create inefficient under-adoption or partial adoption that favors larger auditors. This highlights the role of the regulator to coordinate and facilitate full adoption. Furthermore, our model provides a framework that can facilitate further research into the costs and implications of blockchain adoption. For example, we find that firms' endogenous choice of transaction partners can also lead to adoption failure. We also show that more efficient adoption equilibria would arise if auditors bear the costs of blockchain, at least initially.

Thanks to blockchain's peer-to-peer design (within a consortium), collaboration among auditors would not require a centralized third party to monitor or intermediate. Encryption methods such as secure MPC allow information providers in a federated blockchain system to safeguard proprietary client information while also verifying transactions.[4] Furthermore, the immutable nature of blockchain enables regulators to inspect auditing processes and prevent

[3] Auditing differs from other industries affected by blockchain technology, such as digital payments or trade finance. In particular, the popular open blockchains are not suitable in settings where client information needs to stay private. Companies such as IBM, R3, and Springlab have explored permissioned blockchains in general collaboration contexts. However, what is left out of the discussion is a design of permissioned blockchains specific to the information-sharing task for financial reporting and auditing. Even if both transacting parties use the same auditor, retrieving the records without a global ID costs effort without a blockchain. But if both parties are members of a blockchain system that the auditor has access to and the transaction is recorded in a standardized format onto the blockchain, the validation can be automated. We are not claiming that blockchains eliminate misreporting automatically, a point we elaborate further in Section 2.2. They reduce misreporting because inconsistencies among the reports from various transaction parties can be detected easily and in a more timely fashion, and retrospective manipulations and misreporting can be prevented.

[4] Utilizing private data while preserving data privacy is not a figment of technological imagination, but is already taking place in practice. One example is OpalProject.org, led by the MIT Media Lab and the World Economic Forum. Accounting and consultancy firm Ernst & Young (EY) has also developed blockchain solutions for private business transactions that are advertised as "the Internet of transactions" (Mearian, 2018). See Appendix A for further discussion of the privacy-preserving algorithms.

audit firms or hackers from revising recorded transaction data ex-post. Overall, encrypted federated blockchains can enable collaborative auditing and make the auditing process more efficient and reliable for detecting fraud. That said, adopting a blockchain system entails indirect costs of potentially losing clients who prefer less stringent auditing, as well as direct costs of set-up and standardization.

We take the aforementioned blockchain functionalities and adoption costs as given and examine how public corporations and auditing companies respond to the technology. Specifically, our model features a continuum of corporate clients and two heterogeneous auditors. Without blockchains, auditors compete for client firms through fees and service quality. Once a firm is matched with an auditor, the firm endogenously chooses the level of misstatement to trade off the private misreporting benefit and the cost of being detected by regulators or the market, whereas the auditor determines the monitoring intensity (represented by the audit sampling probability) to minimize auditing costs and the expected penalty when its clients' misreporting is detected. In the competitive equilibrium, auditors derive endogenous market shares or sizes from their heterogeneous skills, and larger client firms with larger transaction volumes pose a greater risk of misreporting and incur higher auditing fees.

When an auditor adopts a blockchain system, the auditing costs of transactions among clients within the auditor are significantly reduced. However, auditing transactions across auditors remains costly if other auditors do not adopt blockchain systems or the systems are all independent. With a federated blockchain, however, two auditors who have their clients' transaction information and are both using blockchains can verify transactions with little cost, thanks to the encrypted verification algorithm.

The auditors' technology adoption yields a first-mover advantage, i.e., if one auditor adopts the blockchain, the other auditor may find it unprofitable to do so. Such partial adoption equilibria can arise due to the unique competition among the auditors. The auditor first adopting blockchain can offer a lower auditing fee and attract more clients, thus increasing profits. In contrast, when the second auditor weighs the adoption decision, the competition with the first auditor renders the potential increased profits lower. Thus the second auditor is less likely to adopt blockchain than the first auditor, other things equal.

Given the fixed costs of blockchain adoption, a larger auditor is more likely to be the first mover as blockchain can further increase its market share by entrenching its position.[5]

If blockchain adoption costs are sufficiently small, both auditors may choose to adopt the blockchain and a full-adoption equilibrium arises. In such cases, the larger auditor typically loses market share to the smaller auditor because blockchain universally reduces auditing costs, further leveling the playing field. We note that in the full-adoption equilibria, social welfare (the reduction in misstatements minus deadweight auditing costs) improves, but auditors' profits fail to increase due to competition. Therefore, despite potential social benefits, full adoption of blockchain technology may not materialize, especially when blockchain technology is still nascent and relatively costly to implement.

Given the existence of socially inefficient partial-adoption or no-adoption equilibria, regulators may coordinate an industry-wide adoption by mandating adoption or subsidizing initial costs for small auditors, which could reduce equilibrium misstatements and expenses associated with auditing and regulation. However, if client firms can endogenously select their transaction partners, high incentives for misstatement can lead them to transact exclusively with private, off-chain partners, causing the full-adoption equilibrium to break down. Therefore, regulatory policies need to carefully consider both firms' and auditors' incentives.

Although we have focused on the audit of transaction-based accounts, the reduction in auditing costs with the new technology may have a *spillover effect* on discretionary accounts where both soft information and auditors' expertise play an indispensable role. In a model extension, we show that the adoption of distributed ledger technology enables auditors to reallocate efforts from monetary transactions to focus more on discretionary accounts, which has been the most challenging for audit firms. Consequently, technology has the potential to disrupt the audit labor market by offsetting a reduction in demand for mechanical audit work with an increased need for skilled auditors.

We model federated blockchains with secure MPC as a leading candidate for effectively improving privacy protection and cross-party verification in a decentralized system. But the economic insights apply more broadly to distributed ledger systems. While previous studies

[5]We note that in other industries, market leaders such as Walmart and Maersk are leading the blockchain development while other competitors are more reluctant to join the game.

have examined the implications of a general technology on cost reduction (e.g., Katz and Shapiro, 1986; Lerner and Tirole, 2014), our model entails a price and market share competition together with technology adoption decisions, which are new and enrich the interactions among auditors. Moreover, we are the first to highlight how coordination and competition issues manifest in auditors' adoption of blockchain technology, which has important practical implications. Our proposed permissioned blockchain framework not only allows firms to enjoy the benefits of decentralization and security via encryption and immutability but also is practically implementable. Thus, our model is related to recent industry developments.[6]

The paper proceeds as follows. Section 2 provides a review of the literature and institutional background. Section 3 sets up the model and discusses key implications. Section 4 considers various extensions of the model. Section 5 offers concluding remarks.

2. Literature and Institutional Background

2.1. Related Literature

Our paper contributes to the emerging literature on FinTech and blockchain. Earlier studies (e.g., Cong, He, and Li, 2021; Easley, O'Hara, and Basu, 2019; Hinzen, John, and Saleh, 2022) focus on public blockchains. Vis-à-vis blockchain applications, studies such as Tsoukalas and Falk (2020), Cong, Li, and Wang (2021), Chod and Lyandres (2021), and Halaburda,

[6]Alisa Dicaprio from R3 informed us at an NBER meeting that R3 has developed ready-to-use permissioned blockchain infrastructure that can integrate with clients' ERP systems with reasonable adoption cost. Cao et al. (2020) show that the system proposed in the current paper can be implemented using standard computing hardware, with a transaction speed of 0.012 seconds per transaction. Cohn (2016) reports that large accounting firms have investigated the use of blockchains and a "triple-entry accounting" system. KPMG partnered with IBM to explore automating and streamlining audit processes (e.g., Smith, 2018); Deloitte (2016) describes how a blockchain-based accounting system works. In practice, auditors can either develop new technologies to audit clients' blockchains or develop their own permissioned blockchains to help their audit process (e.g., Tysiac, 2018). Recent efforts of accounting firms focus on building in-house blockchain capabilities and services (e.g., CNN, 2018), Tencent's standardizing e-invoices (Pymnts, 2019), E&Y's developing Ethereum privacy-preserving protocol (E&Y, 2020), and AntChain's interoperability solutions and privacy-preserving multi-party computing platform (Businesswire, 2023). Our model captures core features of these applications, e.g., auditors being mainly responsible for the development and initiation costs of blockchains, and the need for private-preserving transaction reporting and auditing on permissioned blockchains. To date, the auditing industry has not widely adopted blockchain technologies, likely due to the high adoption costs and coordination challenges emphasized in our model. Our study informs regulators of policies that facilitate blockchain adoption and improve social welfare going forward.

Sarvary, and Haeringer (2022) examine the roles of tokens in platform adoption, financing, and information sourcing.

Treating blockchains as a data infrastructure, Chod et al. (2020) demonstrate that the verifiability of transactions afforded by blockchains can enhance firm operating transparency and thereby finance operations more efficiently. Dai and Vasarhelyi (2017) present an early discussion on blockchain-based accounting. Several studies examine the benefits of (prospective) blockchain adoption to firms and supply chains (e.g., Chen et al., 2023; Cui, Hu, and Liu, 2023; Iyengar et al., 2022a,b; Ma, Xia, and Yang, 2022). We are the first to study the economics of secure MPC built on permissioned blockchains. More recently, Townsend (2020), Chinco (2022), and Hastings, Falk, and Tsoukalas (2022) all recognize and highlight the importance of secure MPC and the potential of blockchains as a database and infrastructure for its implementation.

We are also one of the earliest papers studying blockchain applications in accounting and financial reporting. This growing literature now includes, for example, Amiram, Jørgensen, and Rabetti (2022), Luo and Yu (2022), and Cong et al. (2023). We differ from earlier studies in our focus on permissioned blockchains and in jointly analyzing the auditor competition and adoption games.[7] Doing so highlights for the first time in the literature that even without free entry as seen in public blockchains or the introduction of cryptocurrencies/tokens, permissioned blockchains can create economic impacts that economists hitherto often dismissed. We also provide empirical predictions that future studies can test once the technology sees wider adoption and data become available.

Finally, our study adds to the theoretical literature in auditing. Prior studies have considered issues related to auditors' strategic behavior and risk, including optimal auditing sample size (Scott, 1973), auditor conservatism (Antle and Nalebuff, 1991), strategic testing (Fellingham and Newman, 1985; Patterson, 1993), earnings reports and auditing (Newman, Patterson, and Smith, 2001), financial reporting and audit committees (Caskey, Nagar, and Petacchi, 2010), and joint auditing and quality (Deng et al., 2014). Several theoretical studies

[7]Studies such as Wang and Kogan (2018) point out the possibility of using blockchain and encryption algorithms to process transactions on blockchains while preserving confidentiality. Their proposals either feature independent blockchain/database or exogenously require all firms to adopt blockchain and convert corporate assets into cryptoassets.

focus on issues related to auditing fees and quality, such as lowballing in initial auditing fees, auditor independence, auditor competition, and market reactions (e.g., Simunic, 1980; DeAngelo, 1981; Teoh, 1992; Lu, 2006). We contribute by highlighting how decentralized ledger technologies disrupt the competition, pricing, and labor market in auditing.

2.2. Institutional Background

We describe the basic auditing process of transaction-based (simple revenue and transaction records) and non-discretionary accounts before explaining how a federated blockchain can facilitate collaborative auditing against the backdrop of privacy concerns. Along the way, we provide a primer on the use of permissioned blockchains and secure MPC for privacy preservation.

Figure 1 illustrates a typical client firm's income statement.[8] Auditors' primary job is to verify the accuracy of net income and prevent the occurrence of restatements. To this end, auditors need to verify their clients' sales and expenses, which may be overstated and understated, respectively, to gain favorable valuation or lower financing costs (Strobl, 2013). Auditors often verify the accuracy of sales and, in our case, accounts receivable and related invoices. To do this, they use historical patterns of accounts receivable, industry peer firms' concurrent accounts receivable, or growth patterns of other highly related asset growth such as inventory to estimate errors. A common limitation of these approaches is that all information must be sourced from clients who may have incentives to misreport.

One way to mitigate potential misreporting is to verify clients' information by confirming with their transaction partners. For example, if a seller claims $1M accounts receivable sales, it boosts auditors' confidence in the number if the buyer can verify $1M in accounts payable purchases. Intuitively, the buyer has little incentive to collude with the seller because when the buyer overstates the purchase for the sellers' overstated sales, it implies a lower net income for the buyer (i.e., higher cost of goods sold). The collusion cost for buyers implies that the information that buyers provide to verify sellers' transactions can be more reliable than the information that sellers provide themselves. However, such cross-party information

[8]For simplicity, we focus on transaction-based accounts and do not include easily verifiable cash receipts.

verification is costly in the traditional auditing system. In those cases, an auditor has to contact the transaction counterparty directly to request records and manually verify the information or outsource such labor-intensive cross-party verification to a third party, such as confirmation.com, at significant expense.

