Auditing and Blockchains: Pricing, Misstatements, and Regulation

Sean Cao, Lin William Cong, and Baozhong Yang*

This Draft: November 2018

Abstract

To understand the implications of blockchains for financial reporting and auditing, we analyze auditor competition, audit quality, client misstatements, and regulatory policy all in a unified framework. We demonstrate how collaborative auditing using a federated blockchain can improve auditing efficiency for not only transactions recorded on proprietary databases, but also cross-auditor transactions through zero-knowledge protocols that preserve data privacy. Consequently, the technology disrupts conventional audit pricing and effort focus: Auditors charge competitive fees based on clients' counter-parties' auditor association and corresponding transaction volume instead of client size. Blockchains also reduces 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.

JEL Classification: D21, D40, M42, M48
Key Words: Blockchain, FinTech, Financial Reporting, Collaborative Auditing, Audit Pricing, Audit Sampling, Auditor Risk, PCAOB, Technology Adoption

*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, Bob McDonald, Haresh Sapra, and Larry Wall for detailed feedback and discussion. They also thank Vikas Agarwal, Mark Chen, Matthew DeAngelis, Dalida Kadyrzhanova, Yongtae Kim, W. Robert Knechel, Anya Kleymenova, Clive Lennox, James ("Robbie") Moon, Jr., Curtis Mullis, Mark Peecher, Lin Peng, Shivaram Rajgopal, Ajay Subramanian, Lawrence J. White, Baohua Xin, Mao Ye, and participants at Ant Financial Workshop, DataYes & ACM KDD China FinTech×AI Workshop, Federal Reserve Bank of Atlanta Conference on New Technologies and Financial Stability, PCAOB/JAR Conference on Auditing and Capital Markets, and Georgia State University Workshops at the Departments of Accountancy, Computer Science and Finance 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

The Public Company Accounting Oversight Board (PCAOB) has been constantly seeking ways to improve audit efficiency and quality. One main source of auditing cost comes from the auditors' acquiring information about the transactions of clients and their transaction counterparties for verification. While each audit firm or team (generically referred to as "auditor") may possess information useful to other auditors, each one's auditing process is traditionally independent 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 the legal requirements concerning data privacy (e.g., General Data Protection Regulation). The labor-intensive and mechanical transaction verifications hinder audit firms' ability to devote greater efforts to auditing discretionary accounts and transactions which entail greater value added.

Meanwhile, blockchains have taken the central stage of technology innovation in business. It is widely believed to allow industry-wide collaboration (e.g., R3 CEV) and disrupt corporate governance, industrial organization, payments, and entrepreneurial finance (e.g., Yermack (2017), Cong and He (2018), Cong, Li, and Wang (2018)). Among the various advances, media and industry pay increasing attention to blockchain applications in the world of auditing.[1] Although all Big 4 audit firms are devoting large resources to blockchain 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

[1]Cohn (2016) reports that big accounting firms have investigated the use of blockchains and a "triple-entry accounting" system. Deloitte (2016) describes how a blockchain-based accounting system might work and how would it enhance the current accounting practice. 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)).

industry and what auditors' new role would be with the emerging technology.[2]

This study takes an initial step towards understanding these issues by examining how blockchain technology disrupts traditional audit processes and enables auditor collaboration. Our contributions are three-fold: (1) We detail the functionality of a collaborative audit process, which capitalizes on a federated blockchain and zero-knowledge proof, on 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 by making all transactions openly accessible, they are not suitable in settings where client information needs to stay private. Consequently, many auditors develop private blockchains as an upgrade to their data systems. What is left out of the discussion is the possibility to connect isolated audit processes across audit 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 counter-party directly to request records and manually confirm with clients' transaction parties. A federated blockchain using zero-knowledge protocol can potentially

[2]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), CPA Canada, AICPA, and University of Waterloo (2018)). Recent efforts of accounting firms center on buiding in-house blockchain capabilities and services (e.g. Bajpai (2017), CNN (2018)).

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.

