Financial Reporting and Blockchains: Audit Pricing, Misstatements, and Regulation

Sean Cao, Lin William Cong, and Baozhong Yang*

First Draft: Aug 2018; This Draft: June 2019

Abstract

To understand the implications of decentralized ledger technology for financial reporting and auditing, we analyze auditor competition, audit quality, client misstatements, and regulatory policy in a unified framework. We demonstrate how collaborative auditing using a federated blockchain can improve verification efficiency for not only transactions recorded on auditors or clients' proprietary databases, but also cross-database verifications through zero-knowledge protocols that preserve client privacy. Consequently, the technology disrupts conventional audit pricing and effort focus: auditors' competitive fees depend on clients' counter-parties' characteristics and corresponding transaction volume instead of client size; blockchains also reduce clients' incentives to misreport and auditors' sampling costs, allowing auditors to reallocate effort from transaction-based auditing to discretionary account auditing. Importantly, auditors' technology adoption is costly and exhibits strategic complementarity, hence a regulator can help select an equilibrium with lower endogenous misstatements, audit sampling, and regulatory costs. Our study also demonstrates how permissioned blockchains innovate over existing database technologies.

JEL Classification: D21, D40, M42, M48
Key Words: Auditor Risk and Sampling, Collaborative Auditing, FinTech, PCAOB, Permissioned Blockchains, RegTech, Technology Adoption, Zero-Knowledge Proof.

*Cao is with the J. Mack Robinson College of Business at Georgia State University (Email: scao@gsu.edu). Cong (contact author) is with the Booth School of Business at the University of Chicago (Email: will.cong@chicagobooth.edu). Yang is with the J. Mack Robinson College of Business at Georgia State University (Email: bzyang@gsu.edu). The authors thank Pingyang Gao, Jiasun Li (Discussant), Bob McDonald (Discussant), Venky Nagar (Discussant), Fahad Saleh (Discussant), Haresh Sapra, and Larry Wall (Discussant) for detailed feedback and discussion. They also thank Vikas Agarwal, Mark Chen, Alisa DiCaprio, Matthew DeAngelis, John Hameling, Dalida Kadyrzhanova, Yongtae Kim, W. Robert Knechel, Anya Kleymenova, Clive Lennox, Roni Michaely, James ("Robbie") Moon, Jr., Curtis Mullis, Mark Peecher, Lin Peng, Shivaram Rajgopal, Ajay Subramanian, Lawrence J. White, Baohua Xin, Mao Ye, Hongda Zhong, and participants at Ant Financial Workshop, Baidu Du Xiaoman Financial, DataYes & ACM KDD China FinTech×AI Workshop, Eastern Finance Association Meeting, Federal Reserve Bank of Atlanta Conference on New Technologies and Financial Stability, Geneva Finance Research Institute, Geneva Finance Research Institute, Georgia State University Workshops at the Departments of Accountancy, Computer Science and Finance, JD.com JDD (Financial Arm), University of Minnesota Accounting Department, NBER Conference on Blockchains, Distributed Ledgers, and Financial Contracting, PCAOB/JAR Conference on Auditing and Capital Markets, and SFS Cavalcade at Carnegie Mellon University for constructive comments. The authors gratefully acknowledge research support from the FinTech Lab at J. Mack Robinson College of Business at Georgia State University and from the Center for Research in Security Prices at the University of Chicago.

1. Introduction

Unbiased financial reporting is crucial in financial markets and regulatory agencies such as the Public Company Accounting Oversight Board (PCAOB) have constantly sought ways to improve financial reporting quality and audit efficiency. One main cost in ensuring quality reporting comes from auditors' verification of clients' transactions with their counterparties. While each audit firm or team (generically referred to as "auditor") may possess information useful to other auditors, each one's traditionally audit independently because it is not customary to share proprietary information among audit firms—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 (e.g., General Data Protection Regulation). In practice, auditors contact transaction counterparties for verification either manually or through an outsourced third party who may have misaligned incentives in ensuring auditing quality. Despite strong demands for cross-auditor verification, its labor-intensive nature leads to inefficient allocation of auditor effort to mechanical transaction verification. Consequently, audit firms devote less effort than what is socially efficient to auditing discretionary accounts which entails larger value added, reducing firms' endogenous quality of financial reporting.

Meanwhile, decentralized ledger/database technology, especially blockchains, have taken the central stage of technology innovation in business. It is widely believed to allow industry-wide collaboration (e.g., R3) and disrupt corporate governance, industrial organization, payments, and entrepreneurial finance (e.g., Cong and He 2018). Among the various advances, "one theoretical application of blockchain is to financial reporting and this is exactly the point in time to discuss advantages and disadvantages" (Campbell Harvey, FEI 2018). Yermack (2017) also suggests that blockchain technologies could affect financial reporting by replacing the role of double-entry bookkeeping used for centuries. In particular, media and industry are increasingly paying attention to blockchain applications in auditing. Although all Big 4 audit firms are aware of the importance of blockchain and devoting large resources to its

development by establishing research labs or providing blockchain services (e.g., Bajpai 2017, Vetter 2018, Zhao 2018), it is still unclear how exactly blockchains may affect the auditing industry and what auditors' new role would be with the emerging technology.[1] Many also hold the opinion that permissioned blockchains used in such settings present no fundamental innovation because it lacks decentralized access and the use of a native cryptocurrency.

We take an initial step towards understanding these issues by examining how permissioned blockchains disrupt traditional audit processes and enable auditor collaboration without sacrificing client data privacy. In particular, we analyze two important aspects of financial reporting: firms' endogenous misstatements and auditors' monitoring/inspection of financial reports. We aim to contribute in three dimensions. (1) We detail the functionality of a collaborative audit process, which capitalizes on a federated blockchain and zero-knowledge proof for automated auditing of transaction-based accounts (e.g., accounts receivable/payable). (2) Given such technological functionality, we characterize the equilibrium outcomes concerning auditor competition, audit pricing and sampling, clients' endogenous misstatements, and regulatory policy in a unified framework to delineate the implications of blockchain technology adoption for auditors, clients and regulators. (3) In particular, our findings inform policy discussions on the *coordination* role of a regulator for new technology adoption and the impact of blockchain on (PCAOB) regulatory costs.

Auditing differs from many other industries affected by blockchain technology, such as digital payments or trade finance. While public blockchains can provide more transparency and open access, they are not suitable in settings where client information needs to stay private. Consequently, many auditors are exploring blockchains and their applications as

[1]Cohn (2016) reports that big 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; EY partnered with Accenture and PwC advises clients on various uses of the blockchain technology (Karajovic, Kim, and Lasksowski, 2017). The industry has organized symposiums (e.g., the Blockchain in Accounting Symposium by AICPA and Wall Street Blockchain Alliance, and KPMG's 28th Annual Accounting & Financial Reporting Symposium in 2018) and published research reports (e.g., CPA Canada, AICPA, and University of Waterloo 2018). Auditors can either develop new technologies to audit clients' blockchains or develop their own private blockchains to help their audit process (e.g., Tysiac 2018). Recent efforts of accounting firms center on buiding in-house blockchain capabilities and services (e.g. Bajpai 2017, CNN 2018).

discussed above. What is left out of the discussion is the possibility to connect isolated audit processes across firms while preserving data privacy. Examining records from both parties in a transaction is an efficient way of validating a record in the auditing process, because any inconsistency in transaction information between the two parties immediately suggests unintentional errors or intentional misstatement. Such cross-party verification is costly in the traditional system where an auditor has to contact the transaction counterparty directly to request records and manually confirm with clients' transaction parties.

Permissioned blockchains, as a form of distributed ledger technology, feature distributed infrastructure for distributed data synchronization, encryption, and storage with decentralized consensus, immutability, and privacy. These features allow auditors to collaborate to automate information verification of clients' transactions with minimal sharing of clients' private information.[2] For example, thanks to blockchain's peer-to-peer (within a consortium) design, this collaboration among auditors does not require a centralized third party to monitor or intermediate. In addition, the encryption methods such as zero-knowledge proof also allow information providers in a federated blockchain system to safeguard proprietary client information while verifying transactions.[3] Such zero-knowledge proof/protocols have been well-developed and have led to recent applications in bank communications (ING, 2018) and in public blockchains such as Zcash and Ethereum.[4] Furthermore, the immutable nature of blockchain also makes it easier for the regulator to inspect auditing processes and

[2]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. 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.

[3]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 is advertised as "the Internet of transactions" (Mearian 2018).

[4]Zcash is a cryptocurrency that preserves user anonymity based upon a zero-knowledge proof algorithm, zkSNARK. Ethereum added zkSNARK algorithm support in one of its recent updates, Byzantium, in 2017. Ethereum, Hyperledger, and R3 CEV provide ready-to-use protocols and source codes.

prevent audit firms or hackers from revising recorded transaction data ex post (Section 2 contains more details). Overall, federated blockchains using zero-knowledge protocol can enable collaborative auditing and make the auditing process more efficient and reliable for detecting fraud. That said, adopting a blockchain system incurs indirect costs of potentially losing clients who prefer less stringent auditing, as well as direct costs of set-up and standardization.

We take the above blockchain functionalities as given and examine how auditors and clients respond to the technology. Specifically, our model features two auditing firms and two representative clients. Without blockchains, auditing firms compete for clients on the basis of fees and auditing services they perform. Once a client is matched with an auditor, the client 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 auditing quality (represented by auditing sample size) to minimize auditing costs and the expected penalty when its clients' misreporting is detected. In equilibrium, auditors offer competitive fees, and larger firms with larger transaction volume face greater misstatement risk and higher auditing fees.

When an auditor adopts a blockchain system, the auditing costs of transactions among clients within the auditor are significantly reduced, but auditing transactions across auditors remains costly if other auditors do not adopt a blockchain system or the blockchain systems are all independent. That said, with a federated blockchain, two auditors who have their clients' transaction information and are both using blockchains can verify transactions with little cost, thanks to the zero-knowledge proof algorithm. This also implies that a federated blockchain can disrupt auditing pricing: instead of being largely based on clients' total transaction size, audit price also crucially depends on the nature of transaction counterparties—the number of transactions clients have with firms who are not in a federated blockchain, such as foreign/private firms or retail customers, would drive the cost.

Even though we focus on the audit of transaction-based accounts, the reduction in

auditing costs with the new technology has a spillover effect on discretionary accounts where soft information and auditors' expertise play indispensable roles. We discuss how a federated blockchain enables auditors to reallocate efforts from transaction-based auditing to focus more on discretionary account auditing, which has been the most challenging for audit firms. In addition, the technology potential disrupts audit labor market because it reduces demand for mechanic audit work and increases demand for skilled auditors. On the client side, when both auditors adopt blockchains, clients report more truthfully for both transactions recorded on blockchains and discretionary accounts, leading to lower auditor risk and lower overall audit cost.

The auditors' technology adoption exhibits strategic complementarity because the cost of auditing cross-auditor transactions decreases when more auditors adopt. When clients strongly value the benefit of misreporting even after taking into consideration the possibility of being detected, they would prefer to work with auditors not using blockchain, notwithstanding that the auditor using blockchain can offer a lower auditing fee. Consequently, when other auditors are not adopting, an auditor would not find it profitable to adopt because adoption would not only fail to attract more clients, but also could result in losing clients that the auditor would get with traditional auditing. In this regard, the cost of adopting the technology entails both a direct setup expense and an indirect cost in the competition for client firms. That said, if other auditors are adopting, an auditor would find it attractive to adopt after gaining new clients because the reduction in auditing costs outweighs the adoption cost.

Given that there could be both a full-adoption equilibrium and a no-adoption equilibrium, regulators such as the PCAOB can potentially coordinate an industry-wide adoption when the technology is sufficiently mature, which could reduce equilibrium misstatements and expenses associated with auditing and regulation. This role is especially salient when auditing firms and clients are dispersed or lack coordination. While the concept of coordination is well-studied, our model entails a price competition preceding technology adoption

decisions, which is new and enriches the interactions among auditors. Moreover, we are the first to highlight how coordination issues manifest in auditors' adoption of blockchain technology, which has important practical implications.