Income Statement	
Sales	$= \sum$ Accounts Receivable from transactions with different business partners
Expenses	$= \sum$ Accounts Payable from transactions with different business partners
Net Income	$= \sum$ Accounts Receivable from transactions with different business partners $-$ $\sum$ Accounts Payable from transactions with different business partners

Figure 1: **Income Statement of a Client Firm**

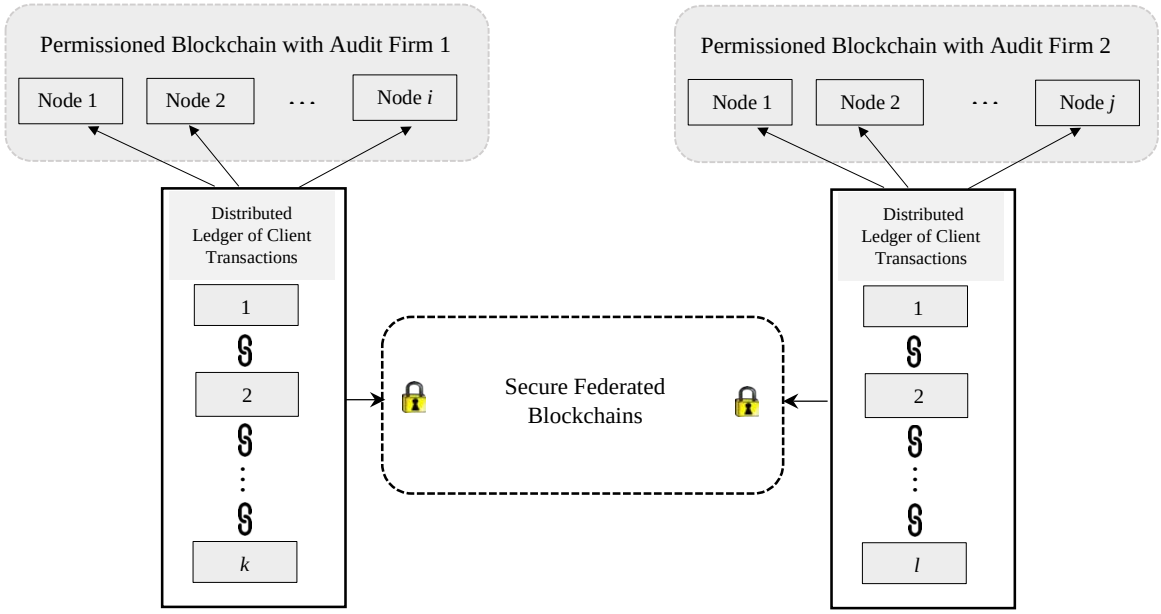

Figure 2: **Structure of the Federated Blockchain**

Figure 2 demonstrates how a federated blockchain with an encryption protocol has the potential to facilitate collaborative auditing and cross-party verification.[9] In a federated blockchain, each auditor operates a permissioned blockchain for clients or has access to

[9] Appendix A contains more details of encryption algorithms, secure MPC, etc.

the blockchain ecosystem of its clients. In a baseline scenario, each node on the permissioned blockchain is administered by a team of the auditing firm.[10] Each client transaction is assigned a unique global ID to facilitate cross-party information verification. Transactions among clients of the same auditor are verified by the auditing teams working with the clients and recorded on the permissioned blockchain. In permissioned blockchains, only permissioned nodes can manage records, and the nodes usually adopt a majority consensus that is efficient and scalable. Consequently, the costly mining process associated with public blockchains that have proof-of-work protocols is avoided. Transactions between parties associated with different auditors, i.e., *cross-auditor* transactions, utilize a cryptographic verification method (e.g., secure MPC or zero-knowledge proof, ZKP) that enables confirmation on the federated blockchain while maintaining the integrity of proprietary information.

For the implementation of the verification process, we first note that transactions between firms on the same auditor's blockchain are automatically verified as on a standard blockchain system and can be done efficiently (e.g., with scalable blockchain solutions such as Cosmos SDK and OP Stack). Next, we illustrate the transaction verification process on the federated blockchain in Figure 3. As shown in Figure 3, for a transaction between two client firms audited by different auditors, the verification occurs on the federated blockchain. The first auditor posts an encrypted record to the blockchain that can only be validated by the second auditor, who works with the counterparty of the transaction. When both the record and validation are encrypted without revealing client-specific information, no other auditors or outsiders can retrieve transaction information from them. This verification process can be automated to make cross-party information verification more efficient because an auditor does not have to manually contact the transaction counter-party to request records and verify the information. After verification, the transaction will be recorded as verified on both auditor's blockchains and no longer needs to be verified again in the future. The secure validation process can be implemented by MPC or ZKP (see detailed discussions in Appendix

[10]We note that permissioned blockchains considered for business applications typically only allow permissioned parties to join, use an efficient consensus mechanism such as majority voting, and may not need an intrinsic cryptocurrency/token, which differs from public/permissionless blockchains like Bitcoin or Ethereum. These features of permissioned blockchains offer more privacy, energy efficiency, and scalability, albeit not being fully decentralized.

A) and there are a number of scalable blockchain solutions that implement such processes.[11]

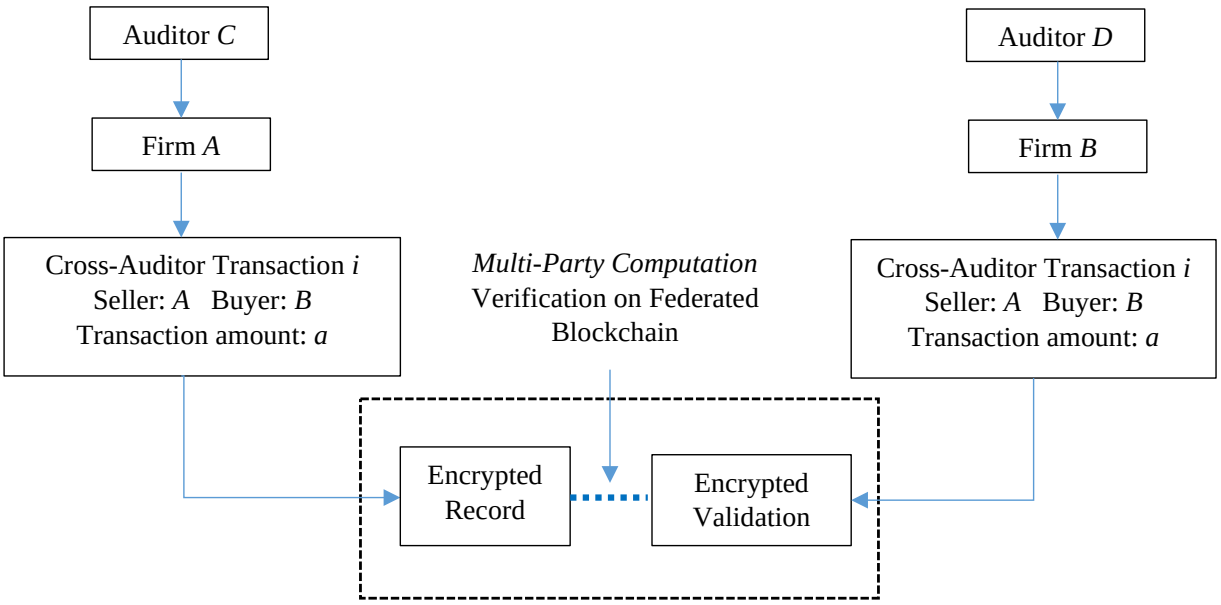

Figure 3: **MPC Transaction Verification on a Federated Blockchain**

These federated blockchain frameworks can facilitate two types of collaborative auditing, as demonstrated in Figure 4. Type 1 concerns within-auditor transactions, that is, when the two parties in the transaction are audited by the same auditing firm but by different auditing teams. However, auditor teams may be located remotely in different audit offices, leading to high communication costs. A permissioned blockchain connecting the audit teams can automate the verification process. Type 2 entails collaborative auditing across firms, which could not happen without the federated blockchain system. In this case, the two parties in the transaction are audited by different auditors, each residing in a separate blockchain ecosystem. The federated blockchain with encryption can facilitate automatic information sharing between auditors considering the privacy of clients' information. If a discrepancy is detected during the secure verification process, the auditors can reach out to the clients for the original records or contact the counterparties of the clients for authorization

[11] Zcash, zksync, Qedit, Espresso Systems, Cybernetica, among others, provide privacy-preserving blockchain systems that can implement ZKP or MPC efficiently. See also Cao et al. (2020) for an implementation with 0.012 seconds per transaction for encryption and 0.001 seconds for verification. Appendix A also provides more discussions on the implementation.

of verification. We note that once the blockchain is in place, discrepancies are automatically detected, so firms will not have incentives to misreport on the blockchain.

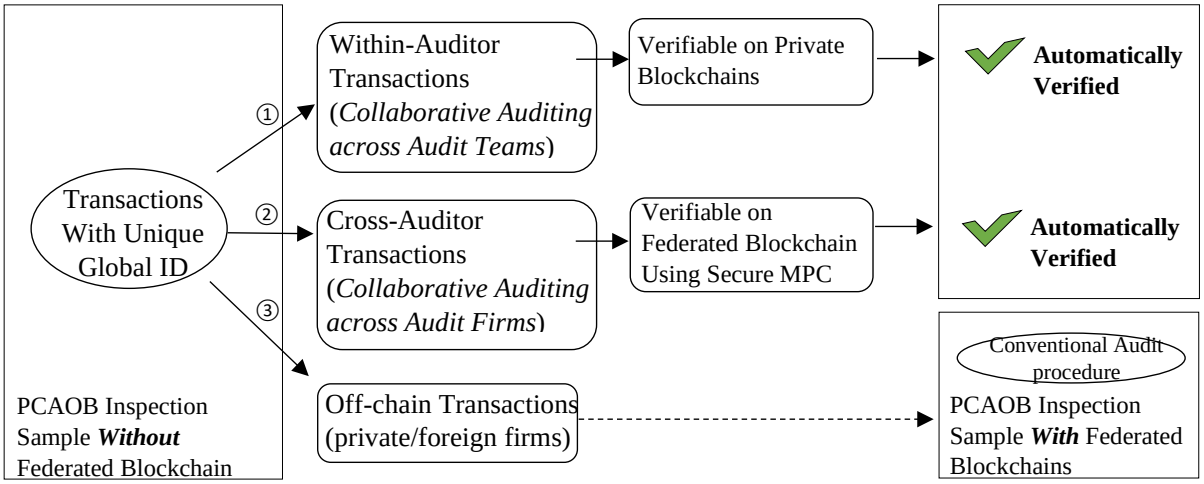

Figure 4: **Auditing Transactions with a Federated Blockchain**

An additional case involves *off-chain* transactions in which a client's transaction counterparty is not on the blockchain, such as an unaudited private or foreign firm. Even with blockchains, auditors still need to conduct conventional auditing procedures for off-chain transactions. However, these typically constitute only a small portion of the sample.

Overall, three technological features of blockchain are conducive to the auditing process: (i) decentralization—the peer-to-peer design of blockchain eliminates the requirement of a trusted central third party; (ii) encryption—secure computation methods allow sensitive communications to preserve data privacy and integrity; and (iii) immutability—once information is requested through the federated blockchain, it is difficult for any auditors or outside hackers to intentionally revise or delete the information, unless they can simultaneously tamper with a majority of nodes on the federated blockchain. In Section 3, we analyze the implications of this federated blockchain for auditors, clients, and regulators. We also note here that the collaborative auditing system built with the permissioned blockchain technology is not fully decentralized since the governance is determined by authorized parties (the auditors). It is, however, still more decentralized than a traditional centralized system.

We should clarify that even though we refer to the blockchain system that transaction

parties associate with as the auditor's blockchain system, it should be broadly interpreted as an ecosystem in which a transaction can be easily verified and recorded on a blockchain. It does not necessarily belong to a particular auditor—it could have been developed by the transaction parties themselves or an independent third party. A client firm may set up or join a blockchain system, which also facilitates internal audits and better data management. What is relevant for our discussion is whether an auditor has access to transaction details on the blockchain. One alternative would be that blockchain systems support transactions directly, rather than being add-on systems that require an interface to existing transactions and reporting databases. However, building and maintaining such infrastructure could be exorbitant for individual firms (Wang and Kogan, 2018), and would require the simultaneous adoption of the blockchain system by all transaction counterparties.