Several features of the blockchain technology allow auditors to collaborate to automate information verification of clients' transactions with minimal sharing of clients' private information.[3] For example, thanks to the peer-to-peer (within a consortium) design of blockchain, this collaboration among auditors does not require a central or third party to monitor or intermediate. In addition, the encryption methods developed in blockchain and zero-knowledge proof also allow information providers in this federated blockchain system to safeguard proprietary client information while confirming certain transactions.[4] Such zero-knowledge proof/protocols have been well-developed and have led to recent applications for facilitating bank communications (ING, 2018) and in public blockchains such as Zcash and Ethereum.[5] Futhermore, the immutable nature of blockchain also makes it easier for the PCAOB to inspect auditing processes and prevent audit firms or hackers to revise recorded transaction data ex post (Section 2 contains more details) .

We take the above blockchain functionalities as given and examine how auditors and clients respond. Specifically, our model features two auditing firms and two representative clients. Without blockchains, auditing firms compete for clients along the dimension of fees

[3]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 mis-reporting 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 more timely, and retrospective manipulations and mis-reporting can be prevented.

[4]Utilizing private data while preserving data privacy is not a 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).

[5]Zcash is a cryptocurrency that preserves anonymity of users based upon a zero-knowledge proof algorithm, zkSNARK. Ethereum started to support the zkSNARK algorithm in one of its recent update, Byzantium in 2017.

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, auditing costs of transactions among clients within the auditor are significantly reduced, but auditing transactions across auditors remain 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 audit 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 the 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 to 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 allows skilled auditors to truly add value. On the client side, when both auditors adopt blockchains, clients report more truthfully for both transactions recorded on blockchains and discretionary accounts, leading to a lower auditor risk and a lower overall audit cost.

The auditors' technology adoption exhibits strategic complementarity because the cost of auditing cross-auditor transactions goes down when both auditors adopt. When clients

value strongly 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 have a potential role of coordinating an industry-wide adoption when the technology matures sufficiently, 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 power. 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 the 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 adoption improves the efficiency of audit sampling by allowing auditors to focus on transactions that cannot be automatically verified. Third, adopting the technology discourages clients' 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 our model is distinct from those examining the implications of a general technology on cost reduction. While alternative technologies may be available, federated blockchains with zero-knowledge proof is a leading candidate for effectively improving privacy protection and cross-party verification in a decentralized system — evident in that technology firms such as R3 CEV and Spring Labs all choose blockchains for facilitating industry-wide collaboration or cross-organization verification and information sharing.

As a first study on blockchain implications for financial reporting and auditing, we have abstracted away from the details of several features observed in real life. We only briefly touched on the impact on discretionary accounts such as bad debt expense, and on the nuanced impact on the auditor labor market. Finer details on these issues, albeit interesting, are not crucial for the economic insights our model delivers. It is our hope that future studies can incorporate them and enrich our framework to further our understanding of the technology's impact on financial reporting and auditing.

Literature — Our paper contributes to the emerging literature on FinTech and blockchain. Focusing on the underlying mechanisms of blockchain and consensus generation, Eyal and Sirer (2014) and Biais, Bisiere, Bouvard, and Casamatta (2017) study mining games involving proof-of-work, whereas Saleh (2018) explores proof-of-stake as an alternative consensus protocol. Cong and He (2018) emphasize information distribution in generating decentralized consensus, with implications for firm competition. Easley, O'Hara, and Basu (2017) and Huberman, Leshno, and Moallemi (2017) examine the market microstructure and transaction fee dynamics of bitcoin. Cong, He, and Li (2018) study mining pools' industrial organization and impact on global energy consumption associated with cryptocurrency mining.

Concerning blockchain applications, Halaburda and Sarvary (2015) and Harvey (2016)

discuss digital currencies and crypto-finance. Yermack (2017) evaluates the potential impacts of the technology 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 research on blockchain, including both theoretical and empirical studies on initial coin offerings (e.g., Li and Mann (2018), Sockin and Xiong (2018), and Howell, Niessner, and Yermack (2018)), and discusses blockchain economics and implications for investment professionals.

Our study 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 report 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)).

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 on auditor pricing, auditor sampling, clients' incentives for misstatement, and regulation. We differ from earlier studies in our focus on permissioned blockchains, and in jointly analyzing the auditor competition and adoption games. 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.

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 discusses regulation and policy. Section 5 extends the model to incorporate discretionary accounts. Section 6 concludes. The appendix contains all the proofs.