In sum, our study documents how blockchains could disrupt auditing industries. First, blockchains make audit pricing dependent on the nature and volume of transaction counterparties instead of clients' total transaction size. Second, such technology improves the efficiency of audit sampling by allowing auditors to focus on transactions that cannot be automatically verified. Third, adopting the technology discourages client misstatements. Fourth, regulators benefit from reduced monitoring costs given that they can focus on smaller samples for inspections (See Figure 4), and auditors or hackers find it more difficult to tamper with transaction records. Finally, given the costs of adoption and strategic behaviors of market participants, our theory suggests that auditors and clients are less likely to adopt such technology themselves even when it is socially beneficial to do so. But regulators can coordinate the technology adoption in order to reduce equilibrium misstatements and costs associated with auditing and its regulation.

It is worth noting that the strategic complementarity in technology adoption distinguishes our model from those examining the implications of a general technology on cost reduction. Relative to other models of technology adoption with network effects, we also differ in allowing an endogenous pricing competition among the firms. We model federated blockchains with zero-knowledge proof as a leading candidate for effectively improving privacy protection and cross-party verification in a decentralized system. Compared with traditional centralized databases, our proposed permissioned blockchain framework not only allows firms to enjoy the benefits of decentralization and security due encryption and immutability, but also is ripe for implementation.[5]

Literature — Our paper contributes to the emerging literature on FinTech and blockchain.

[5]We benefited from discussion with Alisa Dicaprio, R3 representative at the NBER meeting: R3 has developed ready-to-use permissioned blockchain infrastructure that can integrate with clients' ERP systems with reasonable adoption cost. Data integration between audit firms and their clients can also be done with read-to-use technology.

Most prior studies, such as Cong, He, and Li (2018), Alsabah and Capponi (2019), and Easley, O'Hara, and Basu (2018), focus on public blockchains. Cong and He (2018) study information distribution in generating decentralized consensus that could be permission-based, while Hinzen, John, and Saleh (2019) discuss overcoming scalability limitations using a permissioned blockchain. None of the studies analyze transparency issues potentially mitigated by zero-knowledge-proof, which Goldwasser, Micali, and Rackoff (1989) and Rackoff and Simon (1991) introduce.

Concerning blockchain applications, Halaburda and Sarvary (2015) and Harvey (2016) discuss digital currencies and crypto-finance. Yermack (2017) evaluates the technology's potential impacts on corporate governance. Cong, Li, and Wang (2018) introduce a dynamic pricing framework of cryptocurrencies and highlight the roles of crypto-tokens on endogenous platform adoption. Cong (2018) surveys recent blockchain research and discusses blockchain implications for investment professionals. A number of studies such as Chod and Lyandres (2018) discuss initial coin offerings. Falk and Tsoukalas (2019) examine token-weighted voting for crowdsourcing information in various blockchain-based applications. Chod et.al. (2019) 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.

To the best of our knowledge, we are the first to study the implementation of blockchains and zero-knowledge proof algorithms in auditing and accounting, and their implications for auditor pricing, auditor sampling, client incentives for misstatement, and regulation.[6] We differ from earlier studies in our focus on permissioned blockchains and in jointly analyzing the auditor competition and adoption games. Doing so highlights for the first time in the literature that even without free entry as seen in public blockchains or the introduction

[6]Narula, Vasquez and Virza (2018) describe a query-based auditing process based on ZKP; Wang and Kogan (2018) also point out the possibility of using blockchain and ZKP to process transactions on blockchains while preserving confidentiality. Unlike their proposals to either have independent blockchain/database for auditing or to have all firms adopt blockchain and convert corporate assets into cryptoassets for implementation, we only require recording certain transactions on a blockchain and underscore economic issues such as endogenous adoption and auditor competition.

of cryptocurrencies/tokens, permissioned blockchains can have novel economic impacts that economists thus far often dismiss.[7] We also lay out a framework for future studies, especially empirical tests of our model predictions, when the technology sees wider adoption and data become available.

Our study thus also 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, Shibano 1990, Patterson 1993), internal control and testing (Smith, Tiras, and Vichitleckarn 2000), earnings reports and auditing (Newman, Patterson, and Smith 2001), uncertainty about materiality standards (Patterson and Smith 2003), investor protection and auditing (Newman, Patterson, and Smith 2005), joint auditing and quality (Deng et al. 2014), and legal systems and auditing (Simunic, Ye, and Zhang 2017). Several theoretical studies 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, Magee and Tseng 1990, Teoh 1992, and Lu 2006). We contribute by highlighting how decentralized ledger technologies disrupt the industry and prior results.

In particular, our paper sheds light on how accounting data and their management affect the behavior of firms and firms' monitors/regulators. Among seminal studies, Caskey, Nagar, and Petacchi (2010) consider manager's financial reporting in the presence of auditors and investors simultaneously. We model investors' valuation of the firm as a reduced-form payoff given a firm's misstatement, but instead add a regulatory body of auditors. Petacchi and Nagar (2016) study multiplicity of reporting equilibrium when a regulator (equivalent to

[7]For example, some question whether blockchains maintained by central authorities should be called blockchains at all because they merely represent better data-management processes (Schoenberger 2018). Permissioned blockchains, in contrast, are typically maintained by industry consortia and thus allow a certain degree of decentralization. More importantly, they provide the infrastructure for proprietary databases to interact. Alex Pentland, the founder of MIT Media Lab and one of the most prominent data scientists in the world, was quoted as aptly remarking, "[With blockchains, now] you can get insights across countries, across data holders, without exposing individual data and without disobeying either privacy or data localization laws." (Pillar 2018)

an auditor in our setting) is resource constrained. Our model features two representative client firms and abstracts away client firms' coordination. Instead, we focus on the strategic complementarity of technology adoption by auditors.

The rest of the paper proceeds as follows. Section 2 introduces the institutional details of auditing, blockchains, and zero-knowledge proof. Section 3 sets up the model and characterizes the equilibria with and without blockchains. Section 4 analyzes regulation and policy. Section 5 extends the model to incorporate discretionary accounts and discusses alternative model specifications. Section 6 concludes. Appendix A contains a detailed introduction to permissioned blockchains and zero-knowledge proofs. Appendix B includes all the proofs.

2. Institutional Background

In this section, we explain the basic auditing process of transaction-based (simple revenue and transaction records), non-discretionary accounts and how a federated blockchain can facilitate collaborative auditing against the backdrop of privacy concerns without a central facilitating agency. Along the way, we also provide a primer on the use of permissioned blockchains and the concept of zero-knowledge proof.

Suppose client firms' income statements are as shown in Figure 1.[8] Auditors' primary job is to verify the accuracy of net income and prevent the occurrence of restatement. To this end, auditors need to verify their cilents' sales and expenses. Clients have incentive to overstate their sales and understate their expenses to gain favorable valuation and treatment in capital markets; i.e., higher stock prices or lower financing costs (Strobl 2013). Auditors have different ways to verify the accuracy of sales and, in our simplified case, accounts receivable and related invoices. They can rely on the historical pattern of accounts receivable, industry peer firms' concurrent accounts receivable, or the growth pattern of other highly related asset growth such as inventory to estimate accounts receivable errors. One common

[8]We focus on transaction-based accounts here. We also do not include cash receipts because they are easily verified.

feature of these approaches is that all the information is provided by the clients, who have incentives to overstate.

One way to mitigate this potential information bias 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). Such 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 verification is costly in the traditional system, where an auditor has to contact the transaction counter-party directly to request records and manually verify the information.[9]

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 demonstrates how a federated blockchain with a zero-knowledge proof/protocol can facilitate collaborative auditing and cross-party verification.[10] In a federated blockchain, each auditor operates a private blockchain for its clients or has access to the blockchain ecosystem of its clients. In the base scenario, each node on the private blockchain is administered by a team of the auditing firm. We note that permissioned blockchains considered for business applications typically only allow permissioned parties to join, use an efficient

[9] Auditors can also outsource such labor-intensive cross-party verification to a third party such as confirmation.com, as discussed in the introduction.

[10] See Appendix A for a more detailed introduction to zero-knowledge proofs and their applications.

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. 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 are recorded on the private blockchain. Records on the private blockchains are synchronized on all the nodes to ensure immutability. On the private blockchains, only permissioned nodes can manage records and the nodes usually adopt a majority consensus that is efficient and scalable, avoiding the costly mining process associated with public blockchains with proof-of-work protocols. Transactions between parties associated with different auditors, or *cross-auditor* transactions, utilize a cryptographic verification method(i.e., zero-knowledge proof) that allows confirmation on the federated blockchain without revealing proprietary information.

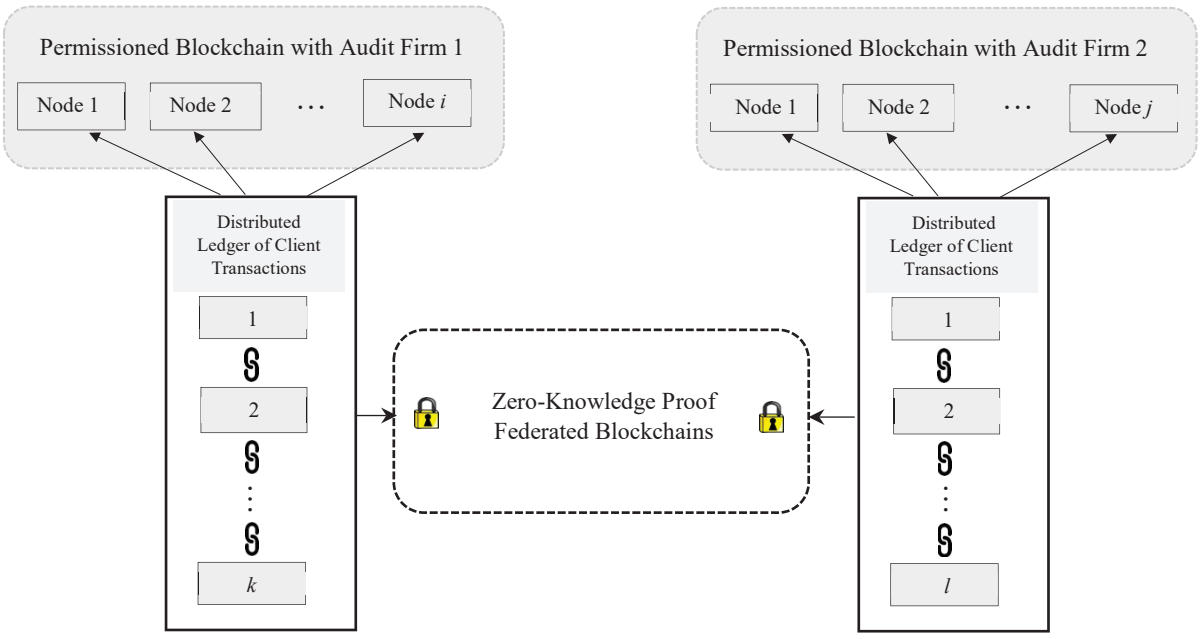

Figure 2: **Structure of the Federated Blockchain**

We illustrate the transaction verification process on the federated blockchain in Figure 3. A *zero-knowledge proof/protocol* is a cryptographic algorithm by which one party (prover)

can prove to another party that she knows a value x, without conveying any information apart from the fact that she knows the value x. In particular, the prover does not need to reveal the value x.[11] As shown in Figure 3, for a transaction between two client firms audited by different audit firms, the verification occurs on the federated blockchain. The first auditor sends a request to the blockchain that can only be confirmed by the second auditor, who works with the counterparty of the transaction. When both the request and confirmation are encrypted without revealing client-specific information (e.g., by following a zero-knowledge proof/protocol), no other auditors 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.