We remark that our reference to blockchains should really be interpreted as referring to distributed ledger technology (DLT) in general. Encrypted bilateral communication between auditors and clients also has the potential to resolve privacy concerns. In the setting of auditing, a system that allows the following features should suffice: automation of verification; immutability and auditable trails of data; privacy of data; mechanisms to monitor abnormal behavior of auditors, resolve conflict, and reach consensus. Blockchain is a salient solution candidate, albeit not the only one.[12] Our proposed blockchain solution has also been shown to be feasible; for example, Cao et al. (2020) demonstrate a detailed implementation of the proposed solution for the auditing industry, which is efficient and scalable. Chinco (2022) and Hastings, Falk, and Tsoukalas (2022) also recognize and highlight the importance and potential of blockchains in secure MPC. R3, Opal project, Springlab, Qedit, Espresso Systems, Cybernetica, and others have also introduced blockchains with secure computing capabilities via ZKP and MPC. Several open-source projects, including Cosmos SDK, OP Stack, Avalanche, Arbitrum, and zkSync also allow flexible, scalable implementations of permissioned blockchains that are interoperable with each other.

One benefit of blockchain often neglected in discussions about adopting blockchain is that

[12]Blockchains versus other DLT is analogous to the choice between using Java and Python for data analytics. Clearly, everything that can be done by Python can also be done by Java. However, from an implementation point of view, most data scientists found Python to be much easier to use, with all of the important data analytics and machine learning packages ready to use.

institutions implicitly agree to a stringent data and communications standard that applies to all members, which resolves many coordination problems. This is also why many industries are beginning to organize consortiums to formalize industry-wide blockchain standards, e.g., the Risk Institute for the insurance industry, and Blockchain in Transport Alliance, or BiTA, for the transportation industry. Ultimately, the choice of DLT implementation likely depends on convenience and availability. We focus on blockchain with MPC capabilities while acknowledging that alternative solutions and implementations exist.

3. A Model of Financial Reporting and Auditing

3.1. Auditors in the Traditional World

Consider an economy with (i) a continuum of publicly audited firms (clients) indexed by u, $\{B_u\ ,\ u \in [0,1]\}$, each of size K, (ii) a measure m_{pr} of unaudited firms, such as private or foreign firms, and (iii) M auditing firms, $A_j, 1 \leq j \leq M$. With pairwise interactions, each firm B_u would report K^2 cross-firm transactions with any other audited firm $B_v, v \in [0,1]$, or any unaudited firm. The total measure of all audited transactions would thus also be K^2. As will be explained below, auditors are heterogeneous in their skills, and clients are heterogeneous in their preferences for auditors.

The game starts with the auditors offering an auditing fee/price and firms each choosing an auditor. Once clients contract with an auditor, they choose the probability of overstatement while the auditor chooses the intensity of auditing in the second stage. We solve the model backward by first analyzing the subgame where each client is already matched to an auditor. We then endogenize audit pricing and auditor-client matches in the first stage.

Second stage: reporting and auditing. Suppose a firm has chosen an auditor and reports a continuum of transactions $i \in [0,T]$, where T represents the transaction volume. Each transaction i has a true value of $\tilde{x}_i \in (-\infty, \infty)$. For example, accounts receivable and accounts payable items correspond to $\tilde{x}_i > 0$ and $\tilde{x}_i < 0$, respectively. The true aggregate income of the client for a year is $\int_0^T \tilde{x}_i di$ (see also Figure 1). For each transaction, the client

reports to the auditor the following:

$$x_i = \tilde{x}_i + \varepsilon_i, \tag{1}$$

$$\textit{where} \qquad \varepsilon_i = \begin{cases} 0, & \text{with probability } 1-p, \\ \mu > 0, & \text{with probability } p \end{cases} \tag{2}$$

and p is endogenous and reflects the client manager's tendency to overstate the transaction value. Since higher earnings are generally associated with higher firm valuation and managerial compensation, managers usually have greater incentives to overstate transaction values (e.g. Newman, Patterson, and Smith, 2001; Callen, Khan, and Lu, 2013). Misstatement can also be interpreted as insufficiently frequent disclosures, which entrenches the managers (Shleifer and Vishny, 1989). Managers may misreport to boost their payoff (e.g., stock price in the case of managers holding shares or being compensated with options). Allowing the error term to represent genuine mistakes or understatement of transaction value does not alter the economic intuition or qualitative results.[13]

For each transaction, the auditor obtains his own estimate $\hat{x}_i$ and computes the aggregate income of the client as $\int_0^T \hat{x}_i di$. Following the literature (e.g., Scott, 1973; Antle and Nalebuff, 1991), the auditor faces legal liabilities from restatements and thus needs to minimize the following loss function (auditor risk):

$$L = \lambda E\left[\int_0^T (\hat{x}_i - \tilde{x}_i)^2 di\right], \tag{3}$$

where $\lambda \in (0,1)$ is a scaling parameter reflecting the expected penalty faced by the auditing firm due to a regulator's market monitoring and misstatement detection. Intuitively, when aggregate misreporting levels are high, prices' ability to aggregate dispersed private informa-

[13]For many firms, e.g., manufacturing firms, highly discretionary accounts do not constitute a large portion of their income statements (Stubben, 2010) Although our model focuses on reducing intentional misstatements, it is straightforward to see that collaborative auditing can also significantly reduce the costs of detecting unintentional errors made either by clients or auditors, which further improves audit quality and facilitates internal auditing. Such unintentional errors or mistakes will be detected either instantaneously (if auditing is continuous) or at the time of auditing. These cases will need to be further verified manually using traditional auditing methods. In fact, this should be equivalent to having a greater number of off-chain transactions, and our results still hold without changes.

tion efficiently is reduced. Welfare is then reduced because of inefficient resource allocation in a free market economy (e.g., Hayek, 2009). Thus, as we discuss later, a legal authority or regulator would aim to require and incentivize auditors to reduce misstatements.

In deriving her own estimate, the auditor can either accept the client's report, i.e., setting $\hat{x}_i = x_i$, or expend effort to verify the transaction, i.e., setting $\hat{x}_i = \tilde{x}_i$. Suppose the auditor has limited resources and decides to audit a fraction $s \in [0, 1]$ of all transactions (Becker, 1968), and the cost of such auditing sampling to be $C(s)$, with $C'(s) > 0$ and $C''(s) > 0$ (Lu, 2006). The convexity of the function captures the fact that it is costly to acquire and retain additional human resources in the auditing season. For simplicity, we assume it costs the same to audit a within-auditor transaction and a cross-auditor transaction.[14]

Consider a client u that chooses auditor j. To be concrete, in the following discussion we assume that the cost function for auditor j is of the following form:

$$C_j(s, T) = a_j(sT)^2 + b, \quad a_j > 0, b > 0. \tag{4}$$

where a_j represents the skill of auditor j, with a smaller a_j indicating greater skill of the auditor. The auditor's complete problem is then to minimize the following objective function by choosing the appropriate auditing sample size s,

$$\min_{s\in[0,1]} \lambda E\left[\int_0^T (\hat{x}_i(s) - \tilde{x}_i)^2 di\right] + a_j s^2 T^2 + b. \tag{5}$$

The client determines the probability p of overstatement by trading off the benefits of overstating earnings (e.g., higher stock market valuation and ease of access to external financing) and the costs of being caught reporting erroneously/committing fraud (which damages the reputation of the firm and entails regulatory penalties). We assume that the client maximizes the following second-stage utility function,

$$\max_{p\in[0,1]} \gamma \Pr(\hat{x}_i(s) = x_i > \tilde{x}_i)\mu T - \delta(\Pr(\hat{x}_i(s) = \tilde{x}_i < x_i)T)^2 - d|u - u_j|. \tag{6}$$

[14]Introducing two separate costs adds no new insights, especially when the reduction in auditing cost with blockchain is much larger than the difference between these two costs.

where $\gamma, \delta > 0$. $\Pr(\hat{x}_i(s) = x_i > \tilde{x}_i)$ is the probability that the manager successfully overstates transaction values without being detected by the auditor, and $\Pr(\hat{x}_i(s) = \tilde{x}_i < x_i)$ is the probability that the manager is caught committing fraud. The convex penalty function reflects that the punishment can be nonlinear and more substantial for more severe fraudulent cases. In practice, the penalty corresponds to the cost of a subsequent lawsuit for misreporting and/or reputational damage (e.g., Fischer and Verrecchia, 2000). The last term, with $d > 0$ and $u_j \in [0, 1]$ being a constant associated with auditor j, represents heterogeneous Hotelling preferences (transportation costs) of clients toward different auditors, including geographical proximity or other business connections between the clients and auditors.[15]

From (5), the auditor's problem reduces to:

$$\min_{s\in[0,1]} \lambda T(1-s)p\mu^2 + a_j s^2 T^2 + b. \tag{7}$$

From (6) and the fact that the auditor randomly investigates a sample s, the client's problem can be rewritten as:

$$\max_{p\in[0,1]} \gamma T(1-s)p\mu - \delta(psT)^2 - d|u - u_j|. \tag{8}$$

We solve from (7) and (8) the equilibrium strategies (s^*, p^*) of the auditor and client:[16]

Proposition 1. *For each auditor j and a matched client u, a unique subgame equilibrium exists in the second stage, with the strategies (s_j^*, p_j^*) characterized by*

$$s_j^* = \frac{\lambda p_j^* \mu^2}{2a_j T} \qquad \textit{and} \qquad p_j^* = \min\left(\frac{\gamma\mu(1-s_j^*)}{2\delta s_j^{*2} T}, 1\right). \tag{9}$$

The equilibrium misstatement probability p_j^* is weakly increasing in a_j (auditor skill) and T (transaction volume), while the auditing intensity s_j^* is weakly decreasing in a_j and T. Both p_j^* and s_j^* are increasing in γ (misreporting incentive).

[15] The Hotelling preferences help prevent corner solutions to the competition game among heterogeneous auditors. Other assumptions of heterogeneity among clients can achieve similar qualitative results.

[16] We note that the proposition is robust to more general forms of the cost functions for the firms and auditors. See the Internet Appendix IA.1 for details.

While the sampling size $s_j^* T$ increases with transaction volume, the sampling intensity s_j^* decreases because the auditor finds it more economical to randomly sample a smaller fraction when the total volume is large. Overall, auditing fees are still higher for larger firms with a higher volume of transactions. The misstatement intensity p_j^* and quantity $p_j^* T$ both increase with T given that the auditor samples with less intensity. When auditing cost a_j increases (i.e., when the auditor is less skilled), the optimal audit intensity s_j^* declines. As a result, clients misreport more and p_j^* increases. If a client has a higher misreporting incentive γ, then its equilibrium misstatement intensity p_j^* is higher, leading the auditor to monitor more intensively with a higher s_j^*. Table 1 reports the complete set of comparative statistics for the equilibrium policies with respect to the model parameters. For brevity, we omit the proofs that follow from arguments similar to those in Proposition 1.

Table 1: Dependence of Equilibrium Policies on Model Parameters

	Model Parameters					
	a_j	T	δ	γ	μ	λ
Policy variables						
Misstatement probability: p_j^*	$+$	$+$	$-$	$+$	$-$	$-$
Auditing intensity: s_j^*	$-$	$-$	$-$	$+$	$+$	$+$
Misstatement sample size: $p_j^* T$	$+$	$+$	$-$	$+$	$-$	$-$
Auditing sample size: $s_j^* T$	$-$	$+$	$-$	$+$	$+$	$+$

First stage: auditor fee and competition. We now characterize the first-stage equilibrium, in which the auditors compete for clients by posting auditing fees and the clients choose auditors. For simplicity, we consider the case $M = 2$ below, i.e., there are two auditing firms. We also assume that $u_1 = 0$ and $u_2 = 1$, i.e., the two auditors are at the two ends of the preference spectrum of clients (see (6)). The intuition of our results carries over to the general case with multiple auditing firms, switching costs, and general values of u_j.

Definition 1. A *first-stage equilibrium* of the model is defined as an assignment of clients to auditors and a choice of auditing fees P_j by each auditor j that satisfy these conditions: (i) Given the fees posted, each client selects the auditor that maximizes the client's utility. (ii) Anticipating the other auditor's fee, fee P_j maximizes auditor j's profits.

Since the auditors have heterogeneous skills and utility functions, the equilibrium auditing fees are also heterogeneous in general. The fees have to satisfy $P_j \geq Z_j$, where Z_j is the total cost associated with auditor j auditing one client (note that the cost is the same for all clients). From Proposition 1 and (7),

$$Z_j = \lambda T(1 - s_j^*)p_j^*\mu^2 + a_j s_j^{*2} T^2 + b. \tag{10}$$

where p_j^* and s_j^* are second-stage equilibrium choices of the client and auditor. We define

$$W_j = \gamma T(1 - s_j^*)p_j^*\mu - \delta(ps_j^* T)^2 \tag{11}$$

to be the part of the client's utility in (8) without the last term involving auditor preference.[17] For a client u that chooses auditor j, the client's first-stage utility is thus given by $CU_{u,j} = W_j - d|u - u_j| - P_j$.