2. Institutional Background

In this section, we explain the basic auditing process for transaction-based, non-discretionary accounts (simple revenue and transaction records) 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 blockchains and the concept of zero-knowledge proof.

Suppose client firms' income statements are as shown in Figure 1.[6] Auditors' primary job is to verify the accuracy of net income and prevent the occurrence of restatement. To this end, auditors need to verify sales and expenses of their clients. Clients have incentive to overstate their sales and underestate 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 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

[6]We do not include cash receipts because it is easily verified.

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.[7]

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. 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 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

[7]Auditors can also outsource such labor-intensive cross-party verification to a third party such as confirmation.com

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 crypographic verification method, i.e., zero-knowledge proof, that allows confirmation on the federated blockchain without revealing proprietary information.

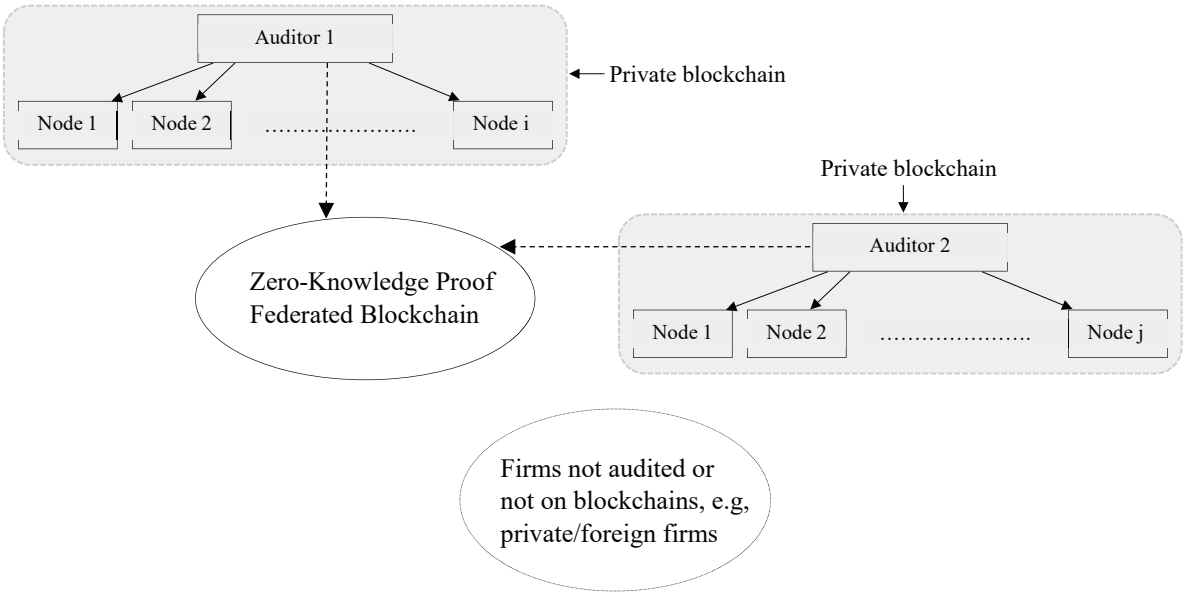

Figure 2: **Structure of the Federated Blockchain**

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.[8] As shown in Figure 3, for a transaction between two client firms audited by different

[8]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, e.g., Allison (2018).

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 and following a zero-knowledge proof/protocol, no other auditors can retrieve transaction information from them, consistent with the peer-to-peer design of blockchain's elimination of the requirement of a centralized party. 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 directly to request records and verify the information.