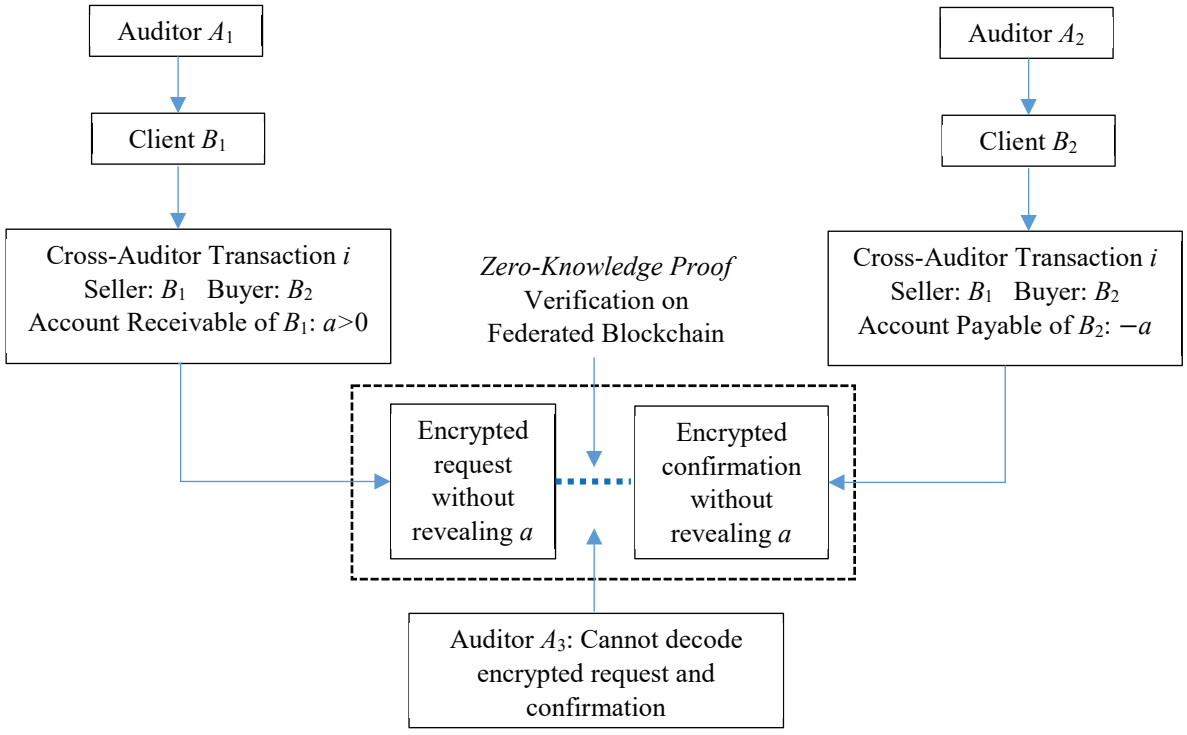

Figure 3: **Transaction Verification on a Peer-to-Peer Federated Blockchain**

[11]Some zero-knowledge protocols, such as the zero-knowledge range proofs by ING, can help to verify whether a number is within a given range without revealing the number. See, for example, Allison (2018).

Such a federated blockchain framework can facilitate two types of collaborative auditing, as demonstrated in Figure 4. Type 1 concerns within-auditor transactions; that is, the two parties in the transaction are audited by the same auditing firm but by different auditing teams. But auditor teams may be located remotely in different audit offices, leading to high communication costs. A private 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 audit firms, each residing in a separate blockchain ecosystem. The federated blockchain with zero-knowledge proof algorithms can facilitate automatic information sharing between auditors with consideration of clients' information privacy.

An additional case involves *off-chain* transactions in which a client's transaction counterparty is not on the blockchain, for example, when it is a private or foreign firm that is unaudited. Even with blockchains, auditors still need to conduct conventional auditing procedures for the sample of off-chain transactions. However, this sample is typically a small fraction of the entire 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 party; (ii) encryption: the zero-knowledge proof method allows encrypted communication that preserves data privacy; (iii) immutability: once auditors request information through the federated blockchain, it is difficult for any auditors or outside hackers to intentionally revise or delete the information, unless they can revise information on a majority of nodes on the federated blockchain. In Section 3, we analyze the implications of this federated blockchain for auditors, clients, and regulators.

Finally, 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. In that sense, it does not necessarily belong to a particular auditor and 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 the blockchain systems support transactions directly, rather than being an add-on data system requiring an interface to existing transaction and reporting databases. However, building and maintaining the infrastructure could represent significant costs to individual firms, as discussed in Wang and Kogan (2018). We also remark that in addition to zero-knowledge proof, alternative algorithms such as homomorphic encryption could also be combined with the federated blockchain infrastructure.

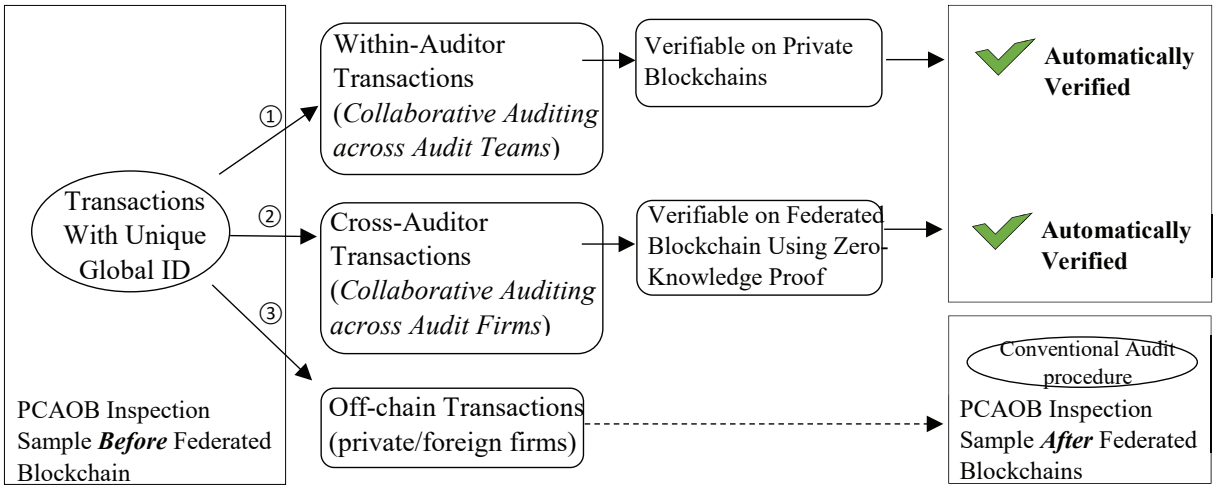

Figure 4: **Auditing Transactions with the Blockchain**

3. A Model of Auditing and Blockchains

3.1. Auditing in the Traditional World

We consider an economy with two representative firms, B_1 and B_2 (or two groups of representative firms), of sizes K_1 and K_2 respectively. The total amount of transactions among these firms scales with the size of the business, and is given by $(K_1 + K_2)^2$. Firm B_i would

report K_i^2 internal transactions and $K_i K_{-i}$ cross-firm transactions. Each firm also reports $K_i K_{pr}$ transactions with unaudited firms, such as private or foreign firms. There are two auditing firms, A_1 and A_2. For simplicity, we assume homogeneous auditors.[12] In particular, $K_1 = K_2$. Client heterogeneity does not change our main mechanisms.

The game starts with the auditors offering an auditing price, and clients each choosing an auditor. Once the clients and auditor firms are matched, the client chooses the probability of overstatement while the auditor chooses the intensity of auditing (which corresponds to auditing quality or misstatement level). We solve the model backward and first analyze the second stage of the game, wherein a client is already matched to an auditor.

Specifically, suppose one client has chosen an auditor and reports a continuum of transactions $i \in [0, T]$. T represents the transaction volume. Each transaction i has a true value of $\tilde{a}_i \in (-\infty, \infty)$. For example, accounts receivable and accounts payable items correspond to $\tilde{a}_i > 0$ and $\tilde{a}_i < 0$ respectively. The true aggregate income of the client for a year is $\int_0^T \tilde{a}_i di$ (see also Figure 1 in Section 2). For each transaction, the client reports to the auditor the following:

$$a_i = \tilde{a}_i + \varepsilon_i, \tag{1}$$

where

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

and p is endogenous. The error term ε_i represents the client manager's tendency to overstate the transaction's value. Since higher earnings are generally associated with higher firm valuation and managerial compensation, managers usually have greater incentive to overstate transaction values (e.g. Newman, Patterson, and Smith 2001; Patterson and Smith 2005; Callen, Lu, and Khan 2013). Misstatement can also be interpreted as a lack of sufficiently frequent disclosures, which helps the managers entrench themselves (Shleifer and

[12] In an earlier draft, we introduce audit firms of smaller size to capture blockchains' impact on auditors of heterogeneous sizes. It does not change our key messages and we leave it out for expositional simplicity.

Vishny 1989). Managers (or even auditors, e.g., Caskey, Nagar, and Petacchi 2010) 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 $\hat{a}_i$ and computes the aggregate income of the client as $\int_0^T \hat{a}_i di$. Following the literature (e.g., Scott 1973 and Antle and Nalebuff 1991), the auditor faces legal liabilities from restatements and thus needs to minimize the following loss function (auditor risk):

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

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 information efficiently is reduced, which reduces welfare because of inefficient resource allocation in a free market economy (e.g., Hayek 1945). Thus, a legal authority or a regulator (as we introduce later) would require and incentivize auditors to reduce misstatements.

In deriving his own estimate, the auditor can either accept the client's report, i.e., setting $\hat{a}_i = a_i$, or spend effort to verify the transaction; i.e., setting $\hat{a}_i = \tilde{a}_i$. 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

[13]For many firms, e.g., manufacturing firms, highly discretionary accounts do not constitute a large portion in their income statements (Stubben 2011). 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 reduces costs of internal auditing.

same to audit a within-auditor transaction and a cross-auditor transaction.[14] To be concrete, in the following discussion we assume that the cost function is of the following quadratic form:

$$C(s,T) = as^2T^2 + b, \quad a > 0, b > 0. \tag{4}$$

The auditor's complete problem is then to minimize the following objective function by choosing the appropriate auditing sample size s,

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

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 penalty). We assume that the client maximizes the following second-stage utility function,

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

where $\gamma, \delta > 0$. $\Pr(\hat{a}_i(s) = a_i > \tilde{a}_i)$ is the probability that the manager successfully overstates transaction values without being detected by the auditor, and $\Pr(\hat{a}_i(s) = \tilde{a}_i < a_i)$ is the probability that the manager is caught commiting 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 subsequent lawsuit cost for misreporting or reputation cost (e.g., Fischer and Verrecchia 2000).

Note that since the auditor randomly investigates a sample s:

$$\Pr(\hat{a}_i(s) = a_i > \tilde{a}_i) = (1-s)p,$$

[14] We could introduce two separate costs, but the reduction in auditing cost with blockchain is much larger than the difference between these two costs, and explicitly modeling these costs does not add any insights or change the implications of our model. Lu, Richardson, and Salterio (2011) further discuss the cost-benefit tradeoffs.

$$\Pr(\hat{a}_i(s) = \tilde{a}_i < a_i) = sp.$$

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

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

The FOC implies that the optimal auditing sample size is

$$s^* = \min\left(\frac{\lambda p\mu^2}{2aT}, 1\right). \tag{7}$$

From (6), the client's problem can be rewritten as

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

Solving this, we have the optimal overstatement probability equal to

$$p^* = \min\left(\frac{\gamma\mu(1-s)}{2\delta s^2T}, 1\right). \tag{9}$$

(7) and (9) form a system from which we can derive the equilibrium strategies (s^*, p^*) of the auditor and client.

Proposition 1. *A unique equilibrium exists in the auditor and client's second-stage problem, with the strategies* (s^*, p^*) *characterized by*

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

The equilibrium misstatement probability p^* *is weakly increasing in the auditing cost parameter* a *and transaction volume* T*, while the auditing intensity* s^* *is weakly decreasing in* a *and*

T. Both p^* and s^* are increasing in the misreporting incentive parameter γ. Furthermore, the sampling size s^*T and the misstatement size p^*T are increasing in T.

While the sampling size s^*T increases with transaction volume, the sampling intensity s^* decreases because the auditor finds it more economical to randomly sample less when there is a larger volume to process. The misstatement intensity p^* and sample p^*T both increase with T given that the auditor samples with less intensity. When auditing cost a increases, the optimal auditing intensity s^* declines; as a result, clients misreport more and p^* increases. If a client has a higher misreporting incentive γ, then its equilibrium misstatement intensity p^* is higher, leading the auditor to monitor more intensively with a higher s^*. Table 1 reports the complete set of comparative statics for the equilibrium policies with respect to the model parameters. For brevity, we omit the proofs since they follow from arguments similar to those in Proposition 1.

Table 1: Dependence of Equilibrium Policies on Model Parameters

	Model Parameters					
	a	T	δ	γ	μ	λ
Policy variables						
Misstatement probability: p^*	$+$	$+$	$-$	$+$	$-$	$-$
Auditing intensity: s^*	$-$	$-$	$-$	$+$	$+$	$+$
Misstatement sample size: p^*T	$+$	$+$	$-$	$+$	$-$	$-$
Auditing sample size: s^*T	$-$	$+$	$-$	$+$	$+$	$+$

When K and thus T are very large, the interior solution yields

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

where p^* is strictly increasing in T while s^* is strictly decreasing in T.