Client u chooses Auditor 1 if $CU_{u,1} > CU_{u,2}$, and Auditor 2 if $CU_{u,1} < CU_{u,2}$. The marginal client t^* indifferent between Auditors 1 and 2 must have:

$$CU_{t^*,1} = CU_{t^*,2}, \tag{12}$$

or (recall that $u_1 = 0$ and $u_2 = 1$), $W_1 - P_1 - dt^* = W_2 - P_2 - d(1 - t^*)$.

Solving this, we obtain

$$t^* = \frac{W_1 - W_2 - (P_1 - P_2) + d}{2d}. \tag{13}$$

If the solution t^* of (13) is outside the interval $[0, 1]$, then there is a corner solution, and all clients select one auditor. We focus on the more interesting interior solutions. Equation (12) implies that, in equilibrium, auditor 1 receives share t^* of all clients, and auditor 2 receives

[17] We assume the quadratic forms of the auditor's and clients' utility functions for simplicity. In the Internet Appendix, we show that the main results hold with more general utility functions.

share $1 - t^*$ of clients. The first-stage profits for Auditors 1 and 2 are thus given by:

$$\max_{P_1} \frac{1}{2d}(W_1 - W_2 - (P_1 - P_2) + d)(P_1 - Z_1), \tag{14}$$

$$\max_{P_2} \frac{1}{2d}(W_2 - W_1 - (P_2 - P_1) + d)(P_2 - Z_2). \tag{15}$$

The first order conditions of equations (14) and (15) determine the equilibrium prices:

$$P_1^* = d + \frac{W_1 - W_2 + 2Z_1 + Z_2}{3}, \tag{16}$$

$$P_2^* = d + \frac{W_2 - W_1 + 2Z_2 + Z_1}{3}. \tag{17}$$

We thus obtain the following proposition.

Proposition 2. *There exists a unique equilibrium in which auditors charge auditing fees as given in (16) and (17). In the equilibrium, an endogenous share of m_j clients chooses auditor j. The equilibrium market share m_j is given by*

$$m_j^* = \frac{1}{2}\left(1 + \frac{1}{3d}(W_j - W_{-j} - Z_j + Z_{-j})\right) \tag{18}$$

and the profit of auditor j is given by

$$\Pi_j = \frac{d}{2}\left(1 + \frac{1}{3d}(W_j - W_{-j} - Z_j + Z_{-j})\right)^2, \tag{19}$$

where $-j$ indicates the auditor other than j. If $\gamma < \lambda\mu$, then the endogenous size m_j^* and profit Π_j of auditor j increase with the auditor's skill $\frac{1}{a_j}$.

The endogenous sizes of auditors are determined via competition among auditors and their heterogeneous skills. As we shall demonstrate later, auditor size/skill plays an important role in the adoption of blockchain technology.

3.2. Auditing with Federated Blockchain

In the traditional world, an auditor incurs a cost for each inspection and is thus limited to random sampling due to resource constraints. Blockchains allow the auditor to automate some of the processes. When an auditor sets up a blockchain, the within-auditor transactions can be validated with little cost and time lag; when another auditor also joins the federated blockchain, the inspection of transactions between firms associated with the two auditors can also be done digitally using privacy-preserving secure verification. We take this cost of automated inspection to be negligible relative to traditional inspections.

In a federated blockchain, each auditor A_i establishes an internal permissioned blockchain, with each node operated by an auditing team within the firm.[18] Whenever a transaction i for client x happens, the team responsible for the client uploads the transaction data on the internal blockchain. Depending on the counterparty y, there are three scenarios:

(1) Within-auditor transactions. If this transaction has a counterparty y also audited by the same firm, then the team responsible for client y would also upload the transaction. The blockchain then verifies if the two transaction reports are consistent and, if so, consolidates them into a consensus record. If the reported transactions do not match, the auditor is immediately aware that one or both transactions are misstated and can investigate. Therefore, we assume that the client never misreports in this scenario since the risk of immediate detection is always certain.

(2) Cross-auditor transactions. If the counterparty y is audited by another auditor B who is on the same federated blockchain with A, then A can send a request to the consortium with encrypted information about the transaction k. Then, the blockchain verifies whether there is a matching transaction k'. Auditor B would then be able to verify that it does have the transaction k' and whether the amounts of k and k' match. The verification procedure can be conducted through a secure method so that only encrypted information is revealed to the other party;the client would not commit fraud or misreport.

[18] Alternatively, the nodes can also be operated by client firms or third parties in a blockchain ecosystem.

(3) Off-chain transactions. If the counterparty y is a private firm or is audited by an auditor not on the federated blockchain, then the auditor cannot automate the process and has to resort to random sampling, i.e., the traditional process.

To model the adoption of blockchain, we assume that A_1 and A_2 can decide whether to incur a cost c_1 to adopt the technology. After the adoption decision, the auditors and clients then play out the two-stage game as described in the previous section. Now, a client firm only elects to misstate transactions not reported to a blockchain system by both counterparties, i.e., the off-chain transactions. Similarly, an auditing firm would only need to engage in random sample auditing for off-chain transactions. Suppose an auditor incurs an upfront adoption cost for the blockchain system c_1. We further assume that each blockchain-adopting auditor incurs a cost c_2 per client for maintaining the blockchain infrastructure, including installation, maintenance, and customer service costs for the client. When the cost c_1 or c_2 is large, not adopting blockchain is an equilibrium.[19]

To see this, suppose everyone is playing the equilibrium characterized by Proposition 2. One auditor may deviate to acquire blockchain capacity if it can lower the cost of auditing for its current clients and thus potentially charge a lower fee to attract the other auditor's clients. The auditing cost of an auditor with blockchain thus becomes:

$$Z_j(T_b) = \lambda T_b(1 - s_b^*)p_b^*\mu^2 + a_j s_b^{*2} T_b^2 + b + c_2., \tag{20}$$

where T_b is the number of off-chain transactions, and (s_b^*, p_b^*) are the second-stage equilibrium strategies for the auditor and client when the number of transactions is T_b. T_b would be $(m_{pr} + m_{j-})K^2$ if the other auditor of size m_{j-} chooses not to adopt blockchain, and would be $m_{pr}K^2$ if the auditors form a blockchain consortium. (20) signifies that the auditor only incurs risk or cost for transactions not on the federated blockchain.

[19]We assume that the auditor cannot deviate to not using blockchain after the fees and matching are determined. One important function of blockchain is to allow different parties to commit to share information in a transparent way, which reduces frictions and incentives to misstate. Therefore, commitment to using or not using blockchain is part of the business agreement between the auditor and its client.

We note that the first-stage objective of a firm is:

$$\max_{P_j} m_j(P_j, P_{-j})(P_j - Z_j(T_b)) - c_1,$$

where m_j is the share of clients choosing auditor j and P_j and P_{-j} are the auditing fees charged by auditor j and its competitor. For a sufficiently large c_1 or c_2, the cost of adopting the blockchain outweighs the potential reduction both in auditing costs and gains in market share achieved by charging lower fees, making it unprofitable for an auditor to deviate to adopt.

When adoption costs are small and the reductions in auditing costs are large enough, both auditors adopting the blockchain can be an equilibrium. In this case, if one auditor deviates by not adopting blockchain, it incurs higher costs and has to charge higher fees, thus losing market share and profits. We show in the following proposition that partial equilibria where one auditor adopts blockchain and the other does not are possible. Furthermore, there can be multiple equilibria where both partial equilibria exist at the same time. The intuition is that due to competition, the market shares in the all-adoption equilibrium are similar to those in the no-adoption equilibrium, e.g., the market shares of the auditors would be equal in both cases if the auditors have the same skills. As a result, the benefit for the first auditor adopting blockchain is typically a larger gain in market share than the second adopting auditor, analogous to a first-mover advantage. Therefore, given suitable adoption costs, only one auditor adopts blockchain in equilibrium.

When $\gamma < \lambda\mu$, i.e., when the private benefits of clients are not too large, we have:

Proposition 3. *With auditing based on permissioned blockchains and secure MPC, and with heterogeneous auditing skills, in addition to the no-adoption and all-adoption equilibria, there can be two partial-adoption equilibria in which only one auditor adopts blockchain.*
(i) The all-adoption and no-adoption equilibria do not coexist with the partial-adoption equilibria. When a_1 and a_2 are sufficiently close, the two partial-adoption equilibria can coexist.
(ii) With sufficiently small blockchain operating cost c_2, in a partial adoption equilibrium, the market share of the adopting auditor increases relative to the non-adopting auditor.

(iii) The clients' misreporting probability and auditing fees for blockchain-adopting auditors are lower in the all-adoption equilibrium than those in the partial adoption equilibrium, which are, in turn, lower than those in the no-adoption equilibrium.

By facilitating both the standardization and sharing of data, blockchain can make the switching of clients across auditors easier (i.e., by reducing costs inhibitive to changing auditors over marginal improvements), thus increasing competition among auditors. This ex ante deters auditors from joining a federated blockchain. As such, when full adoption generally results in higher social welfare, regulators may need to coordinate and possibly subsidize adoption (see Section 3.3).

We plot in Figure 5 the equilibrium adoption strategies and the market share distributions for the model with heterogeneous auditor skills. In particular, we consider the case where $a_1 < a_2$ and A_1 is the more skilled or larger auditor.

First, we note that both types of partial equilibria exist for a wide range of parameter values of the manager's misstatement incentive γ and blockchain adoption cost c_1 (Panel A). For a fixed γ, when c_1 is very low, all adoption is the only equilibrium, and when c_1 is high, no adoption is the only equilibrium. For intermediate values of blockchain adoption cost c_1, either one or both partial equilibria exist. We note that for smaller values of c_1, the partial equilibrium where smaller auditor A_2 adopts is more likely to exist, and for larger values of c_1, the equilibrium where A_1 adopts is more likely to exist. This reflects that the marginal benefit of blockchain adoption is likely higher for the smaller auditor.

Second, we examine the size or market share of the more skilled auditor (A_1) in different equilibria as γ varies in Panel B.[20] Several interesting patterns emerge here. The market share or size of A_1 is the largest in the partial adoption equilibrium where A_1 adopts and the smallest in the partial adoption equilibrium where A_2 adopts. This is intuitive as partial equilibria provide a first-mover advantage to the adopting auditor. Moreover, the market share of A_1 is smaller in the full adoption equilibrium than in the no adoption equilibrium. This suggests that the improved efficiency offered by blockchain technology allows smaller

[20] In the model, the equilibrium market shares of the auditors do not depend on the value of c_1, although the existence of certain types of equilibria can depend on c_1.

auditors to be more competitive against larger auditors, leveling the playing field.

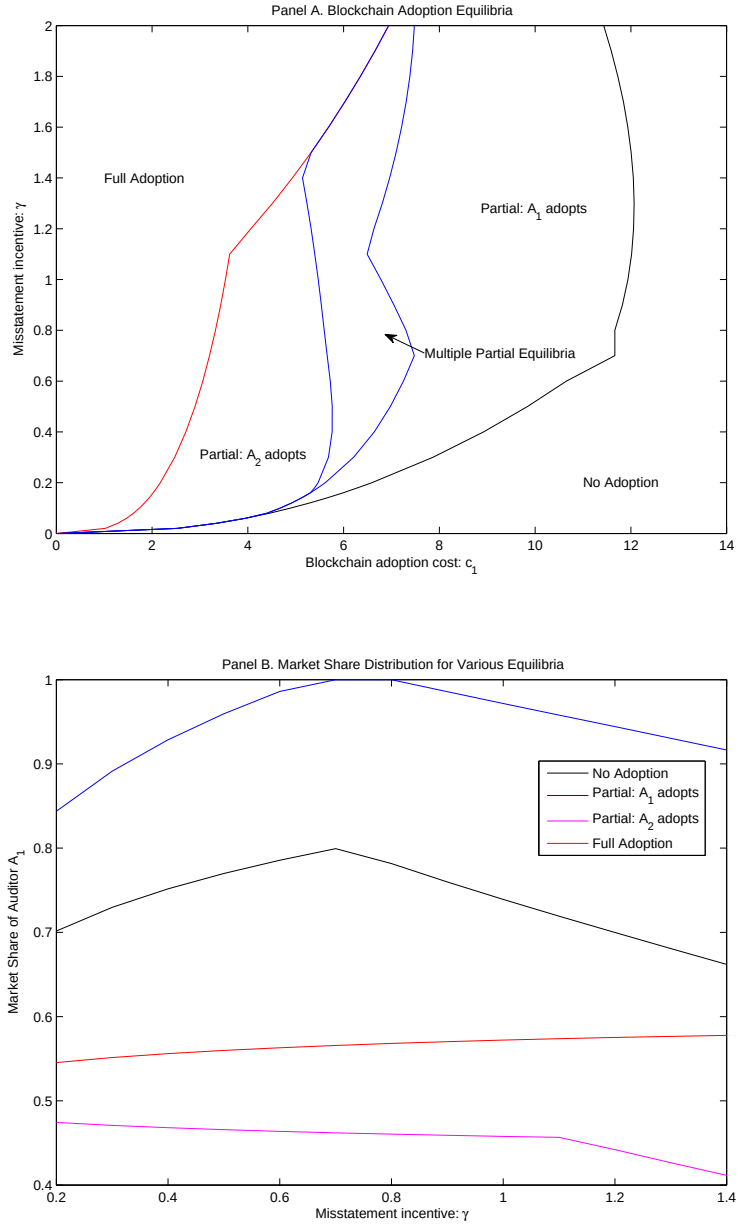

Figure 5: **Equilibrium Adoption of Blockchains and Market Share: Heterogenous Auditors and Clients** This figure shows how the model's equilibria vary with parameters. Panel A plots the regions with different equilibria for varying blockchain adoption cost γ and client's misstatement incentive γ. Panel B depicts the market share of auditor A_1 under the different equilibria. The values of other parameters are $K = 5, K_{pr} = 5, \mu = 1, \delta = 1, \lambda = 1, a_1 = 0.05, a_2 = 0.10, b = 0, c_1 = 1, c_2 = 0.02, d = 15$.