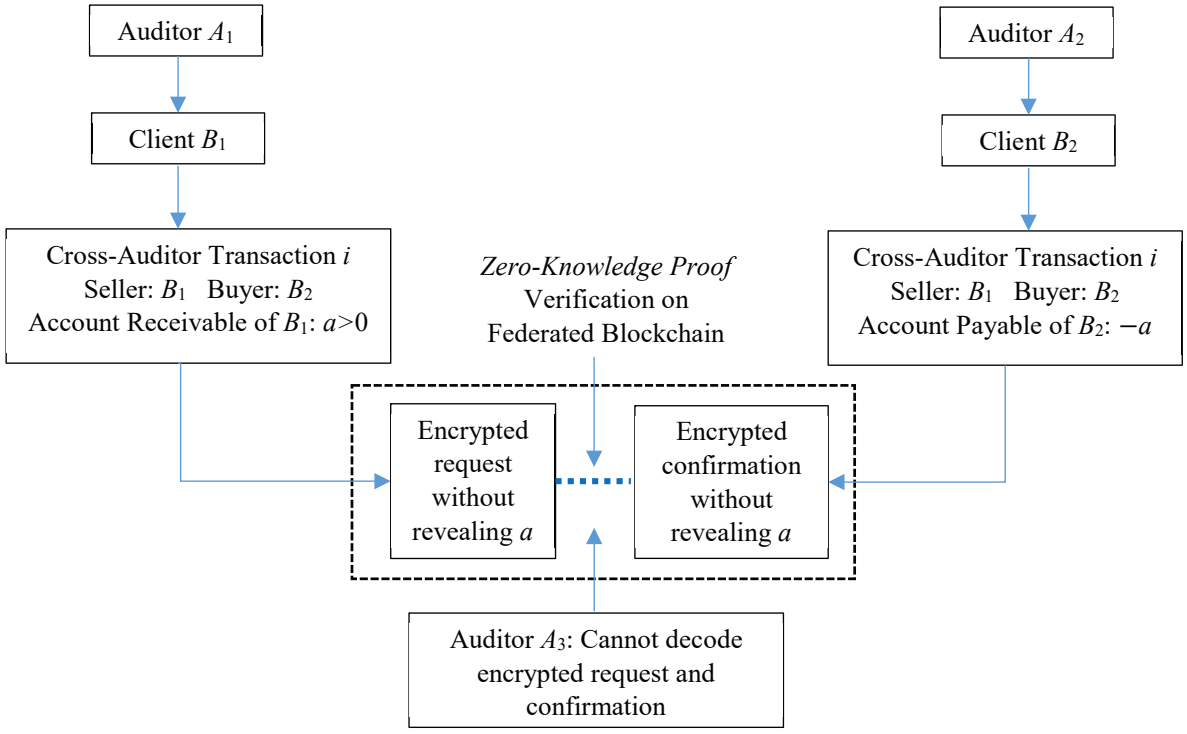

Figure 3: **Transaction Verification on a Peer-to-Peer Federated Blockchain**

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. Without blockchains, cross-party information verification is done manually; that is, audit teams manually check the information of the two parties in the transaction. However, 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, two parties in the transaction are audited by different audit firms, each residing in a separate blockchain ecosystem. In this case, 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 can be significantly smaller than the entire sample that requires manual labor without blockchain.

Overall, three technological features of blockchain are condusive to the auditing process: 1) decentralization: the peer-to-peer design of blockchain eliminates the requirement of a trusted central party; 2) encryption: the zero-knowledge proof method allows encrypted communication that preserves client privacy; 3) 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 analytically show the implications of this federated blockchain for auditors, clients, and the regulator.

Finally, we should clarify that even though we refer to the blockchain system 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. Even better 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. This way, costs on maintaining the databases are lower and the concern of recording a transaction wrongly is mitigated in the first place.

We also should point out that while other technologies (such as centralized databases) can also help to facilitate communication among auditors, federated blockchains with zero-knowledge proof is a leading candidate because they provide systematic and ready-to-use algorithms and infrastructure with key benefits such as privacy protection, decentralization, and immutability. For example, if incentives to manipulate or modify transaction records ex post arise, an optimized SQL system would be compromised for auditing but a federated blockchain would not because of the immutability through the one-way hashing functions connecting the blocks.