Equilibrium Fee and Auditor Choice

We now characterize the first-stage equilibrium in the traditional world without a blockchain that fosters automatic reconciliation and collaborative auditing. In the first stage, the clients have the option to switch to another auditor.[15] The auditors compete for clients by posting auditing fees. When the auditors' market is perfectly competitive, the zero profit condition leads to the following equilibrium auditing fee, which is the minimum an auditor would charge.

$$F(s^*) = \lambda E\left[\int_0^T (\hat{a}_i(s^*) - \tilde{a}_i)^2 di\right] + as^{*2}T^2 + b.$$

Firms $B_1$and B_2 take the second-stage utility as anticipated and choose an auditor to maximize the following objective

$$\gamma T(1 - s^*)p^*\mu - \delta(p^*s^*T)^2 - F,$$

where F is the auditing fee charged. Given that the technology of the two auditors is identical, the problem reduces to a Bertrand competition in auditing fees, thus the auditors indeed charge the minimum fee to break even.

Proposition 2. *A unique equilibrium exists in which each auditor gets one client and charges an auditing fee increasing in the size of the transaction volume,*

$$F(s^*) = \lambda E\left[\int_0^T (\hat{a}_i(s^*) - \tilde{a}_i)^2 di\right] + as^{*2}T^2 + b,$$

where $T = 2K^2$ is the transaction volume for each client, and (s^*, p^*) are as given in Proposition 1.

When the transaction volume T increases, it is more difficult and costly for the auditor to verify a representative sample. Therefore, the client has a greater propensity to overstate

[15]The main intuition and qualitative results are robust to the case where there is a cost associated with switching auditors.

and the auditing risk increases. In equilibrium, although the convexity in auditing costs reduces the auditing intensity, the auditing sample size increases in response to the higher overstatement probability by the client. The auditing fee consists of two components, the auditing risk and the auditing costs. Since both components increase with T, so does the auditing fee. This implication is consistent with the empirical literature that finds firm size to be one of the most important determinants of auditing fees. The auditing fee $F(s^*)$ also increases with μ and the cost parameters a and b, which is intuitive.

3.2. Auditing with Federated Blockchain

In the traditional world, an auditor incurs a cost for each inspection and can only randomly sample 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 sets up a blockchain, the inspection of transactions between firms associated with the two auditors can also be done at little cost (privacy concerns can be mitigated using zero-knowledge proof in a federated blockchain). For simplicity, we take this cost to be negligible.

In a federated blockchain, each auditor A sets up an internal permissioned blockchain, with each node operated by an auditing team inside the auditing firm.[16] Whenever a transaction i for client x happens, the team in charge of 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 that is also audited by the same firm, then the team in charge of client y would also upload the transaction. The blockchain can check if the two transaction reports match and consolidate them into a consensus record. If the two transactions do not match, the auditor immediately knows that one or both of the

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

transactions are misstated and can investigate. We therefore assume that the client would not misreport in this scenario since it is always immediately detected.

(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 and have the blockchain verify 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 the *zero-knowledge proof* method so that only encrypted information is revealed to the other party.[17] Because the auditor again has automatic detection of potential fraud, the client would not commit fraud or misreport.

(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 in the traditional way. Considering private firms only shift auditing fees by a constant, we omit this from our discussion.

To model the adoption of blockchain, we assume that after posting auditing fees and being matched with clients, A_1 and A_2 can decide whether to incur a cost c to adopt the blockchain system. In reality, while it is possible to commit to using the blockchain system even before posting fees (by incurring the cost first to set up the blockchain system), it is infeasible to commit to NOT using blockchains. Therefore the ordering of decisions in the game is equivalent to letting auditors decide on adoption first but with an option for non-adopters to regret, i.e., switching to blockchains after posting fees.

Now, a client firm can only choose to misstate transactions not reported to a blockchain system by both counterparties. Similarly, an auditing firm would only need to audit a

[17]We can also extend our model with a cost of privacy so that zero-knowledge proof carries concrete economic benefits.

random sample from this group of transactions. Suppose an auditor incurs an adoption cost for the blockchain system c, which could include not only the system set-up expenses, but also effort and costs in learning the new technology and educating clients about it. For example, setting up global transaction identifiers for clients and auditors can be very costly (e.g., Global Legal Entity Identifier System).[18] When c is large, not adopting blockchain is an equilibrium.

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

$$\min_{s\in[0,1]} \lambda T_{nb}(1-s)p\mu^2 + as^2T_{nb}^2 + b + c. \tag{10}$$

where T_{nb} is the number of transactions that are not on the blockchain. T_{nb} would be $K^2 + KK_{pr}$ if the other client of size K stays with the other auditor who chooses not to adopt blockchain, and would be KK_{pr} if both clients choose the same auditor or if the other auditor also adopts blockchain and the auditors form a blockchain consortium. (10) signifies the fact that the auditor only incurs risk or cost for transactions not on the federated blockchain. The FOC gives the optimal auditing sample size

$$s_b^* = \min\left(\frac{\lambda p\mu^2}{2aT_{nb}}, 1\right). \tag{11}$$

From (6), the client's problem in the second stage can be rewritten as

$$\max_{p\in[0,1]} \gamma(1-s)T_{nb}p\mu - \delta(psT_{nb})^2.$$

[18] In practice, the cost could also be borne by the client firm when they choose to join a blockchain system which the auditor can access. Since we show later that auditors charge competitive prices and break even in equilibrium, the clients bear the costs anyway and the distinction would not change our main results.

Solving this, we have the optimal overstatement probability equal to

$$p_b^* = \min\left(\frac{\gamma\mu(1-s)}{2\delta s^2 T_{nb}}, 1\right). \tag{12}$$

(11) and (12) form a system from which we can solve the equilibrium strategies (s_b^*, p_b^*) of the auditor and client.

We note that the first-stage objective of a firm is $\frac{\gamma^2\mu^2}{4\delta}\frac{(1-s^*)^2}{s^{*2}} - F$. For sufficiently large γ relative to λ and c, the decrease in the first term when the auditing sample decreases from T to T_{nb} outweighs the potential reduction in fee, making it unprofitable for an auditor to deviate to adopt blockchain because it cannot attract both clients, but would lose its own client for the reason that if the other client does not join, cross-auditor transactions would result in a higher fee than with two clients. An endogenous cost of adopting the technology is therefore the possibility of losing clients who would prefer less stringent auditing. This observation is consistent with the common criticism that auditors have vested interests and cater to clients with whom they have multiple business relationships.

What prevents an auditor from posting a traditional competitive fee and then adopting blockchain? In this case, switching to blockchain reduces the auditing expenses only to a certain extent because the other auditor is not on blockchain and cross-auditor transactions have to be audited manually. For c sufficiently large, the auditor has no incentive to deviate.

Now consider the equilibrium in which both auditors adopt blockchain. They are then in a Bertrand competition and would offer the same auditing fee equal to the lower second-stage auditing fee plus c. Would one of them have incentive to deviate to use the traditional system? Because fees are the only way to signal to clients that he would use the traditional system, this auditor must charge a higher fee. But what prevents it from using blockchain while charging a higher fee, which can reduce its auditing cost? Whether it gets one or two clients, using blockchain reduces this auditor's costs because the other auditor is already using blockchain in equilibrium. Therefore, the auditor cannot credibly deviate because it cannot credibly commit to not using blockchain.

We can also similarly rule out the equilibrium where only one auditor adopts blockchain. We thus have the following proposition.

Proposition 3. *An equilibrium in the blockchain world features either both auditors adopting blockchain or neither adopting blockchain. In the equilibrium with full adoption,*

$$s_b^* T_{nb} < s^* T, \quad p_b^* T_{nb} < p^* T$$
$$s_b^* > s^*, \quad p_b^* < p^*$$

i.e., the clients misreport less in the model with a federated blockchain and the auditors choose a smaller auditing sample. The auditing fee F_b and auditor's risk L_b are smaller than those in the equilibrium without blockchains.

Interestingly, the auditing intensity s_b^* with a federated blockchain is higher than that without blockchains, because the auditor now only needs to verify a smaller sample, T_{nb}, of transactions. Obviously, the auditing fee and auditor's risk are increasing in the fraction of off-chain transactions for the same transaction volume. In other words, $\frac{\partial F_b}{\partial \alpha} > 0$ and $\frac{\partial L_b}{\partial \alpha} > 0$, where α is the fraction of off-chain transactions.

Which types of equilibria prevail ultimately depends on the model parameters. For illustration, we plot in Figure 5 the scenarios with respect to two key parameters of the model: the blockchain adoption cost c and the client misstatement incentive γ. Several patterns emerge from the plot. First, for fixed γ, full adoption and no adoption equilibria correspond to regions with low and high values of c, respectively. This is intuitive since auditors are more likely to adopt the technology with lower cost. Second, there is a region in which the two equilibria co-exist due to strategic complementarity between the auditors. Third, when the misstatement incentive of clients is very high, only the no-adoption equilibrium remains. The intuition is that blockchain auditing makes it harder for clients to misstate and thus is not preferred by those with stronger misreporting incentives. Catering to clients' preferences, auditors opt not to adopt the technology. Interestingly, when γ is very low, we also see that

the region with full adoption equilibrium shrinks. This is because clients with very low γ misreport less, reducing the benefits of adopting blockchains and netting costs. Therefore, the type of the model's equilibrium is *non-monotone* with respect to γ. This intuition is formalized in the following corollary:

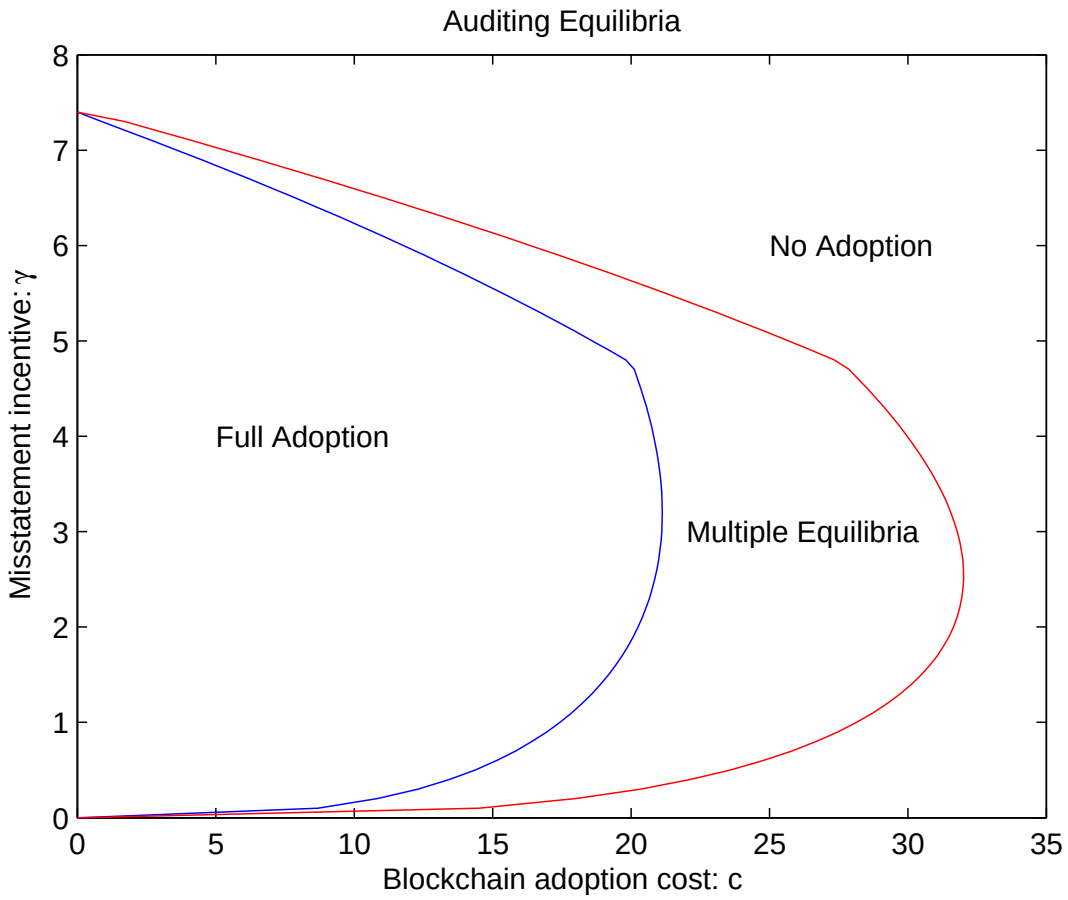

Figure 5: **The Evolution of Equilibrium Adoption of Blockchains** Parameters are $K = 5, K_{pr} = 0.4, \mu = 1, \delta = 1, \lambda = 1, a = 0.05, b = 0$.