In the partial equilibrium where only the larger auditor adopts blockchain, the cost of

implementing blockchain creates hurdles for small auditors and further widens the disparity between large and small auditors. There are different potential solutions to this in practice. First, small auditors can form consortiums, sharing the fixed development costs of blockchains. Second, it might be possible for small auditors to pay a fee to large auditors to utilize the established blockchain, thus avoiding prohibitive entry costs associated with implementing infrastructure. Third, regulators can provide subsidies to the auditors to facilitate full adoption (motivated by the potential for increased social welfare via reductions in misstatements) – a solution we discuss in the next section.

Non-collaborative auditing. When each auditor chooses to operate his own independent blockchain rather than joining the integrated, federated structure, within-auditor transactions can be costlessly verified as in the federated case. However, verifying cross-auditor transactions remains costly, despite the fact that both auditors have blockchains. The following corollary demonstrates that a federated blockchain is superior to a system of independent blockchains as it further reduces auditing fees and risks. The key difference between the federated blockchain and independent blockchains is that *cross-auditor transactions* can be automatically verified on the network using secure encryption methods.

Corollary 1. *In the full adoption equilibrium with independent blockchains, the misstatement probability and auditing fees are lower than those in the model without blockchains, but higher than those in the full adoption model with a federated blockchain.*

3.3. Social Welfare and Regulatory Interventions

Auditors have several limitations and frictions in blockchain adoption. First, entry costs consist of the implementation cost of blockchain infrastructure and the auditors' cost of onboarding the new system. Second, collaborative auditing necessitates a certain standardization of blockchain platforms for client and audit firms. While further technological progress, the establishment of consortiums, or simple subsidization may mitigate the fixed expense of implementation, the challenge of coordinating simultaneous industry-wide technology adoption remains daunting, necessitating regulatory interventions.

As shown in the last section, competition among auditors can lead to partial adoption equilibria, which are suboptimal from the social viewpoint. We define social welfare in our model as the negative of the sum of the auditor's costs, i.e.,

$$SW_0 = -\sum_{j=1}^{2} m_j^*(\lambda T(1-s_j^*)p_j^*\mu^2 + a_j s_j^{*2} T^2 + b).$$

The social welfare in the case of full blockchain adoption is

$$SW_b = -\sum_{j=1}^{2} m_j^*(\lambda T_b(1-s_{j,b}^*)p_{j,b}^*\mu^2 + a_j s_{j,b}^{*2} T_b^2 + b + c_2) + 2c_1,$$

where c_2 is the blockchain operation cost and c_1 is the adoption cost of blockchain by each auditor. We exclude the clients' private utility in the social welfare because the private benefits of clients from restatement typically come at a cost for the broad investor base.[21]

We present the following proposition regarding the social optimality of blockchain adoption equilibria and the possibility of conducting a wealth transfer to facilitate full adoption. For ease of treatment, we assume the auditors are of the same size, i.e., $a_1 = a_2$, in the proposition. The intuition carries over to more general cases.

Proposition 4. *When the operation cost c_2 is sufficiently small, $\exists\ C_1 > C_2 > 0$ such that:*

(i) Full adoption is an equilibrium if and only if the adoption cost satisfies $c \leq C_2$. Full adoption increases social welfare, i.e., $SW_b > SW_0$, if and only if $c < C_1$.

(ii) For $C_2 < c < C_1$, the industry equilibrium does not realize the social optimum. A regulator (or social planner) can make a wealth transfer to the auditors and coordinate the full adoption equilibrium to achieve the social optimum.

Given the potential reduction of misstatements and costs associated with auditing competition, we expect the government to play a pivotal role in facilitating the coordination and adoption of the technology. For example, government subsidies and regulatory standards can be critical to implementing blockchain-based auditing successfully.

[21] The following results still hold even if we include clients' utility in the above definition.

4. Model Extensions and Discussions

4.1. Endogenous Choice of Transaction Partners

Up to this point, we have assumed that the amount and type of transactions of clients are exogenously given. However, blockchain adoption may reduce some clients' private utility by making it harder for them to misreport earnings. These clients, in anticipation of blockchain adoption by the auditing industry, may choose to transact with more private partners who are off the blockchain. Such actions by the clients, in turn, can change the amount of on-chain transactions and affect the benefits of blockchain implementation. In this section, we model clients' endogenous choice of transaction partners and study its implications.

We keep the model structure the same as before, except by adding an endogenous choice step at the beginning of the time period. We assume that a client is unaware of their type $u \in [0, 1]$ to start with. Each client needs to decide the ratio of private partners m and public partners $1 - m$ before its type is known. After this, the client's type is revealed publicly, and the game proceeds as set up before. With the choice m, the number of transactions that cannot be automated by blockchain is mK^2, and that can potentially be automated is $(1 - m)K^2$. We consider symmetric equilibria where all clients choose the same ratio m ex-ante. We show that the endogenous choice of transactions can change the outcome substantially. There are two interesting cases:

(1) If the private benefit of clients (γ) is large and blockchain adoption increases social welfare, then clients may find it optimal to switch all transactions to be off-chain ex-ante, rendering blockchain adoption infeasible.

(2) If γ is small and all-adoption is an equilibrium, then clients may find it optimal to only transact with public partners and put all transactions on-chain.

Internet Appendix IA.2 contains the derivations while Figure 6 illustrates the results.

Panel A of Figure 6 shows that when γ is low ($= 3$), both the client's ex-ante expected utility (before making the choice of trade partners) and the social welfare decrease with the private share m of transactions. Depending on the value of m, there are three equilibrium outcomes: the industry full-adoption equilibrium for $m < 0.19$ in which the auditors volun-

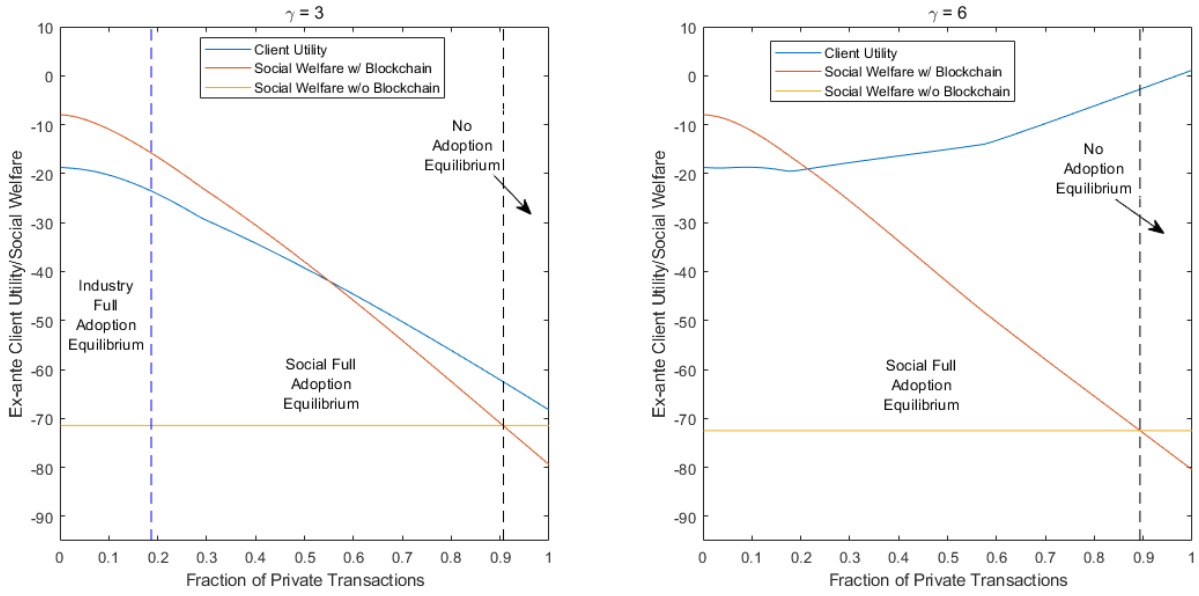

Figure 6: **Endogenous Choice of Transaction Partners and Blockchain Adoption** This figure shows how blockchain equilibrium adoption and the ex-ante client's expected utility and social utility functions depend on the fraction of private transactions (m). $c_1 = 4$ and the other parameters are the same as in Figure 5.

tarily adopt blockchain, the social full-adoption equilibrium for $0.19 < m < 0.91$ in which the social planner subsidizes and coordinates the full-adoption equilibrium, and the no-adoption equilibrium when $m > 0.91$ where it is not socially optimal to adopt blockchains due to its limited benefits. Since the client's ex-ante utility is decreasing with m, they would choose the optimal level of m, which is zero, and the industry's full adoption happens. Therefore, in this case, the option to endogenously select trade partners helps to convert all transactions online and make full adoption possible.

Pane B displays the scenario for a higher $\gamma = 6$. With greater private benefits, the clients now find the transparency offered by blockchains to be costly, and their ex-ante utility increases with the private share of transactions. Therefore, the client will choose the optimal $m = 1$, i.e., have all transactions with private partners. In this case, even the social-planner-subsidized adoption equilibrium breaks down because blockchain can no longer bring social benefits with all transactions off the chain.

Overall, the endogenous choice of partners can add complexity to the equilibria. Depending on the parameters of the model, these endogenous choices can either increase or

decrease social welfare. In cases with large private clients' incentive to misstate, it can lead to suboptimal non-adoption despite the social planner's efforts. Regulators thus need to consider the potential repercussions when weighing blockchain adoption policies.

4.2. Discretionary Auditing and Blockchains

As discussed above, many of the auditing tasks for transaction-based or nondiscretionary accounts can be automated with blockchain. In reality, many companies also have discretionary items such as bad debt expenses, which may not be automatically verifiable because they require auditors' experience, discretion, and industry expertise. Nonetheless, the introduction of blockchain can still have indirect effects on discretionary auditing. We consider below a model extension in which auditors conduct both nondiscretionary and discretionary auditing. Details of the extension are provided in Internet Appendix IA.3.

When auditors adopt blockchain, the volume of a client's transaction-based accounts that need to be verified by conventional methods shrinks. Discretionary accounts, meanwhile, still need to be audited in the traditional way. We show that in the full-adoption equilibrium with discretionary account auditing and blockchains, compared with the equilibrium in the traditional world, the clients misreport less in both the discretionary and transaction-based accounts, and auditing fees decrease.

This proposition implies that with the adoption of blockchains, auditors need to focus less on the more routine, non-discretionary tasks and can focus auditing efforts on discretionary accounts instead. There is a *spillover* effect from the cost savings in transaction-based auditing to discretionary auditing: since auditors now devote a larger proportion of resources to discretionary auditing, clients are forced to misstate less in discretionary accounts in addition to transaction-based accounts, and thus auditing quality in both types of accounts improves. In the auditor labor market, there will likely be lower demand for less skillful auditors but greater demand for more skillful auditors due to the increased focus on off-chain transactions and highly discretionary accounts.

4.3. Blockchain Costs Paid by Firms

We have so far assumed that auditors will maintain the blockchain and pay for the costs. Indeed, due to the economy of scale and to avoid duplication costs, it is in general optimal for the auditors to bear the fixed development and investment costs. Nonetheless, we consider a model extension that allows the clients to cover the operating costs of blockchain and examine the implications. Details and proofs of the model are in Internet Appendix IA.4.