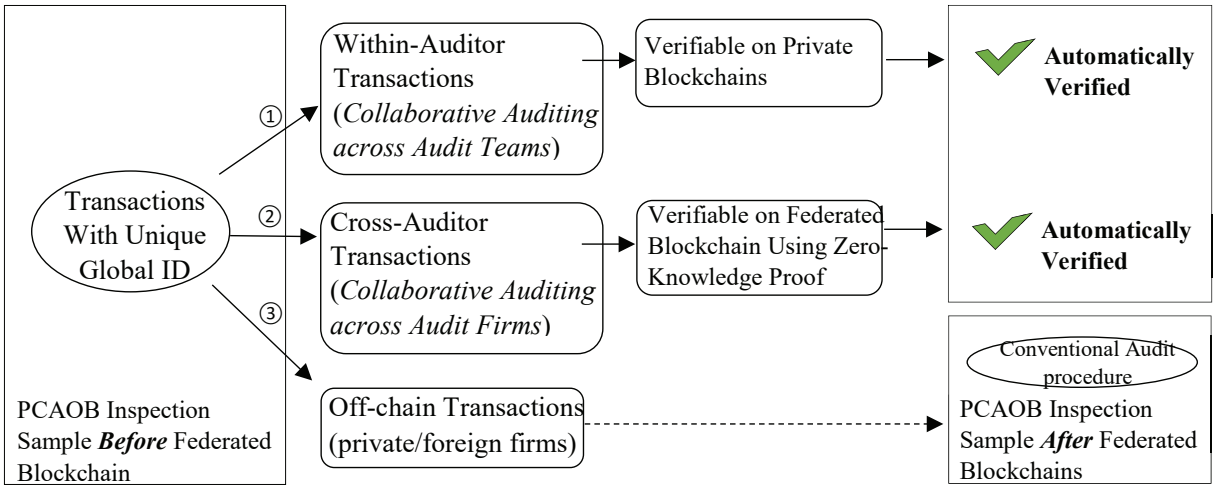

Figure 4: **Auditing Transactions with the Blockchain**

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 and homogeneous.[9] 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, supposing one client has chosen an auditor, it submits 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:

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

[9] 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.

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 incentives to overstate transaction values (e.g. Newman, Patterson, and Smith (2001), Patterson and Smith (2005)). Allowing the error term to represent genuine mistakes or understatement of transaction value does not alter the economic intuition or qualitative results.[10]

For each transaction, the auditor obtains his own estimate $\hat{a}_i$ and computes the aggregate income of the client as $\int_0^T \hat{a}_i di$. Similar to 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:

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

where $\lambda \in (0,1)$ is a scaling parameter reflecting the expected penalty faced by the auditing firm due to PCAOB and market monitoring and misstatement detection. 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 decides to audit a fraction $s \in [0,1]$ of all transactions, and the cost of such auditing sampling to be $C(s)$, with $C'(s) > 0$ and $C''(s) > 0$ (Lu (2006)). The convexity of the function captures the fact that it is costly to acquire and retain additional human resources in the auditing season. For simplicity, we assume it costs the same to audit a within-auditor transaction and a cross-

[10]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, either made by clients or auditors, which further improves audit quality and reduces costs of internal auditing.

auditor transaction.[11] 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,

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

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/ fraud (which damages the reputation of the firm and entails regulatory penalty). We assume that the client maximizes the following second-stage utility function,

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

where $\gamma, \delta > 0$. $\Pr(\hat{a}_i = a_i > \tilde{a_i})$ is the probability that the manager successfully overstates transaction values without being detected by the auditor, and $\Pr(\hat{a}_i = \tilde{a}_i < a_i)$ 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.

Note that since the auditor randomly investigates a sample s:

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

[11] 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 our model implications.

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

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 equal to

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

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 parame-*

ter 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 tends to increase 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 sample 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.[12] The auditors compete for clients by posting auditing fees. Now 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 of auditing fees, thus the auditors indeed charge the minimum fee.

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

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

to verify a representative sample. Therefore, the client has a greater propensity to overstate 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 for 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, the 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. 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 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. 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

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 global transaction identifiers across clients and auditors can be very costly (e.g., Global Legal Entity Identifier System).[13] 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

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

[13] 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 because 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 about auditors having vested interests and catering 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 fee is the only way for it to signal and to make clients believe it 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 saves auditing cost for the auditor because the other auditor is already using blockchain in equilibrium. Therefore, it 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 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 clients' 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 the region with full adoption equilibrium shrinks. This is due to that clients with very low γ misreports less, reducing the benefits of adopting blockchains netting costs.