Corollary 1. *With all other parameters other than the misstatement incentive γ fixed, there exists $\gamma_1 > \gamma_2 > 0$, such that if $\gamma > \gamma_1$ or $\gamma < \gamma_2$, no adoption is the unique equilibrium.*

Non-collaborative Auditing

One can also consider the case where each auditor operates their own independent blockchain without the federated structure. In other words, while within-auditor transactions can be verified on the auditor's blockchain, there is no efficient way of verifying cross-auditor transactions, even when both auditors have blockchains. The following corollary points out that a federated blockchain is superior to a system of independent blockchains in that it further reduces auditing fees and risk. The key difference between the federated blockchain and independent blockchains is that *cross-auditor transactions* can be automatically verified on the network using zero-knowledge proof methods. Let T_{nib} denote the number of transactions for which the transaction parties do not both reside in an independent blockchain system.

Corollary 2. *There is a unique equilibrium* (s^*_{ib}, p^*_{ib}) *when each auditor operates an independent blockchain. The optimal policy satisfies*

$$s^*T > s^*_{ib}T_{nib} > s^*_bT_{nb}, \quad p^*T > p^*_{ib}T_{nib} > p^*_bT_{nb}.$$

Furthermore, the auditing fee F_{ib} *and auditor's risk* L_{ib} *are lower than those in the model without blockchains, but higher than those in the model with a federated blockchain.*

4. Regulation

In this section, we extend the model to incorporate a regulator (PCAOB). We first examine how blockchain adoption helps reduce regulation cost, then highlight the regulator's role in coordinating auditor adoption.

4.1. Regulated Auditing and Regulator Costs

Regulated Auditing without Blockchains

The regulator has access to all transactions among clients of auditing firms. The regulator can also manually verify a random sample t of all transactions. The verification cost function for the regulator is given by

$$C_r(t) = et^2T^2 + f,$$

where f is a fixed set-up cost. The regulator's objective is

$$\min_{0\leq t\leq 1} \lambda_r E\left[\int_0^T (\hat{a}_i^r - \tilde{a}_i)^2 di\right] + et^2T^2 + f \tag{13}$$

where $\hat{a}_i^r$ is the state of transaction i after auditing by both the auditor and PCAOB and $\tilde{a}_i$ is the true state of the transaction. We assume that while the auditor may reduce the auditing sample due to conflicts of interest or influence from the client, the auditor cannot misreport the results from its sampling. Therefore, the samplings of PCAOB and auditors are independent.[19] The regulator's objective function is simplified to

$$\min_{0\leq t\leq 1} \lambda_r(1-s)(1-t)pT\mu^2 + et^2T^2 + f. \tag{14}$$

Because the regulator can find a deviation of a transaction from its true value, the auditor's risk of being punished for oversight increases with regulatory monitoring. Therefore, we generalize the auditor's risk function to be of the form

$$L = \lambda_a tE\left[\int_0^T (\hat{a}_i - \tilde{a}_i)^2 di\right]. \tag{15}$$

Parameter $\lambda_a > 0$ captures how much penalty the auditor receives when there are discrepancies between the true state and audited state of the transactions. The penalty is proportional

[19] Our model can be modified to accommodate the possibility that the auditor may misreport auditing results and PCAOB may thus check the auditor's sampling.

to the regulator's inspection propensity t since the probability of finding a discrepancy is proportional to t. The auditor's objective thus becomes

$$\min_{0\leq s\leq 1} \lambda_a tE\left[\int_0^T (\hat{a}_i(s)-\tilde{a}_i)^2 di\right] + as^2T^2 + b. \tag{16}$$

This can be simplified to

$$\min_{0\leq s\leq 1} \lambda_a t(1-s)pT\mu^2 + as^2T^2 + b. \tag{17}$$

The client's incentive is the same as given in (8).

Proposition 4. *There is a unique equilibrium for the auditing model with a regulator in which the client, the auditor, and the regulator choose a policy* (p^*, s^*, t^*) *that solves the problems* (8)*,* (17)*, and* (14)*, respectively. The auditing sample* s^*T *and regulatory sample* t^*T *are weakly increasing in the regulatory cost parameter* e *but the misstatement sample* p^*T *is weakly decreasing in* e*.*

When regulatory costs are reduced, auditors face more scrutiny from the regulator and need to boost their auditing samples to avoid greater potential detection due to discrepancies. As a result, clients misreport less. Therefore, a reduction in regulatory costs is beneficial for audit quality. Although outside the model, another implication of the proposition is that lower regulatory costs lead to greater auditor independence since auditors have to exert more effort, *ceteris paribus*. Regulatory costs in the traditional world can be substantial and the effectiveness of regulation is to a large extent limited by the PCAOB's resources. Naturally, a question is then whether blockchains can help the regulator to achieve higher efficiency.

Regulated Auditing with Blockchains

In this section, we consider regulated auditing with a federated blockchain. Similar to the unregulated auditing model with blockchains, there are three classes of transactions: within-auditor, cross-auditor, and off-chain transactions. The regulator has access to all data on the

federated blockchain and can thus also automate its inspection of within- and cross-auditor transactions. Again, let T_{nb} be the number of off-chain transactions. Both the auditor and the regulator only incur costs for off-chain transactions. As a result, the clients will also only misreport in off-chain transactions.

The objective functions can be written as follows. The client's objective function is

$$\max_p p(1-s)\mu T_{nb} - \delta s T_{nb}^2.$$

The auditor's objective function is

$$\min_s \lambda_a(1-s)tp\mu^2 T_{nb} + as^2 T_{nb}^2 + b.$$

The regulator's objective function is

$$\min_t \lambda_r p(1-s)(1-t)\mu^2 T_{nb} + et^2 T_{nb}^2 + f.$$

Proposition 5. *Assuming that the auditors adopt blockchain, there is a unique equilibrium under regulated auditing with a federated blockchain. The equilibrium policy* (p_b^*, s_b^*, t_b^*) *satisfies*

$$p_b^* T_{nb} < p^* T, \quad s_b^* T_{nb} < s^* T, \quad t_b^* T_{nb} < t^* T.$$

Therefore, auditing cost and the regulator's monitoring cost are lower than those in the case without blockchains. Auditing fees and misstatement risk also decrease.

Therefore, blockchain adoption can help lower both auditing and regulatory costs and increase auditing quality. However, we note that the initial adoption of the blockchain system can be costly (see also our discussion in Section 2) and may require auditor coordination.

4.2. Coordinating Adoption and Collaborative Auditing

There are several limitations or frictions for auditors to adopt the new technology. First, switching costs consist of the implementation cost of blockchain adoption and auditors' cost of learning the new system. Second, collaborative auditing necessitates a certain standardization of blockchain platforms for client and audit firms. While technological progress may reduce implementation costs, how to coordinate an industry-wide technology adoption is a challenging problem and a regulator's intervention might be needed.

As shown in Proposition 3, under a certain range of parameters, there could be two equilibria: no adoption equilibrium and full adoption equilibrium. Because the equilibrium misstatements and costs associated with auditing and its regulation are lower in the full adoption equilibrium (whether we count regulatory cost or not), it is a dominant policy for the regulator to coordinate adoption. The following proposition formalizes this intuition:

Proposition 6. *When there exist multiple equilibria, then in the regulated auditing model, if the adoption cost c is sufficiently small, then the regulator strictly prefers the full adoption equilibrium to the no adoption equilibrium.*

Given the potential reduction of misstatements and costs associated with auditing and regulation when using blockchains and the possibility of a no adoption equilibrium, we thus expect PCAOB to play a pivotal role in facilitating coordination among auditors and client firms once the technology is relatively mature and the adoption cost is still non-trivial. For example, PCAOB can impose regulatory standards or coordinate the development of the underlying infrastructure of blockchains.

5. Discussion and Extensions

5.1. Discretionary Accounts and Blockchains

In the models considered in the previous sections, clients have transaction-based accounts. As Friedman and Mahieux (2018) have shown, much of the auditing task for transaction-

based or nondiscretionary accounts can be automated with blockchains. In reality, most 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 blockchains can still have indirect effects on discretionary auditing. We consider below an extension of our baseline model in which auditors conduct both nondiscretionary and discretionary auditing.

In the model, each client has transaction-based accounts with total volume T as before, labeled by $i \in [0, T]$, and discretionary accounts with total volume D, labeled by $j \in (T, T + D]$. The client can choose to misstate with a probability p for nondiscretionary transactions, and a probability p_D for discretionary accounts. The auditor selects audit sampling probability s and s_D, for transaction-based and discretionary accounts, respectively. The objective for the auditor is

$$\min_{s,s_D\in[0,1]} \lambda E\left[\int_0^T (\hat{a}_i(s) - \tilde{a}_i)^2 di + \int_T^{T+D} (\hat{a}_j(s_D) - \tilde{a}_j)^2 dj\right] + a(sT + ks_D D)^2 + b, \tag{18}$$

where $k > 0$ represents the relative difference in the costs for transaction-based and discretionary auditing. In typical scenarios, $k > 1$ since discretionary auditing may require more experience and efforts. Equation (18) can be rewritten as

$$\min_{s,s_D\in[0,1]} \lambda\mu^2(T(1-s)p + D(1-s_D)p_D) + a(sT + ks_D D)^2 + b. \tag{19}$$

Similarly, the objective for the client is generalized to

$$\max_{p\in[0,1]} \gamma\mu \Pr(\hat{a}_l = a_l > \tilde{a}_l | l \in [0, T + D])(T + D) - \delta \left(\Pr(\hat{a}_l = \tilde{a}_l < a_l | l \in [0, T + D])(T + D)\right). \tag{20}$$

or

$$\max_{p,p_D\in[0,1]} \gamma\mu\left(T(1-s)p + D(1-s_D)p_D\right) - \delta(spT + s_D p_D D)^2. \tag{21}$$

We have the following result about the equilibrium without blockchains.

Proposition 7. *A unique equilibrium exists in which each auditor gets one client and the equilibrium strategies (s^*, s_D^*) and (p^*, p_D^*) for auditors and clients satisfy*

$$p^* = \frac{p_D^*}{k}, \quad s^* = s_D^*.$$

Furthermore, (s^*, p^*) are the same as the equilibrium solution to the model with only transaction-based accounts (as in Proposition 1) and transaction volume $T + kD$.

The intuition is that if $p^* \neq \frac{p_D^*}{k}$, say, $p^* > \frac{p_D^*}{k}$, then the marginal benefits of auditing trasaction-based accounts is higher than that of auditing discretionary transactions, which implies that auditors would spend more effort on transaction-based auditing and thus it is not an equilibrium. Similarly, in equilibrium, the auditors must set $s^* = s_D^*$; otherwise the clients would have incentive to misstate more in one of the two pools of transactions.

When an auditor adopts blockchain, the volume of a client's transaction-based accounts that need to be verified by conventional methods shrinks to $T_{nb} < T$, but all discretionary accounts still need to be audited in the traditional way. We have the following characterization of the equilibrium with blockchains:

Proposition 8. *An equilibrium with discretionary account auditing and blockchains features either both auditors adopting blockchain or neither adopting blockchain. In the equilibrium with full adoption, compared with the equilibrium in the traditional world,*

1) The clients misreport less in both the discretionary and transaction-based accounts;

2) The auditors choose a smaller auditing sample for transaction-based accounts but a larger auditing sample for discretionary accounts;

3) Auditor risk and auditing fees decrease.

We note that 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. There is a *spillover* effect from the cost savings in transaction-based auditing to discretionary auditing: since auditors now have more resources devoted to discretionary auditing, the client is forced to misstate less both in discretionary and transaction-based accounts and thus auditing quality in both types of accounts increase. Relating to the auditor labor market, there is likely lower demand for less skillful auditors but greater demand for more skillful auditors for off-chain transactions and highly discretionary accounts.

5.2. Firm Adoption, Switching Auditors, and Signaling

Our model can be extended to include a client firm's adoption cost of the federated blockchain. Such costs are typically associated with learning about and using a blockchain system provided by a third party. If the client firms were to build their own private blockchains, there would be huge duplicate adoption costs. Moreover, when a firm switches to a different auditor, there could be substantial switching cost because of non-audit services that are often bundled with the auditing service (e.g., Friedman and Mahieux 2018). A moderately high switching cost would ensure that in the no adoption equilibrium, an auditor deviating to adopt blockchain would not attract all the clients.