We show that there is a coordination problem when clients need to decide whether to adopt blockchain. Essentially, there needs to be a critical mass of clients who decide to switch. Otherwise, the network benefits of blockchain adoption are insufficient to cover the cost of adoption, and the equilibrium is no one will adopt. This coordination problem is related to the coordination among different auditors but is more severe because there are many more clients to coordinate with.

For this reason, we believe it is better for auditors to cover the costs of blockchain, at least initially. Once blockchain reporting/auditing gains a sufficient toehold in adoption (over the critical threshold), the business model can be potentially converted to one where clients share at least some of the operating costs.

4.4. Heterogeneous Transaction Sizes

We have modeled how client firms could manipulate the extensive margins of transactions (how many transactions to misreport) but not the intensive margins (how much to misstate for each transaction). In reality, a firm can reap greater benefits if it can manipulate fewer, larger items without getting caught. Being aware of this incentive, the auditor would also pay closer attention to larger transactions. In equilibrium, the optimal allocation of misreporting and monitoring efforts for large and small transactions will depend on both parties' incentives and utility functions.

In an extension of the basic auditing model that allows heterogeneous transaction sizes (Internet Appendix IA.5), we show that the auditor would sample larger transactions more frequently. Interestingly, in equilibrium, the clients in fact are more likely to misstate smaller transactions than larger transactions.

This issue actually highlights another benefit of blockchain—it works regardless of the size of the transaction. With blockchain, any manipulation can be found, making size less important. For larger transactions, blockchain automation can thus help to save more manual labor and reduce auditors' costs even more.

5. Conclusion

We analyze equilibrium outcomes of financial reporting and auditing in settings with and without distributed ledger technology combined with secure MPC to demonstrate how permissioned blockchains are not merely a database upgrade but have novel economic implications. Specifically, we model an economy in which auditors post fees to compete for client firms while clients determine the optimal level of misstatement in anticipation of the endogenous auditing intensity. We argue that federated blockchains and secure encryption can allay data-privacy concerns without requiring a trusted third party, and thus connect isolated auditing processes either across audit teams or audit firms. Blockchains therefore potentially facilitate automated and collaborative auditing by reducing audit costs for transaction-based accounts. The technology can thus disrupt conventional audit pricing, sampling, and effort allocation. Private benefits of client firms and first-mover advantages of auditors can cause non-adoption or partial blockchain adoption equilibria. Importantly, regulators can coordinate systematic adoption to capitalize on the positive externality in utilizing the technology, increasing social welfare. Our model also provides an initial framework for further studies of the costs and implications of blockchain adoption. For example, we find that it would be more efficient for auditors to bear the initial costs of blockchain.

To capture the first-order implications of blockchains on financial reporting in a transparent manner, we have abstracted away some finer details of the tradeoffs in consensus generation and encryption of private data. We also note that blockchain is not the only technology that can enable collaborative auditing, though it is a salient candidate. It is our hope that this study will lead to future research about how technological advances impact financial reporting and auditing. Moreover, our paper illustrates how permissioned

blockchains without free entry or native crypto-tokens can still constitute an innovation that disrupts existing industries. In addition to better data management, they provide an infrastructure for independent databases to interact without sacrificing data privacy. Given that information-sharing algorithms are important in many services, such as lender services in credit markets (Liberti, Sturgess, and Sutherland, 2022), the economic implications of multi-party computation remain a fruitful area for future research.

References

Amiram, D., B. N. Jørgensen, and D. Rabetti. 2022. Coins for bombs: The predictive ability of on-chain transfers for terrorist attacks. *Journal of Accounting Research* 60:427–66.

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

Bajpai, P. 2017. Big 4 accounting firms are experimenting with blockchain and bitcoin. *Nasdaq.com* July 5.

Becker, G. S. 1968. Crime and punishment: An economic approach. *Journal of Political Economy* 76:169–217.

Bogdanov, D., M. Jõemets, S. Siim, and M. Vaht. 2015. How the estonian tax and customs board evaluated a tax fraud detection system based on secure multi-party computation. In *International conference on financial cryptography and data security*, 227–34. Springer.

Businesswire. 2023. AntChain unveils multiple new Web3 initiatives with partners. April 26.

Callen, J. L., M. Khan, and H. Lu. 2013. Accounting quality, stock price delay, and future stock returns. *Contemporary Accounting Research* 30:269–95.

Cao, S., L. W. Cong, M. Han, Q. Hou, and B. Yang. 2020. Blockchain architecture for auditing automation and trust building in public markets. *IEEE Computer* 53:20–8.

Caskey, J., V. Nagar, and P. Petacchi. 2010. Reporting bias with an audit committee. *The Accounting Review* 85:447–81.

Chen, L., L. W. Cong, and Y. Xiao. 2021. A brief introduction to blockchain economics. In *Information for efficient decision making: Big data, blockchain and relevance*, 1–40. World Scientific.

Chen, M. A., S. S. Hu, J. Wang, and Q. Wu. 2023. Can blockchain technology help overcome contractual incompleteness? evidence from state laws. *Management Science* 69:6540–67.

Chinco, A. 2022. Proving you can pick stocks without revealing how. Working Paper.

Chiu, J., and T. V. Koeppl. 2019. Blockchain-based settlement for asset trading. *The Review of Financial Studies* 32:1716–53.

Chod, J., and E. Lyandres. 2021. A theory of ICOs: Diversification, agency, and information asymmetry. *Management Science* 67:5969–89.

Chod, J., N. Trichakis, G. Tsoukalas, H. Aspegren, and M. Weber. 2020. On the financing benefits of supply chain transparency and blockchain adoption. *Management science* 66:4378–96.

CNN. 2018. Big four giant pwc announces blockchain auditing service. March 17.

Cohn, M. 2016. Get ready for blockchain's big impact. *Accounting Today* Dec. 6.

Cong, L. W., and Z. He. 2019. Blockchain disruption and smart contracts. *The Review of Financial Studies* 32:1754–97.

Cong, L. W., Z. He, and J. Li. 2021. Decentralized mining in centralized pools. *The Review of Financial Studies* 34:1191–235.

Cong, L. W., W. Landsman, E. Maydew, and D. Rabetti. 2023. Tax-loss harvesting with cryptocurrencies. *Journal of Accounting and Economics* forthcoming.

Cong, L. W., Y. Li, and N. Wang. 2021. Tokenomics: Dynamic adoption and valuation. *The Review of Financial Studies* 34:1105–55.

Cui, Y., M. Hu, and J. Liu. 2023. Value and design of traceability-driven blockchains. *Manufacturing & Service Operations Management* 25:1099–116.

Dai, J., and M. A. Vasarhelyi. 2017. Toward blockchain-based accounting and assurance. *Journal of Information Systems* 31:5–21.

DeAngelo, L. E. 1981. Auditor independence, 'low balling', and disclosure regulation. *Journal of Accounting and Economics* 3:113–27.

Deloitte. 2016. Blockchain technology: A game-changer in accounting? Industry Report.

Deng, M., T. Lu, D. A. Simunic, and M. Ye. 2014. Do joint audits improve or impair audit quality? *Journal of Accounting Research* 52:1029–60.

Easley, D., M. O'Hara, and S. Basu. 2019. From mining to markets: The evolution of bitcoin transaction fees. *Journal of Financial Economics* 134:91–109.

E&Y. 2020. EY launches Baseline protocol, an open source initiative for the public ethereum blockchain. March 4.

FEI. 2018. Blockchain and the future of financial reporting.

Fellingham, J. C., and D. P. Newman. 1985. Strategic considerations in auditing. *Accounting Review* 634–50.

Fischer, P. E., and R. E. Verrecchia. 2000. Reporting bias. *The Accounting Review* 75:229–45.

Goldreich, O., S. Micali, and A. Wigderson. 1987. How to play any mental game – A completeness theorem for protocols with honest majority. *STOC* 218–29.

Halaburda, H., M. Sarvary, and G. Haeringer. 2022. *Beyond Bitcoin: Economics of digital currencies and blockchain technologies*. Springer.

Harvey, C. R. 2016. Cryptofinance. *Available at SSRN 2438299* .

Harvey, C. R., A. Ramachandran, and J. Santoro. 2021. *Defi and the future of finance*. John Wiley & Sons.

Hastings, M., B. H. Falk, and G. Tsoukalas. 2022. Privacy-preserving network analytics. *Management Science* forthcoming.

Hayek, F. A. 2009. The use of knowledge in society. *American Economic Review* 35:519–30.

Hinzen, F. J., K. John, and F. Saleh. 2022. Bitcoin's limited adoption problem. *Journal of Financial Economics* 144:347–69.

Iyengar, G., F. Saleh, J. Sethuraman, and W. Wang. 2022a. Blockchain adoption in a supply chain with market power. Working Paper.

———. 2022b. Economics of permissioned blockchain adoption. *Management Science* forthcoming.

Katz, M. L., and C. Shapiro. 1986. Technology adoption in the presence of network externalities. *Journal of Political Economy* 94:822–41.

Lerner, J., and J. Tirole. 2014. A better route to tech standards. *Science* 343:972–3.

Liberti, J., J. Sturgess, and A. Sutherland. 2022. How voluntary information sharing systems form: Evidence from a us commercial credit bureau. *Journal of Financial Economics* 145:827–49.

Lu, T. 2006. Does opinion shopping impair auditor independence and audit quality? *Journal of Accounting Research* 44:561–83.

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

Ma, H., Y. Xia, and B. Yang. 2022. Blockchains, smart contracts, and supply chain efficiency. Working Paper.

Mearian, L. 2018. Coming soon: Public blockchains for private business data. *Computer World* Nov. 6.

Nakamoto, S. 2008. Bitcoin: A peer-to-peer electronic cash system. *Decentralized business review* 21260.

Narula, N., W. Vasquez, and M. Virza. 2018. zkledger: Privacy-preserving auditing for distributed ledgers. In *15th USENIX Symposium on Networked Systems Design and Implementation (NSDI 18)*, 65–80.

Newman, D. P., E. Patterson, and R. Smith. 2001. The influence of potentially fraudulent reports on audit risk assessment and planning. *The Accounting Review* 76:59–80.

Patterson, E. R. 1993. Strategic sample size choice in auditing. *Journal of Accounting Research* 31:272–93.

Pymnts. 2019. Tencent spearheads blockchain invoice standardization initiative. October 29.

Scott, W. R. 1973. A bayesian approach to asset valuation and audit size. *Journal of Accounting Research* 304–30.

Shleifer, A., and R. W. Vishny. 1989. Management entrenchment: The case of manager-specific investments. *Journal of Financial Economics* 25:123–39.

Simunic, D. A. 1980. The pricing of audit services: Theory and evidence. *Journal of Accounting Research* 161–90.

Smith, S. S. 2018. Blockchain augmented audit–benefits and challenges for accounting professionals. *The Journal of Theoretical Accounting Research* 14:117–37.

Strobl, G. 2013. Earnings manipulation and the cost of capital. *Journal of Accounting Research* 51:449–73.

Stubben, S. R. 2010. Discretionary revenues as a measure of earnings management. *The Accounting Review* 85:695–717.

Teoh, S. H. 1992. Auditor independence, dismissal threats, and the market reaction to auditor switches. *Journal of Accounting Research* 30:1–23.

Townsend, R. M. 2020. *Distributed ledgers: Design and regulation of financial infrastructure and payment systems*. MIT Press.

Tsoukalas, G., and B. H. Falk. 2020. Token-weighted crowdsourcing. *Management Science* 66:3843–59.

Tysiac, K. 2018. How blockchain might affect audit and assurance. *Journal of Accountancy* 15.

Vetter, A. 2018. Blockchain is already changing accounting. *Accounting Today* May 7.

Wang, X., S. Ranellucci, and J. Katz. 2017a. Authenticated garbling and efficient maliciously secure two-party computation. In *Proceedings of the 2017 ACM SIGSAC conference on computer and communications security*, 21–37.

———. 2017b. Global-scale secure multiparty computation. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, 39–56.

Wang, Y., and A. Kogan. 2018. Designing confidentiality-preserving blockchain-based transaction processing systems. *International Journal of Accounting Information Systems* 30:1–18.

Yao, A. C.-C. 1986. How to generate and exchange secrets. In *FOCS*, 162–7. IEEE.

Yermack, D. 2017. Corporate governance and blockchains. *Review of Finance* 21:7–31.