So far we have also left out the potential benefit for firms to commit ex ante to not misreporting. By choosing an auditor in the federated blockchain, a client firm may convey to investors that it would incur fewer misstatements. Alternatively, it is possible that instead of directly influencing auditors' adoption of the new technology, a regulator can require transparency of auditing technologies. To see this, suppose the clients hire auditors to audit their financial reports for the purpose of raising financing from investors or receiving favorable market valuation (e.g., Gao and Zhang 2018). If the auditing technologies are disclosed publicly, investors rationally anticipate that clients choosing an auditor with blockchain

would have less misstatement in equilibrium, and thus prefer financing them over clients choosing an auditor under the traditional system. Consequently, the auditor adopting the technology might win over all the clients, which helps overcome the cost of adoption. The signaling or certification effect of choosing an auditor with the blockchain technology can therefore help eliminate the no-adoption equilibrium when the adoption cost is not very high. Although not explicitly modeled here, this channel is straightforward once allowed in our model. It not only has policy implications on technology transparency, but also constitutes an interesting theoretical extension as an example of how adding a stage of auditor competition would break equilibrium multiplicity in technology adoption — a phenomenon unexplored in earlier models.

That said, if the auditing industry is not dominated by two large players but is populated with a number of auditors who do not coordinate, then even when firms want to costly signal that they are the better type that can afford committing to lowering misstatements (by adopting the blockchain system, for example), or switch from a long-term auditing firm to another one with blockchain, there could still be an equilibrium that enough firms choose not to adopt, via a similar mechanism as in Petacchi and Nagar (2016). To see this, suppose most of the firms believe that others are not choosing auditors using federated blockchains, then the benefit of adoption is not very high even though the firm can separate from the rest. In contrast, a large number of firms' not adopting means it is very hard for a client firm to get caught, given auditors' limited resources. The net benefit of misstatement still outweighs the commitment to using an auditor under the federated blockchain.

6. Conclusion

In this paper, we analyze equilibrium outcomes of financial reporting and auditing in settings with and without the blockchain technology, and 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 clients and clients endogenously

determine the level of misstatement in anticipation of the endogenous auditing intensity. We argue that federated blockchains and zero-knowledge proof can allay data-privacy concerns without requiring a trusted third party, and thus connect isolated auditing process either across audit teams or audit firms. Blockchains therefore potentially facilitate automated and collaborative auditing to reduce audit costs for transaction-based accounts. The technology potentially disrupts conventional audit pricing, sampling, and effort allocation. In equilibrium, auditors either all stick with the traditional systems or all adopt the blockchain technology. Wide adoption of the technology also reduces regulators' cost of monitoring, allowing them to focus on a smaller sample for inspection. Regulators can coordinate systematic adoption to capitalize on the positive externality in utilizing the technology, and reduce equilibrium misstatements and costs associated with auditing and its regulation.

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, although it is a leading candidate. It is our hope that this study would 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 service in credit markets (Liberti, Sturgess, and Sutherland 2018), the economic implications for such multi-party computation remain a fruitful area for future research.

Appendix A. Blockchains and Zero-Knowledge Proofs

Distributed Ledgers and Permissioned Blockchains

Blockchains, or more generally, distributed ledger technologies, are based on several advancements in computing science, including hashing, digital signature, distributed systems, and consensus mechanisms. Although these individual elements were introduced earlier, Nakamoto (2008) brings them all together and proposes a peer-to-peer distributed transaction and ledger system, i.e., Bitcoin, that aims 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 Harvey (2016) and Yermack (2017) for excellent introductions to 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.[20] 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 2017 and Cong, He, and Li 2018). Permissioned blockchains are also more secure from attacks and can handle higher throughput. Open-source software for permissioned blockchains include Corda (by R3), Hyperledger Fabric (by IBM), and Quorum (by J.P. Morgan). Various companies also developed their

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

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 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 Zero-Knowledge Proofs

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. Zero-knowledge proofs are a set of algorithms from the field of cryptography that can ensure both validity and confidentiality of records in a blockchain.

Goldwasser, Micali, and Rackoff (1989) first introduced the notion of *zero-knowledge proofs* (ZKP). A ZKP is a proof of a statement by one party (the prover) to another party (the verifier) without conveying any additional information to the verifier, other than the correctness of the statement. This may sound paradoxical but is possible using ideas in cryptography. We give two examples below to illustrate the main intuition of ZKPs.

Example 1. Two cards and a color-blind friend. Suppose you have two cards identical in all aspects except that one is green and the other red. You also have a color-blind friend who cannot distinguish red and green. How do you convince your friend that the two cards have different colors? You can give the two cards to your friend and ask him to put them behind his back. Next, he picks one card and shows it to you. He then puts it behind his back again and chooses one card at random (with equal probabilities) and shows it to you. He asks you whether he has switched the card. The whole process can

then be repeated as needed. If the two cards indeed have different colors, then you can give the correct answer every time. Otherwise, if you cannot tell the two cards apart, then you answer incorrectly 50% of the time. If the experiment is repeated many times, then your friend can be very certain that you can indeed distinguish the two cards and thus that they are of different colors.

Example 2. Knowledge of a discrete logarithm. Consider a positive integer q and modulo-q arithmetic. Let g and y be relatively prime integers. If an integer x satisfies $g^x \equiv y \pmod{q}$ then x is called a discrete logarithm of y to the base g. If one knows the prime factorization of q, it is easy to determine the discrete logarithm using a theorem in number theory. Otherwise, finding the discrete logarithm can be computationally impractical for a large y. In other words, the function $f(x) = g^x \pmod{q}$ is a one-way function, similar to the hash function. This function has many applications in cryptography, including in the famous RSA public-key cryptography. Suppose Peggy (the prover) knows the discrete logarithm x of y (for example, Peggy has created y from the equation $y = g^x$) and wants to prove it to Victor (the verifier) without revealing the value of x. The following procedure can achieve this goal.

1. Peggy picks a random integer v and computes $t = g^v$ to Victor.
2. Victor chooses a random integer c and sends it to Peggy.
3. Peggy computes $r = v - cx$ and sends r to Victor.
4. Victor checks whether $t \equiv g^r y^c \pmod{q}$. If $y \equiv g^x$,this is true as $g^r y^c \equiv g^{v-cx} g^{cx} = g^v = t$.

If Peggy does not know x, it would be virtually impossible for her to find the correct number r in Step 3 above, given the difficulty of computing the discrete logarithm. Therefore, the above experiment (with repeats if necessary) proves that Peggy knows x without revealing x, as Victor cannot deduce v or x from the messages t and r.

We note that in both examples, the ZKP requires interactions between the prover and the verifier and depends on randomness in the actions of the two parties. Indeed, this is almost

always the case for all ZKP schemes and the verifier's randomness is especially important. As a result, the ZKP is a statistical proof, i.e., it is valid with a probability arbitrarily close to 1. For all practical purposes, this will suffice. In practice, interactions between multiple parties can be time-consuming and inefficient. Therefore, a *non-interactive zero-knowledge proof* (NIZK) would be desirable. An NIZK contains a single message produced by the prover that can be verified by anyone. The advantage of NIZK is that the message can be stored or shared among many different parties. Blum, Feldman, and Micali (1988) used the Fiat-Shamir heuristic (Fiat and Shamir, 1986) to show that a string shared between a proposer and a verifier is sufficient for achieving ZKP computationally without requiring further interactions. Recall that the verifier's randomness is key to interactive ZKP schemes and requires interactions. The Fiat-Shamir heuristic replaces the verifier's randomness (and therefore the interactions) with a cryptographic hash function. Since the prover cannot predict the output of a hash function, this effectively removes the need for the interactive step. We illustrate this by modifying the ZKP algorithm in Example 2 into an NIZK.

Example 3. Discrete logarithm: Non-interactive zero-knowledge proof. The new algorithm is as follows:

1. Peggy picks a random integer v and computes $t = g^v$.
2. Peggy computes $c = H(g, y, t)$, where $H()$ is a cryptographic hash function.
3. Peggy computes $r = v - cx$ and sends r and c to Victor.
4. Victor checks whether $t \equiv g^r y^c \pmod{q}$.

Note that only Step 2 of Example 3 is changed, where the random input c by Victor is replaced by the output of a cryptographic hash function. Since the output of a hash function is pseudo-random (and thus unpredictable), this achieves the same purpose.

Zero-knowledge proofs can be very useful in privacy-sensitive environments. We discuss below several applications of zero-knowledge proofs.

Digital signature. If what the prover needs to show is that he knows the password to an account, then NIZK can be used to generate a *digital signature* that can authenticate the

prover's identity, without the need to reveal the password to the verifier.

Zcash. Zcash is a crypocurrency that is similar to Bitcoin but employs cryptographic tools to truly anonymize transactions. Zcash uses a new type of zero-knowledge protocol called zk-SNARKs. zk-SNARK stands for *zero-knowledge succinct non-interactive argument of knowledge*, which allows very efficient storage and fast execution. For example, a recent paper (Ben-Sasson, Chiesa, Tromer, and Virza, 2019) proposes a zk-SNARK system that generates 288-byte proofs that can be verified in milliseconds. zk-SNARKs allow Zcash transactions to be anonymous and still can be verified by miners – even transaction amounts can be hidden to the public. In order to comply with regulatory requirements, however, Zcash also provides the option to keep transactions transparent.

Ethereum. Ethereum has also introduced zk-SNARKs in a recent update named Byzantium, in 2017. This allows private transactions to be verified on Ethereum without revealing information about the parties.

zkLedger. zkLedger is a protocol allowing outside auditors and regulators to verify accurate information while protecting privacy through zero-knowledge proofs of cryptography. Narula, Vasquez and Virza (2018) provide details on implementation.

Bulletproofs. Bunz et al (2018) propose *Bulletproofs*, an algorithm that allows efficient proofs that a number is within a given range.

In our model, the combination of ZKP and blockchains allows the secure verification of cross-auditor transactions in a traceable way. A potential algorithm is as follows. Suppose a transaction happens between two clients, say, Apple made a payment of \$98M to Intel. Apple and Intel are audited by audit firms A_1 and A_2, respectively. Let a pair of strings (s_1, s_2) represent the details of the transaction, where s_1 contains the transaction identifying details, such as the counter party identities (Apple, Intel), date, and transaction number, s_2 contains the transaction amount (\$98M). Let g be a generator (a large number) commonly known to all parties so that it is difficult to compute digital logarithms with respect to g (see Examples 2 and 3 above).

1. Auditor A_1 generates two strings (t_1, t_2) and puts them on the federated blockchain, where $t_1 = g^{s_1}$ and $t_2 = g^{s_2}$.

2. Using techniques in Example 3, A_1 can also write a ZKP string on the blockchain so that other auditors can verify that A_1 knows s_1 and s_2 without learning the values of s_1 and s_2.

3. Auditor A_2, equipped with the counterparty's record (from Intel), also knows s_1 and a potentially different transaction amount s_2'. A_2 can put the string $(t_1, t_2' = g^{s_2'})$ on the blockchain together with a ZKP string proving that he knows (s_1, s_2').

4. The algorithm then verifies that $t_1 = g^{s_1}$ to confirm the transaction details and check whether $t_2 = g^{s_2'}$. A_1 then can infer from A_2's verification whether the transaction matches with the counterparty's record or not. If and only if $t_2 = t_2'$, the records match. Due to the nature of ZKP, A_1 cannot infer the amount on A_2's record except when a match occurs.

5. Other auditors/nodes on the federated blockchain can see whether a match happens and can confirm from the ZKPs that both sides indeed have private information about the transaction details and amounts. However, they are unable to see any information about the transaction.