Appendix A. Blockchains and Privacy

Distributed Ledgers and Permissioned Blockchains

Blockchains, or more generally, distributed ledger technologies, are based on several advancements in computing science, including hashing, digital signatures, distributed systems, and consensus mechanisms. Although these individual elements were introduced earlier, Nakamoto (2008) brought them all together and proposed a peer-to-peer distributed transaction and ledger system, i.e., Bitcoin, that aimed to solve a number of problems facing decentralized digital currencies, such as double-spending, consensus, economic incentives of peer nodes, and security. Since then, many more applications of blockchains have been developed, including fundraising through initial coin offerings on social platforms, trades and settlements of financial securities, supply chain management, and other business applications. The key features of a blockchain typically include transparency, immutability, security, and resilience. Many of these features make blockchains an attractive option in financial or business applications. We refer the reader to Yermack (2017), Cong and He (2019), Harvey, Ramachandran, and Santoro (2021), and Chen, Cong, and Xiao (2021) for the basics and business applications of blockchains.

In this paper, we consider permissioned blockchains, which have become the focus of many recent business start-ups. While public or permissionless blockchains such as Bitcoin or Ethereum typically allow anyone to join as peer nodes in the network, a permissioned blockchain only includes identified nodes that can be trusted to some extent.[22] One main benefit of the permissioned blockchain is that it can adopt a more efficient consensus algorithm (e.g., majority voting) and thus prevent the energy waste associated with mining and proof-of-work (the consensus algorithm currently employed by Bitcoin and many other cryptocurrencies; see, for example, Chiu and Koeppl (2019) and Cong, He, and Li (2021)). Permissioned blockchains are also more secure from attacks and can handle higher throughput. Some early open-source software for permissioned blockchains include Corda (by R3), Hyperledger Fabric (by IBM), and Quorum (by J.P. Morgan). Various companies have

[22]The nodes on the network can still be motivated by individual economic incentives.

also developed their own proprietary permissioned blockchain systems. For example, Digital Asset Holdings helped the Australian Stock Exchange in transitioning their trading and settlements to a new system based on permissioned blockchains.

In recent years, open source blockchain systems have offered a number of new options for permission blockchains. For example, Cosmos SDK allows the building of proof-of-stake permissionless blockchains and proof-of-authority permissioned blockchains that can natively interoperate with each other.[23] Similarly, OP Stack (Avalanche) has also made it possible to build public or private Layer-2 blockchains (subnets) that are both scalable and interoperable.[24] These open-source and highly scalable solutions may provide promising solutions to the auditing and financial reporting applications in our model. The interoperability of such blockchains can also be key to building a system of federated blockchains for auditing.

In our setting, permissioned blockchains can include nodes for auditors, clients and their transaction counterparties, and regulators. The immutability and traceability of records on blockchains are particularly important for auditing purposes. However, protecting the privacy of clients can also be an important concern, which we address below.

Privacy and Encryption

One key feature of blockchains is that transactions are typically accessible to the public (for permissionless blockchains) or to all the permissioned parties (for permissioned blockchains). This transparency feature helps to ensure the validity of transactions but can come at the cost of the transacting counterparties' privacy. There are a number of encryption algorithms such as zero-knowledge proofs, homomorphic encryption, and multi-party secure computation, from the field of cryptography that can ensure both validity and confidentiality of records in a blockchain.

Zero-knowledge proof. A *zero-knowledge proof* (ZKP, Goldreich, Micali, and Wigderson, 1987) is a proof of a statement by one party (the prover) to another party (the verifier)

[23] https://docs.cosmos.network/main/learn.

[24] More information is available at https://docs.optimism.io/stack/getting-started and https://docs.avax.network/intro.

without conveying any additional information to the verifier, other than the correctness of the statement. This may sound paradoxical, but it is possible using ideas in cryptography. Zero-knowledge proofs have found many applications in privacy-sensitive environments. For example, Zcash is a cryptocurrency that is similar to Bitcoin but employs cryptographic tools to truly anonymize transactions, which can hide transaction counterparties and amounts while allowing others to validate the transactions. Zcash uses a new type of zero-knowledge protocol called zk-SNARKs.[25] Ethereum introduced support for zk-SNARKs in its Byzantium hard-fork update in 2017. Since then, many smart contracts on Ethereum, such as Railgun and Tornado Cash, have enabled the privacy of transactions with ZKPs.[26] ZKPs also allow the verification of the validity of transactions without the need to see all transactions and enable an important scaling Layer-2 solution, zk-EVM and zk-rollups. In 2023, several zk-EVM became available, including zkSync, Polygon, and Consensys Linea, which have the potential to vastly expand the scalability and security of the Ethereum ecosystem.[27]

Several protocols have been proposed to use ZKPs to verify transactions and records. For example, zkLedger is a protocol allowing outside auditors to verify accurate information while protecting privacy through zero-knowledge proofs (Narula, Vasquez, and Virza, 2018). Qedit provides a number of privacy-preserving solutions on the blockchain using zero-knowledge proofs, including asset transfers, supply chain transactions, and auditing.[28] In one application, their system can help Airlines verify the flown hours of pilots and the maintenance status of airlines without revealing detailed flight and service schedules. Espresso Systems has also developed similar applications that can verify sanction-compliance of transactions. Their CAPE (Configurable Asset Privacy for Ethereum) application is a smart contract that allows the privacy of transactions to normal users and, at the same time, access by auditors and regulators.[29]

[25] Details about Zcash's implementation of zero-knowledge proof algorithms for anonymous transactions are available at https://z.cash/technology/zksnarks.

[26] See https://docs.railgun.org/wiki.

[27] https://cointelegraph.com/news/four-zk-proof-l2s-that-scaled-ethereum-in-2023.

[28] https://qed-it.com/.

[29] More information is available at https://www.espressosys.com/.

Secure multi-party computation. Secure multi-party computation (MPC) algorithms allow different parties to interact and compute a function jointly from their private inputs, without revealing the values of the inputs. For example, in the millionaire's problem, two millionaires would like to compare their wealth but do not want to reveal the amount of wealth to each other. Yao (1986) first proposes a solution of the two-party computation problem and Goldreich, Micali, and Wigderson (1987) solve the multi-party case. Wang, Ranellucci, and Katz (2017a,b) provide efficient algorithms for two-party and multi-party secure computations. Secure multi-party computation algorithms often involve *homomorphic encryption*, which are encryption algorithms that preserve arithmetic operations. In recent years, given the importance of data privacy, MPC has found many applications, e.g., private financial transactions such as auctions and private machine learning where the original data need to be kept secret. As an application of MPC to auditing, Cybernetica applied MPC to go through all sales data in Estonia to identify potential value-added tax fraud, while preserving the privacy of business owners (Bogdanov et al., 2015).

Appendix B. Proofs

Proof of Proposition 1. For simplicity of notation, we omit subscript j that indicates the auditor in this proof. The system of FOC equations from (7) and (8) are

$$s = \min\left(\frac{\lambda\mu^2 p}{2aT}, 1\right), \tag{A1}$$

$$p = \min\left(\frac{\gamma\mu(1-s)}{2\delta s^2 T}, 1\right). \tag{A2}$$

Consider the two curves on the $s-p$ plane determined by Equations (A1) and (A2). Define $g(s) = \frac{2asT}{\lambda\mu^2}$ and $h(s) = \frac{\gamma\mu(1-s)}{2\delta s^2 T}$. The first curve is given by $p = g(s)$ when $0 \le s < 1$ and $p \ge g(1)$ when $s = 1$. The second curve is given by $p = \min(h(s),1)$ for $0 \le s \le 1$. Since $g(s)$ is increasing in s, the first curve is increasing in s. We have

$$h'(s) = \frac{\gamma\mu}{2\delta T} \cdot \frac{s-2}{s^3} < 0, \quad \text{if } 0 < s \le 1.$$

Therefore, the second curve is decreasing in s for $s \in [0,1]$. Note that $g(0) = 0$, $g(1) > 0$, $\min(h(0),1) = 1$, $\min(h(1),1) = 0$, by continuity, there is a unique intersection point (s^*, p^*) of the two curves with $0 < s^* < 1$ such that $p^* = g(s^*) = \min(h(s^*),1)$. (p^*, s^*) thus gives the unique equilibrium of the clients' and auditors' problems. We note that in equilibrium the strict inequality in (A1) always holds.

For comparative statics, we can focus on the interior solution. The equilibrium policy s^* satisfies the following equation derived from (A1) and (A2),

$$4a\delta T^2 s^{*3} = \lambda\gamma\mu^3(1-s^*). \tag{A3}$$

Taking derivatives of the equation and using the fact that $0 < s^* < 1$, one can then easily show that $\frac{\partial s^*}{\partial a} < 0$. Equation (A2) then implies that

$$\frac{\partial p^*}{\partial a} = l\frac{-s^{*2} - 2s^*(1-s^*)}{s^{*4}}\frac{\partial s^*}{\partial a} = l\frac{s^*-2}{s^{*3}}\frac{\partial s^*}{\partial a} > 0,$$

where l is a constant independent of a. For brevity of notation, when we derive comparative statics for a variable, we shall always use l to denote a quantity that is independent of the key variables in question. Therefore, l may represent different constants below in different contexts. Similarly, from (A3), we have $\frac{\partial s^*}{\partial T} < 0$. (A3) then implies that

$$s^*T = \frac{(s^{*3}T^2)^{1/2}}{s^{*1/2}} = l\frac{(1-s^*)^{1/2}}{s^{*1/2}}$$

increases with T, where l is independent of T. From (A2),

$$p^* = \frac{\gamma\mu(1-s^*)}{2\delta s^{*2}T} = \frac{\gamma\mu(1-s^*)}{2\delta s^{*1/2}(s^{*3}T^2)^{1/2}} = l\frac{(1-s^*)}{s^{*1/2}(1-s^*)^{1/2}} = l\frac{(1-s^*)^{1/2}}{s^{*1/2}},$$

which is again increasing with T, where l is independent of T. $p^*T = \frac{\gamma\mu(1-s^*)}{2\delta s^{*2}}$ also increases with T. Similarly, we have $\frac{\partial s^*}{\partial \gamma} > 0$ from (A3). From (A2) and (A3),

$$p^* = l\frac{\gamma(1-s^*)}{s^{*2}} = l's^*$$

also increases with γ, where l and l' are independent of γ. Q.E.D.

Proof of Proposition 2. From (13), (16), and (17), we obtain

$$m_1^* = t^* = \frac{1}{2}\left(1 + \frac{1}{3d}(W_1 - W_2 - Z_1 + Z_2)\right)$$

and

$$m_2^* = 1 - t^* = \frac{1}{2}\left(1 + \frac{1}{3d}(W_2 - W_1 - Z_2 + Z_1)\right).$$

Hence (18) holds. The profit of auditor 1 is thus

$$\Pi_1 = m_1^*(P_1^* - Z_1) = \frac{d}{2}\left(1 + \frac{1}{3d}(W_1 - W_2 - Z_1 + Z_2)\right)^2.$$

We can derive Π_2 similarly and thus (19).

To show that m_j^* and Π_j are increasing in $1/a_j$, or decreasing in a_j, we only need to show that $W_j - W_{-j} - Z_j + Z_{-j}$ is decreasing in a_j. Since $W_{-j} - Z_{-j}$ does not depend on a_j, we just need to show that $W_j - Z_j$ is decreasing in a_j. (10), (11), and Proposition 1 imply that

$$\begin{aligned} W_j - Z_j &= \gamma T(1 - s_j^*)p_j^*\mu - \delta(ps_j^*T)^2 - (\lambda T(1 - s_j^*)p_j^*\mu^2 + a_j s_j^{*2}T^2 + b) \\ &= \frac{1}{2}\gamma T(1 - s_j^*)p_j^*\mu - \lambda\mu^2 T(1 - \frac{1}{2}s_j^*)p_j^* - b \\ &= \frac{\gamma\mu^2}{2\delta}\left[(\frac{1}{2}\gamma - \lambda\mu) - \frac{1}{2}(\gamma - \lambda\mu)s_j^*\right]\frac{1 - s_j^*}{s_j^{*2}} - b. \end{aligned}$$

Since $\gamma < \lambda\mu$, $W_j - Z_j$ is increasing in s_j^*. Proposition 1 implies that s_j^* is decreasing in a_j and thus $W_j - Z_j$ is decreasing in a_1. Q.E.D.

Proof of Proposition 2.