Appendix B. Proofs

Proof of Proposition 1. The system of FOC equations 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 $0 \leq s < 1$ and $p \geq g(1)$

when $s = 1$. The second curve is given by $p = \min(h(s),1)$ for $0 \leq s \leq 1$. Since $g(s)$ is increasing in s, the first curve is increasing in s. We have

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

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. We only need to show that auditor risk and auditing cost both increase with T. From Proposition 1, $\frac{\partial(s^*T)}{\partial T} > 0$, hence the auditing cost, $as^{*2}T^2 + b$, increases with T. The auditor risk is

$$L = \lambda(1-s^*)p^*T\mu^2.$$

By (A1) and (A2), this is equal to $\frac{\lambda\gamma\mu^3(1-s^*)^2}{2\delta s^{*2}}$, which increases with T because $\frac{\partial s^*}{\partial T} < 0$. 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_T, p_T be the solution to the equilibrium conditions when transaction volume is T; in other words, they satisfy

$$p_T = \frac{\gamma\mu(1-s)}{2\delta s^2 T},$$
$$s_T = \frac{\lambda p_T \mu^2}{2aT}.$$

Recall from the proof of Proposition 1 that s_T is the solution to the following equation

$$4a\delta T^2 s_T^3 = \lambda\gamma\mu^3(1-s_T). \tag{A4}$$

Define $CU(T)$ and $F(T)$ as the second-stage utilities of the client and auditor, respectively. In other words,

$$CU(T) = \gamma T(1-s_T)p_T\mu - \delta(p_T s_T T)^2 = \frac{\gamma^2\mu^2(1-s_T)^2}{4\delta s_T^2}, \tag{A5}$$

$$F(T) = \lambda(1-s_T)Tp_T\mu^2 + as_T^2T^2 + b = \frac{\lambda\gamma\mu^3(1-s_T)^2}{2\delta s_T^2} + \frac{\lambda\gamma\mu^3}{4\delta}\frac{1-s_T}{s_T} + b. \tag{A6}$$

For simplicity of notation, 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, respectively. We note that $T_2 < T_1 < T_0$.

No Adoption Equilibrium We first consider conditions under which the no adoption equilibrium exists. Without blockchains, both auditors charge a fee of $F(T_0)$ to their client. If one auditor deviates to adopt blockchain, then the minimum fee it charges is $F(T_1)+c$. In order for the auditor to retain its client, the following client incentive condition has to be satisfied:

$$CU(T_1) - F(T_1) - c \geq CU(T_0) - F(T_0)$$

Therefore, the auditor's no-deviation condition is

$$CU(T_1) - F(T_1) - CU(T_0) + F(T_0) \leq c. \tag{A7}$$

Using (A5) and (A6), this can be simplified to

$$\frac{\gamma\mu^2}{2\delta}\left[(\frac{\gamma}{2} - \lambda\mu)\left(\frac{1-s_{T_1}}{s_{T_1}} + \frac{1-s_{T_0}}{s_{T_0}}\right) - \frac{\lambda\mu}{2}\right]\left(\frac{1-s_{T_1}}{s_{T_1}} - \frac{1-s_{T_0}}{s_{T_0}}\right) \leq c. \tag{A8}$$

From Proposition 1, s_T decreases with T and thus $\frac{1-s_T}{s_T}$ increases with T. Therefore, the term $\frac{1-s_{T_1}}{s_{T_1}} - \frac{1-s_{T_0}}{s_{T_0}}$ is negative. It follows that if γ is sufficiently large, then the left hand side of (A8) is negative and the no adoption equilibrium always exists regardless of the value of c. For smaller values of γ, a sufficiently large c also ensures that the no adoption equilibrium exists.

Full Adoption Equilibrium When both auditors adopt blockchain, the fee they charge is $F(T_2) + c$. If one of the them deviates, the minimum fee it charges is $F(T_0)$. Therefore, the no deviation condition is

$$CU(T_2) - F(T_2) - CU(T_0) + F(T_0) \geq c. \tag{A9}$$

This is equivalent to, by (A5) and (A6),

$$\frac{\gamma\mu^2}{2\delta}\left[(\frac{\gamma}{2}-\lambda\mu)\left(\frac{1-s_{T_2}}{s_{T_2}}+\frac{1-s_{T_0}}{s_{T_0}}\right)-\frac{\lambda\mu}{2}\right]\left(\frac{1-s_{T_2}}{s_{T_2}}-\frac{1-s_{T_0}}{s_{T_0}}\right)\geq c. \tag{A10}$$

The above condition is satisfied when γ is sufficiently small and c is sufficiently small relative to γ. We note that since $\frac{1-s_{T_2}}{s_{T_2}}<\frac{1-s_{T_1}}{s_{T_1}}<\frac{1-s_{T_0}}{s_{T_0}}$, the conditions (A8) and (A10) potentially can be both satisfied for certain ranges of parameter values. This illustrates the strategic complementarity of the auditors' adoption decisions: when both auditors adopt blockchain, the benefit to each of them is larger than that when only one adopts.

In the generic case, one auditor adopting a blockchain while the other does not is not an equilibrium. In this case, the client with the blockchain-adopting auditor has first-stage utility $CU(T_1)-F(T_1)-c$ while the other client has first-stage utility $CU(T_0)-F(T_0)$. For the auditor with blockchain not to deviate, the condition is

$$CU(T_1)-F(T_1)-CU(T_0)+F(T_0)\geq c.$$

For the auditor without blockchain not to deviate, the condition is

$$CU(T_2)-F(T_2)-CU(T_0)+F(T_0)\leq c.$$

It is easy to see that these conditions cannot be satisfied at the same time.

In the full adoption equilibrium, the comparative statics of s_T, p_T, s_TT and p_TT with respect to T, follow from the comparative statics shown in Proposition 1. The auditing fee is lower than that in the traditional world by the equilibrium condition (A9) and the fact that $CU(T_2)<CU(T_0)$. The auditor risk also decreases, by Proposition 2. Q.E.D.

Proof of Corollary 1. The fact that $\frac{1-s_{T_1}}{s_{T_1}}-\frac{1-s_{T_0}}{s_{T_0}}$ is negative (from the proof of Proposition 3) implies that for γ sufficiently small or large, the left hand side of (A8) is negative. Therefore, (A8) holds and no adoption is an equilibrium. Similarly, when γ is sufficiently small or large, the left hand side of (A10) is negative and (A10) cannot hold; therefore, full adoption is not an equilibrium and no adoption is the unique equilibrium. Q.E.D.

Proof of Proposition 4. First-order conditions to the client's, auditor's, and regulator's problems are

$$p^* = \min\left(\frac{\gamma\mu(1-s^*)}{2\delta s^{*2}T}, 1\right), \tag{A11}$$

$$s^* = \min\left(\frac{\lambda_a\mu^2 p^* t^*}{2aT}, 1\right), \tag{A12}$$

$$t^* = \min\left(\frac{\lambda_r\mu^2(1-s^*)p^*}{2eT}, 1\right). \tag{A13}$$

For brevity, we focus on interior solutions to the above equations (solutions to the corner cases are available upon request). Solving p^* and t^* in terms of s^* and plugging back into (A12), we obtain

$$\frac{16ae\delta^2T^4}{\lambda_a\lambda_r\gamma^2\mu^6}s^{*5} - (1-s^*)^3 = 0. \tag{A14}$$

Taking derivatives on both sides and noting that $0 < s^* < 1$, we see that $\frac{\partial s^*}{\partial e} < 0$. Equation (A11) then implies that $\frac{\partial p^*}{\partial e} > 0$. From Equations (A13), (A11), and (A14),

$$t^* = \frac{\lambda_r\mu^2}{2T}\frac{(1-s^*)p^*}{e} = \frac{\gamma\lambda_r\mu^2}{4\delta T^2}\frac{(1-s^*)^2}{es^{*2}} = l\frac{(1-s^*)^2}{\frac{(1-s^*)^3}{s^{*3}}} = l\frac{s^{*3}}{1-s^*},$$

where l is a constant independent of e. Therefore, $\frac{\partial t^*}{\partial e} < 0$. Since T is independent of e, we have $\frac{\partial(s^*T)}{\partial e} < 0$, $\frac{\partial(p^*T)}{\partial e} > 0$, and $\frac{\partial(t^*T)}{\partial e} < 0$. Q.E.D.

Proof of Proposition 5. The first-order conditions for the equilibrium with blockchains are

$$p_b^* = \min\left(\frac{\gamma\mu(1-s_b^*)}{2\delta s_b^{*2}T_{nb}}, 1\right), \tag{A15}$$

$$s_b^* = \min\left(\frac{\lambda_a\mu^2 p_b^* t_b^*}{2aT_{nb}}, 1\right), \tag{A16}$$

$$t_b^* = \min\left(\frac{\lambda_r\mu^2(1-s_b^*)p_b^*}{2eT_{nb}}, 1\right). \tag{A17}$$

Comparing these equations to (A11), (A12), and (A13), it is clear that we only need to prove that $\frac{\partial(s^*T)}{\partial T} > 0$, $\frac{\partial(p^*T)}{\partial T} > 0$, and $\frac{\partial(t^*T)}{\partial T} > 0$ to show that client misstatements, auditor sampling size, and regulator sampling size all decrease with the introduction of blockchains. We first note that by

taking derivatives with respect to T on both sides of Equation (A14), we have $\frac{\partial s^*}{\partial T} < 0$. Equation (A14) also implies

$$l(s^{*4}T^4) = \frac{(1-s^*)^3}{s^*},$$

for some constant l independent of T. Since the right hand side increases with T, so does the left hand side and s^*T. From Equation (A11), $p^*T = \frac{\gamma\mu(1-s^*)}{2\delta s^{*2}}$ increases with T. From (A13) and (A14),

$$\begin{aligned} tT &= \frac{\lambda_r\mu^2}{2e}(1-s^*)p^* = l\frac{(1-s^*)^2}{s^{*2}T} = l\frac{(1-s^*)^2}{(s^{*5}T^4)^{\frac{1}{4}}s^{*\frac{3}{4}}} \\ &= l'\frac{(1-s^*)^2}{(1-s^*)^{\frac{3}{4}}s^{*\frac{3}{4}}} = l'\frac{(1-s^*)^{\frac{5}{4}}}{s^{*\frac{3}{4}}}, \end{aligned}$$

where l and l' are independent of T. Therefore, $\frac{\partial(t^*T)}{\partial T} > 0$.

The auditing fee is given by

$$F = \lambda_a(1-s^*)pT\mu^2 + as^{*2}T^2 + b.$$

Since $(1-s^*)pT = \frac{(1-s^*)^2}{s^{*2}}$ and s^*T both increase with T, F also increases with T. With blockchains, as long as the decrease in auditing fee is more than the cost of maintaining the blockchain system c, the auditing fee will decrease. Q.E.D.

Proof of Proposition 6.

In the regulated auditing model, we only need to show that the regulator's equilibrium objective without the blockchain adoption cost c,

$$\lambda_r(1-s^*)(1-t^*)p^*T\mu^2 + et^{*2}T^2 + f, \tag{A18}$$

increases with T, since it then follows that the social planner's objective at $T = T_2$ (full adoption) is lower than that at $T = T_0$ (no adoption) as long as c is sufficiently small. By (A11), the first term of (A18) is equal to

$$\lambda_r(1-s^*)(1-t^*)p^*T\mu^2 = l\frac{(1-s^*)^2}{s^{*2}}(1-t^*),$$

for some constant l independent of T. Since $\frac{\partial s^*}{\partial T} < 0$, we only need to show that $\frac{\partial t^*}{\partial T} < 0$. From (A11), (A13), and (A14),

$$t^* = l\frac{(1-s^*)^2}{s^{*2}T^2} = l\frac{(1-s^*)^2 s^{*\frac{1}{2}}}{(s^{*5}T^4)^{\frac{1}{2}}} = l'\frac{(1-s^*)^2 s^{*\frac{1}{2}}}{(1-s^*)^{\frac{3}{2}}} = l'\left((1-s^*)s^*\right)^{\frac{1}{2}},$$

with constants l and l' independent of T. When T is large enough, $s^* \leq \frac{1}{2}$, and $\frac{\partial}{\partial T}\left((1-s^*)s^*\right) = (1-2s^*)\frac{\partial s^*}{\partial T} < 0$. Therefore, $\frac{\partial t^*}{\partial T} < 0$. Q.E.D.

Proof of Proposition 7. The FOCs for s and s_D from the auditor's objective (19) are as follows:

$$-\lambda\mu^2 pT + 2a(sT + ks_D D)T = 0, \tag{A19}$$

$$-\lambda\mu^2 p_D D + 2a(sT + ks_D D)kD = 0. \tag{A20}$$

These imply that in equilibrium,

$$p = \frac{p_D}{k} = \frac{2a(sT + ks_D D)}{\lambda\mu^2}.$$

The FOCs for p and p_D from the client's objective are

$$\gamma\mu T(1-s) - 2\delta(spT + s_D p_D D)sT = 0, \tag{A21}$$

$$\gamma\mu D(1-s_D) - 2\delta(spT + s_D p_D D)s_D D = 0. \tag{A22}$$

This implies that in equilibrium,

$$\frac{1-s}{s} = \frac{1-s_D}{s_D} = \frac{2\delta(spT + s_D p_D D)}{\gamma\mu}.$$

Since the function $\frac{1-x}{x}$ is monotone, $s = s_D$.