The equation for the marginal client t^*, (13), and the equations for prices, (16) and (17), determine that

$$t^* = \frac{1}{2}(1 + (W_1 - W_2) - (P_1^* - P_2^*)) = \frac{1}{2}[1 + \frac{1}{3}(W_1 - W_2 - (Z_1 - Z_2))]. \tag{A4}$$

As before, we focus on the interior solution $t^* \in (0, 1)$ for brevity. The equations (16), (17), and (A4) ensure that when the auditors charge P_1^* and P_2^*, respectively, any client $u \in [0, t^*)$ chooses auditor A_1 and any client $u \in (t^*, 1]$ chooses auditor A_2. The endogenous market shares (or sizes) of the auditors in the equilibrium are $m_1 = t^*$ and $m_2 = 1 - t^*$. Therefore, this gives rise to a unique equilibrium. The equilibrium market share of auditor j can also be written as

$$m_j^* = \frac{1}{2}\left(1 + \frac{1}{3}(W_j - W_{-j} - Z_j + Z_{-j})\right). \tag{A5}$$

The profit of auditor j is then

$$\Pi_j = m_j^*(P_j^* - Z_j) = \frac{1}{2}\left(1 + \frac{1}{3}(W_j - W_{-j} - Z_j + Z_{-j})\right)^2 = \frac{1}{2}\left(1 + \frac{1}{3}(W_j - Z_j - (W_{-j} - Z_{-j})\right)^2.$$

The key quantity in equation (A4) is $W_i - Z_i$. From (10) and (11) and Proposition 1, we have

$$\begin{aligned} W_i - Z_i &= \frac{1}{2}\gamma T(1 - s_i^*)p_i^*\mu + \lambda\mu^2 T(1 - \frac{1}{2}s_i^*)p_i^* \\ &= \frac{1}{2}Tp_i^*\mu(\gamma(1 - s_i^*) - \lambda\mu(2 - s_i^*)) \\ &= \frac{\gamma\mu^2}{4\delta}\frac{1 - s_i^*}{s_i^{*2}}(\gamma - 2\lambda\mu - (\gamma - \lambda\mu)s_i^*). \end{aligned} \tag{A6}$$

where we used the equation $p_i^* = \frac{\gamma\mu(1-s_i^*)}{2\delta T s_i^{*2}}$. Proposition 1 implies that s_i^* decreases with a_i. Since $0 \le s_i^* < 1$ and $\gamma < \lambda\mu$, $\gamma - 2\lambda\mu - (\gamma - \lambda\mu)s^*$ decreases with s_i^*. Therefore, $W_i - Z_i$ decreases with s_i^*, and increases with a_i. Therefore, from (A5), m_j^* decreases with a_j. In other words, each auditor's market share/size depends positively with skill $1/a_i$.

Q.E.D.

Proof of Proposition 3. We first formalize the intuition about the equilibria delineated in the main text. For convenience, we introduce the following notations. Let $s_{j,T}, p_{j,T}$ be the solution to the equilibrium conditions for auditor j when transaction volume is T; in other words, they satisfy

$$\begin{aligned} p_{j,T} &= \frac{\gamma\mu(1 - s_{j,T})}{2\delta s^2 T}, \\ s_{j,T} &= \frac{\lambda p_{j,T}\mu^2}{2a_j T}. \end{aligned}$$

Recall from the proof for Proposition 1 that $s_{j,T}$ is the solution to the following equation

$$4a_j\delta T^2 s_{j,T}^3 = \lambda\gamma\mu^3(1 - s_{j,T}). \tag{A7}$$

Define $W_j(T)$ and $Z_j(T)$ as the second-stage utilities of the client and auditor, respectively. In

other words,

$$W_j(T) = \gamma T(1 - s_{j,T})p_{j,T}\mu - \delta(p_{j,T}s_{j,T}T)^2 = \frac{\gamma^2\mu^2(1 - s_{j,T})^2}{4\delta s_{j,T}^2}, \tag{A8}$$

$$Z_j(T) = \lambda(1 - s_{j,T})Tp_{j,T}\mu^2 + as_{j,T}^2T^2 + b = \frac{\lambda\gamma\mu^3(1 - s_{j,T})^2}{2\delta s_{j,T}^2} + \frac{\lambda\gamma\mu^3}{4\delta}\frac{1 - s_{j,T}}{s_{j,T}} + b. \tag{A9}$$

We also define $CU_j(T) = W_j(T) - Z_j(T)$ as the client utility in the first-stage equilibrium except the auditor preference term. We note that from Proposition 1, $W_j(T)$ and $Z_j(T)$ are decreasing in $s_{j,T}$ and increasing in a_j and T. If $\gamma < \lambda\mu$, then by (A6) and Proposition 1, $CU_j(T)$ is increasing in $s_{j,T}$ and decreasing in a_j and T.

We use $T_2 = KK_{pr}$, $T_1 = K(K + K_{pr})$, and $T_0 = 2K^2 + KK_{pr}$ to represent the number of transactions associated with an auditor that need to be manually verified when both auditors adopt blockchain, when only the given auditor adopts blockchain, and when no auditor adopts blockchain (or when only the other auditor adopts blockchain), respectively. It is clear that $T_2 < T_1 < T_0$ and therefore $CU_j(T_2) > CU_j(T_1) > CU_j(T_0)$, indicating that blockchains increases the first-stage values for clients if we do not consider adoption costs.

No Adoption Equilibrium We first consider conditions under which the no adoption equilibrium exists. Without blockchains, both auditors has to verfiy T_0 transactions per client. If one auditor deviates to adopt blockchain, then it only needs to verify T_1 transactions. From (19), the auditor's no deviation conditions are, for $j = 1, 2$,

$$\frac{d}{2}\left[1 + \frac{1}{3d}(CU_j(T_0) - CU_{-j}(T_0))\right]^2 \geq \frac{d}{2}\left[1 + \frac{1}{3d}(CU_j(T_1) - c_2 - CU_{-j}(T_0))\right]^2 - c_1. \tag{A10}$$

It is clear that if the cost c_1 or c_2 is sufficient large, the above condition holds for $j = 1, 2$ and no adoption would be an equilibrium.

Full Adoption Equilibrium When both auditors adopt blockchain, the no deviation conditions are, for $j = 1, 2$,

$$\frac{d}{2}\left[1 + \frac{1}{3d}(CU_j(T_2) - CU_{-j}(T_2))\right]^2 - c_1 \geq \frac{d}{2}\left[1 + \frac{1}{3d}(CU_j(T_0) - CU_{-j}(T_1) + c_2)\right]^2. \tag{A11}$$

Partial Adoption Equilibrium Assume there is a partial adoption equilibrium where auditor j adopts the blockchain, and auditor $-j$ does not. For the partial equilibrium to hold, there are two no deviation conditions. First, auditor j does not deviate to non-adoption,

$$\frac{d}{2}\left[1+\frac{1}{3d}(CU_j(T_1)-c_2-CU_{-j}(T_0))\right]^2-c_1\geq\frac{d}{2}\left[1+\frac{1}{3d}(CU_j(T_0)-CU_{-j}(T_0))\right]^2. \tag{A12}$$

Second, auditor $-j$ does not deviate to adopt blockchain,

$$\frac{d}{2}\left[1+\frac{1}{3d}(CU_{-j}(T_0)-CU_j(T_1)+c_2)\right]^2\geq\frac{d}{2}\left[1+\frac{1}{3d}(CU_{-j}(T_2)-CU_j(T_2))\right]^2-c_1. \tag{A13}$$

We note that (A10) and (A12) cannot simultaneously hold (except in the knife-edge case when both equality hold). Therefore, no adoption and partial adoption equilibria cannot coexist. Similarly, (A11) and (A13) cannot hold at the same time and thus full adoption and partial adoption equilibria cannot coexist as well.

For existence of the partial equilibrium, we first consider the case $a_1 = a_2$, or when the two auditors are symmetric. Given the symmetry,

$$CU_j(T_0)=CU_{-j}(T_0), CU_{-j}(T_2)=CU_j(T_2).$$

Therefore, (A12) and (A13) simplify to

$$\begin{aligned}\frac{d}{2}(1+e)^2-c_1&\geq\frac{d}{2},\\ \frac{d}{2}(1-e)^2&\geq\frac{d}{2}-c_1.\end{aligned}$$

where $e=\frac{1}{3d}(CU_1(T_0)-c_2-CU_2(T_1))$. Therefore, both partial equilibria exist when

$$\frac{d}{2}(2e-e^2)<c_1<\frac{d}{2}(2e+e^2). \tag{A14}$$

For a_1 and a_2 sufficiently close, if (A14) holds, equations (A12) and (A13) are only slightly perturbed and thus the partial equilibria still exist.

By Proposition 2, the market share of the blockchain adopting auditor j is

$$\frac{1}{2}\left(1+\frac{1}{3d}(CU_j(T_1)-c_2-CU_{-j}(T_0))\right).$$

If c_2 is sufficiently small, the above is greater than the market share of auditor j in the no adoption equilibrium

$$\frac{1}{2}\left(1+\frac{1}{3d}(CU_j(T_0)-CU_{-j}(T_0))\right)$$

because $CU_j(T_1) > CU_j(T_0)$. Since $W_j(T)$ and $Z_j(T)$ are increasing in T, the auditing fee charged by auditor j in the partial equilibrium is equal to $P_j^*(T_1) = d + \frac{1}{3}(W_j(T_1) - W_{-j}(T_0) + 2(Z_j(T_1) + c_2) + Z_{-j}(T_0))$, which is smaller than auditing fee in the no adoption equilibrium $P_j^*(T_0) = d + \frac{1}{3}(W_j(T_0) - W_{-j}(T_0) + 2Z_j(T_0) + Z_{-j}(T_0))$ if c_2 is sufficiently small. Finally, the misreporting probability in the partial equilibrium $p_j^*(T_1) < p_j^*(T_0)$ by comparative statics in Proposition 2. In the full adoption equilibrium, the auditing fee is

$$\begin{aligned}P_j^*(T_2) &= d+\frac{1}{3}(W_j(T_2)-W_{-j}(T_2)+2(Z_j(T_2)+c_2)+Z_{-j}(T_2))\\ &\leq d+\frac{1}{3}(W_j(T_1)-W_{-j}(T_0)+2(Z_j(T_1)+c_2)+Z_{-j}(T_0)) = P_j^*(T_1),\end{aligned}$$

where we used the fact that W_j, Z_j and $-(W_{-j} - Z_{-j}) = -CU_j$ are increasing in T. The reporting probability also satisifies $p_j^*(T_2) < p_j^*(T_1)$ by the same argument as above. Q.E.D.

Proof of Corollary 1. In the independent blockchain equilibrium, the number of transactions that remains to be verified is equal to T_1. Since $T_0 > T_1 > T_2$, the results follow from the proof in Proposition 3.

Proof of Proposition 4. We use the notations from the proof of Proposition 3. Since $a_1 = a_2$, the full adoption conditions reduce to a single equation

$$\frac{d}{2}-c_1 \geq \frac{d}{2}\left[1+\frac{1}{3d}(CU_1(T_0)-CU_2(T_1)+c_2)\right]^2,$$

or equivalently,

$$c_1 \leq \frac{d}{2}-\frac{d}{2}\left[1+\frac{1}{3d}(CU_1(T_0)-CU_2(T_1)+c_2)\right]^2.$$

Note that $CU_1(T_0) < CU_1(T_1) = CU_2(T_1)$. Given the symmetry, we omit the subscripts for the auditor below. Therefore, if c_2 is sufficiently small, $C_2 = \frac{d}{2} - \frac{d}{2}\left[1 + \frac{1}{3d}(CU(T_0) - CU(T_1) + c_2)\right]^2 > 0$ and the full adoption equilibrium exists when $c_1 \leq C_2$.

Given the symmetry between the auditors, the social welfare in the full adoption case is

$$SW_b = R(T_2) + c_2 + 2c_1.$$

and the social welfare without blockchain is $SW_0 = R(T_0)$. Therefore,

$$SW_b - SW_0 = R(T_2) - R(T_0) + c_2 + 2c_1 > 0$$

if

$$c_1 < C_1 = \frac{1}{2}(R(T_0) - R(T_2) - c_2).$$

Since $R(T_0) > R(T_2)$, C_1 is positive if c_2 is sufficiently small.

We now compare C_1 and C_2. Since $W(T)$ and $R(T)$ are decreasing in T (see proof of Proposition 3) and $T_0 > T_1 > T_2$,

$$\begin{aligned} CU(T_1) - CU(T_0) &= W(T_1) - W(T_0) + R(T_0) - R(T_1) \\ &\leq R(T_0) - R(T_1) \leq R(T_0) - R(T_2). \end{aligned}$$

Therefore, if c_2 is small,

$$\begin{aligned} C_1 &= \frac{1}{2}(R(T_0) - R(T_2) - c_2) > \frac{1}{3}(CU(T_1) - CU(T_0) + c_2) \\ &\geq \frac{1}{3}(CU(T_1) - CU(T_0) + c_2) - \frac{2}{9d}(CU(T_1) - CU(T_0) + c_2)^2 = C_2. \end{aligned}$$

Thus in the interval $c_1 \in (C_2, C_1)$, full adoption is socially optimal but not an equilibrium. In this case, a regulator can make a subsidy $s > 0$ to each auditor with the condition that both auditors have to adopt blockchain to receive the subsidy. The subsidy size can be determined so that the full adoption conditions hold with equality, i.e.,

$$s = C_1 - c_1.$$

This will thus make full adoption an equilibrium and achieves the social optimum.