Now from (A19) and (A21), the equilibrium conditions can be easily written as

$$s = s_D = \frac{\lambda p \mu^2}{2a(T + kD)},$$
$$p = \frac{p_D}{k} = \frac{\gamma(1-s)\mu}{2\delta s^2 (T + kD)}.$$

Note that this gives the *same solution* to the model with nondiscretionary accounts (as in Proposition 1) and total transaction volume $T + kD$. Q.E.D.

Proof of Proposition 8. From Proposition 7, in the full adoption equilibrium, the equilibrium strategies of the auditor, (s_b^*, s_{bD}^*), and the client, (p_b^*, p_{bD}^*) satisfy $s_{bD}^* = s_b^*$ and $p_{bD}^* = kp_b^*$. Further, (s_b^*, p_b^*) are the same as the equilibrium strategies in the full adoption equilibrium with only nondiscretionary transaction (Proposition 3) and total transaction volume $T_{nb} + kD$. Let (s^*, s_D^*, p^*, p_D^*) be the equilibrium strategies without blockchains. By Propositions 3 and 7,

$$s_b^* > s^*, \quad p_b^* < p^* \tag{A23}$$
$$s_b^*(T_{nb} + kD) < s^*(T + kD). \tag{A24}$$

Therefore, $p_b^* T_{nb} < p_b^* T < p^* T$ and $p_{bD}^* D = k p_b^* D < k p^* D = p_D^* D$, i.e., the client misstates less in both nondiscretionary and discretionary accounts. We also have

$$s_{bD}^* D = s_b^* D > s^* D = s_D^* D, \tag{A25}$$

i.e., the auditor chooses a larger auditing sample for discretionary auditing. Equations (A24) and (A25) imply that $s_b^* T_{nb} < s^* T$, i.e., the auditor selects a smaller auditing sample when auditing nondiscretionary transactions. Given the mapping of the equilibria with discretionary auditing to the equilibria with only nondiscretionary auditing with modified total volumes ($T_{nb} + kD$ and $T + kD$), Proposition 3 implies that both auditor risk and auditing fee decrease. Q.E.D.

References

Allison, Ian, 2018, ING bank launches zero-knowledge tech for blockchain privacy, *Coindesk*, Oct. 22.

Alsabah, H, and A. Capponi, 2019, Pitfalls of Bitcoin's Proof-of-Work: R&D Arms Race and Mining Centralization, Working paper.

Antle, Rick, and Barry Nalebuff, 1991, Conservatism and auditor-client negotiations, *Journal of Accounting Research* 29, Studies on Accounting Institutions in Markets and Organizations, 31-54.

Bajpai, Prableen, 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. In *The Economic Dimensions of Crime* (pp. 13-68). Palgrave Macmillan, London.

Blum, Manuel, Paul Feldman, and Silvio Micali, 1988. Non-interactive zero-knowledge and its applications. *Proceedings of the 20th Annual ACM Symposium on Theory of Computing*, STOC '88, 103-112.

Bunz, Benedikt, Jonathan Bootle, Dan Boneh, Andrew Poelstra, Pieter Wuille, and Greg Maxwell, 2018. Bulletproofs: Short proofs for confidential transactions and more. *2018 IEEE Symposium on Security and Privacy*, 319-338.

Callen, Jeffrery, Hai Lu, and Mozaffar Khan, 2013. Accounting Quality, Stock Price Delay, and Future Stock Returns, *Contemporary Accounting Research* 30 (1), 269-295.

Caskey, J., Nagar, V. and Petacchi, P., 2010. Reporting bias with an audit committee. *The Accounting Review*, 85(2), 447-481.

Chiu, J. and Koeppl, T.V., 2017. The economics of cryptocurrencies–bitcoin and beyond. Available at SSRN 3048124.

Chod, Jiri, and Evgeny Lyandres, 2018, A Theory of ICOs: Diversification, Agency, and Information Asymmetry, *Working Paper*.

Chod, Jiri, Nikolaos Trichakis, Gerry Tsoukalas, Henry Aspegren, and Mark Weber, 2019,

On the Financing Benefits of Supply Chain Transparency and Blockchain Adoption, *Forthcoming, Management Science*.

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

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

Cong, Lin William, 2018, Blockchain economics for investment professionals, *Invited for Publication in Journal of Institutional Investors*.

Cong, Lin William, and Zhiguo He, 2018, Blockchain disruption and smart contracts, *Forthcoming*, *Review of Financial Studies*.

Cong, Lin William, Zhiguo He, and Jiasun Li, 2018, Decentralized mining in centralized pools, *Working Paper*.

Cong, Lin William, Ye Li, and Neng Wang, 2018, Tokenomics: Dynamic adoption and valuation, *Working Paper*.

CPA Canada, AICPA, and the University of Waterloo, 2018, Blockchain technology and its potential impact on the audit and assurance profession.

Dai, J., and M.A., Vasarhelyi, 2017, Toward Blockchain-based accounting and Assurance. Journal of Information Systems. 31(3), 5-21.

DeAngelo, Linda Elizabeth, 1981, Auditor independence, "low balling", and disclosure regulation, *Journal of Accounting and Economics* 3 (2), 113-127.

Deloitte, 2016, Blockchain technology: A game-changer in accounting?

Deng, Mingcherng, Tong Lu, Dan A. Simunic, and Minlei Ye, 2014, Do joint audits improve or impair audit quality? *Journal of Accounting Research* 52 (5), 1029-1060.

Easley, David, Maureen O'Hara, and Soumya Basu, 2018, From mining to markets: The evolution of bitcoin transaction fees, *Journal of Financial Economics, Forthcoming*.

Falk, Brett Hemenway, and Gerry Toukalas, 2019, Token Weighted Crowdsourcing, *Working Paper*.

Fellingham, J., and D. Newman, 1985, Strategic considerations in auditing, *The Accounting Review* 60 (4), 634-650.

Fiat, Amos, and Adi Shamir, 1986. How to Prove Yourself: Practical Solutions to Identification and Signature Problems. CRYPTO '86, 186-194.

Financial Executives International (FEI), 2018, Blockchain and the future of financial reporting, Available at https://www.financialexecutives.org/Research/News/2017/Blockchain-and-the-Future-of-Financial-Reporti-(1).aspx

Fischer, P.E. and Verrecchia, R.E., 2000. Reporting bias. *The Accounting Review* 75(2), pp.229-245.

Friedman, H.L. and Mahieux, L., 2018. Market Interactions between Audit and Non-Audit Services: Bundling, Bans, and Competition. Working Paper.

Gao, P., & Zhang, G. 2018. Accounting manipulation, peer pressure, and internal control. *Journal of Accounting Research* 52 (5), 1029-1060.

Goldwasser, Shafi, Silvio Micali, and Charles Rackoff, 1989. The knowledge complexity of interactive proof systems. *SIAM Journal on Computing*, 18(1), 186-208.

Halaburda, H. and Sarvary, M., 2015, Beyond Bitcoin: The economics of digital currencies, *Palgrave Macmillan*

Harvey, Campbell R, 2016, Cryptofinance, *Working Paper*.

Hayek, F. A., 1945. The use of knowledge in society. *American Economic Review*, 35(4), 519-530.

Hinzen, F., Kose John, and Fahad Saleh, 2019, Proof-of-Work's Limited Adoption Problem, *Working Paper*.

ING, 2017, Blockchain transactions just got a lot safer, *Company News Release*, Nov. 16.

Karajovic, M., Kim, H.M. and Laskowski, M., 2017. Thinking outside the block: Projected phases of blockchain integration in the accounting industry. *Australian Accounting Review*.

Liberti, J.M., Sturgess, J. and Sutherland, A., 2018. Economics of voluntary information sharing. Available at SSRN 3068461.

Lu, Hai, Gordon Richardson, and Steve Salterio, 2011, Direct and Indirect Effects of Internal

Control Weakness and External Audit Effort on Accruals Quality: Evidence from a Unique Canadian Regulatory Setting, *Contemporary Accounting Research* 28 (2), 675-707.

Lu, Tong, 2006, Does opinion shopping impair auditor independence and audit quality, *Journal of Accounting Research* 44 (3), 561-583.

Magee, Robert P., and Mei-Chiun Tseng, 1990, Audit pricing and independence source, *The Accounting Review* 65 (2), 315-336.

Mearian, Lucas, 2018, Coming soon: Public blockchains for private business data, *ComputerWorld*, Nov. 6.

Murphy, Kevin M., Andrei Shleifer, and Robert W. Vishny, 1989, Industrialization and the big push, *Journal of Political Economy* 97 (5), 1003-1026.

Nagar, V. and Petacchi, P., 2016. A Model of Aggregate Reporting Quality. *Journal of Financial Reporting*, 1(2), 1-19.

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

Newman, D. Paul, Evelyn Patterson, and Reed Smith, 2001, The influence of potentially fraudulent reports on audit risk assessment and planning, *The Accounting Review* 76 (1), 59-80.

Newman, D. Paul, Evelyn Patterson, and Reed Smith, 2005, The role of auditing in investor protection, *The Accounting Review* 80 (1), 289-313.

Patterson, Evelyn, 1993, Strategic sample size choice in auditing, *Journal of Accounting Research* 31 (2), 272-293.

Patterson, Evelyn, and Reed Smith, 2003, Materiality uncertainty and earnings misstatement, *The Accounting Review* 78 (3), 819-846.

Pillar, 2018. Machine Learning for Encrypted Blockchains -- Sandy Pentland, MIT, *Medium*, Jun 26. Available at https://medium.com/pillar-companies/machine-learning-for-encrypted-

blockchains-sandy-pentland-mit-79c2d18eaf.

PCAOB, 2015, Staff Inspection Brief, Vol. 2015/2, Washington, DC.

Rackoff, C., and D.R., Simon, 1991, Non-interactive Zero-knowledge Proof of Knowledge and Chosen Ciphertext Attack. Annual Internationl Cryptology Conference.

Schoenberger, C., 2018, Blockchain's weakest links, *Chicago Booth Review,* Nov 26. Available at http://review.chicagobooth.edu/economics/2018/article/blockchain-s-weakest-links.

Scott, William R., 1973, A Bayesian approach to asset valuation and audit size, *Journal of Accounting Research* 11 (2), 304-330.

Shleifer, A. and Vishny, R.W., 1989. Management entrenchment: The case of manager-specific investments. *Journal of Financial Economics*, 25(1), 123-139.

Shibano, Toshiyuki, 1990, Assessing audit risk from errors and irregularities, *Journal of Accounting Research* 28, Studies on Judgment Issues in Accounting and Auditing, 110-140.

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

Simunic, Dan A., Minglei Ye, and Ping Zhang, 2017, The joint effects of multiple legal system characteristics on auditing standards and auditor behavior, *Contemporary Accounting Research* 34(1), 7-38.

Smith, S., 2018. Blockchain augmented audit–benefits and challenges for accounting professionals. *Journal of Theoretical Accounting Research*, 14(1), pp.117-137.

Smith, Reed, Samuel L. Tiras, and Sansakrit S. Vichitleckarn, 2000, The interaction between internal control assessment and substantive testing in audits for fraud, *Contemporary Accounting Research* 17 (2), 327-356.

Strobl, Günter, 2013, Earnings manipulation and the cost of capital, *Journal of Accounting Review* 51 (2), 449-473.

Stubben, Stephen R., 2010, Discretionary revenues as a measure of earnings management, *The Accounting Review* 85 (2), 695-717.

Teoh, Siew Hong, 1992, Auditor independence, dismissal threats, and the market reaction to auditor switches, *Journal of Accounting Research*, 30 (1), 1-23

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

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

Wang, Yunsen, and Alexander Kogan, 2018. Designing confidentiality-preserving Blockchain-based transaction processing systems, *International Journal of Accounting Information Systems*, 30 (C), 1-18.

Yermack, David, 2017, Corporate governance and blockchains, *Review of Finance* 21 (1), 7-31.

Zhao, Wolfie, 2018, All "Big four" auditors to trial blockchain platform for financial reporting, *Coindesk*, July 19.