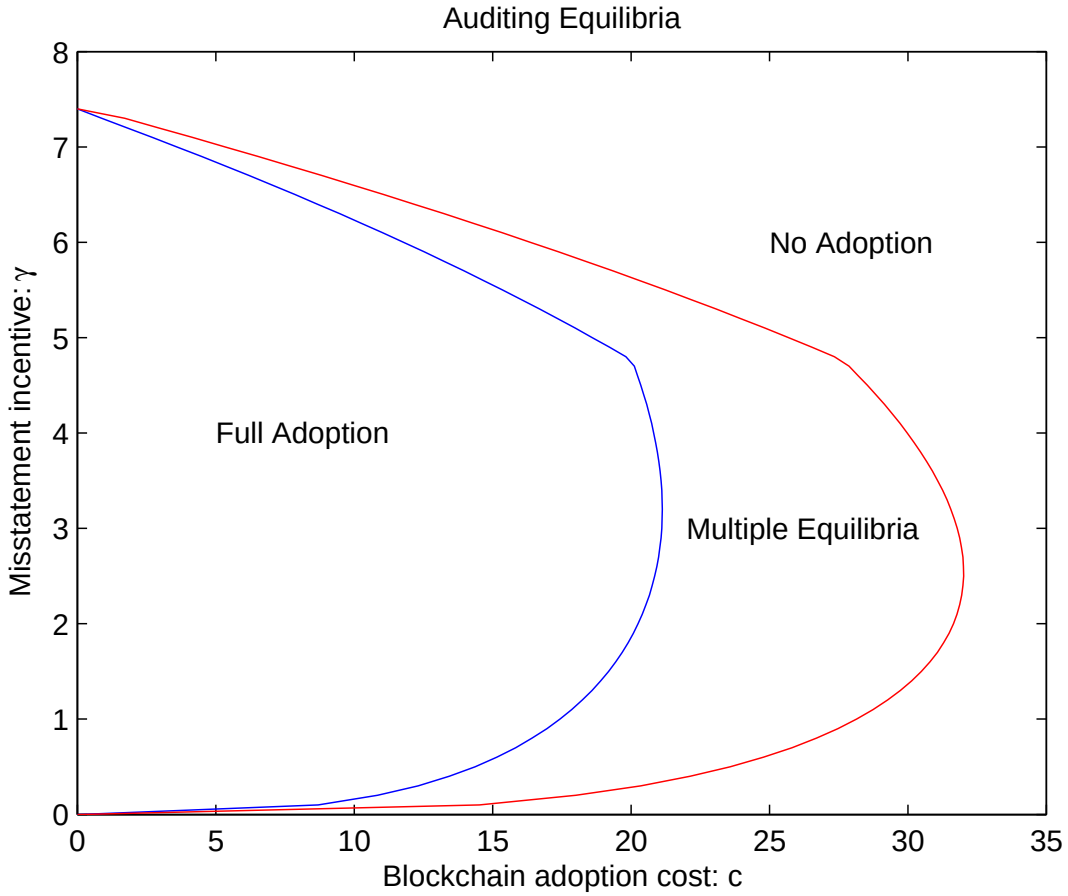

Figure 5: **The Evolution of Equilibrium Adoption of Blockchains** Parameters are $K = 5, K_{pr} = 0.4, \mu = 1, \delta = 1, \lambda = 1, a = 0.05, b = 0$.

Non-collaborative Auditing

One can also consider the case where each auditor operates its 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 1. *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. PCAOB 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.[14] 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 assume in general that the auditor's risk function is of the form

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

Parameter $\lambda > 0$ 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 to the regulator's inspection propensity t since the probability of finding a discrepancy is proportional to t. The auditor's objective thus becomes

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

This can be simplified to

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

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

The client's incentive is the same as given in (8). We note that when there are no regulatory costs, i.e., $e = f = 0$, the regulator always monitors with $t = 1$ and the client's and auditor's problems take the same form as those in the unregulated model considered before.

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 with the regulatory cost parameter* e *and the misstatement sample* p^*T *is weakly decreasing.*

When regulatory costs are reduced, auditors face more scrutiny from the regulator and need to boost their auditing samples to avoid greater potential punishment due to discrepancies. As a result, clients misreport less. Therefore, a reduction in regulatory costs is beneficial for audit quality. Another implication of the proposition is that lower regulatory cost lead to greater auditor independence since auditors have to exert more effort, *ceteris paribus*. Regulatory cost 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

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

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 blockchains, 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, the adoption of blockchains 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 the coordination of auditors.

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' learning cost of the new system. Second, collaborative auditing necessitates 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 or social planner to coordinate adoption. The following proposition formalizes this intuition. In the unregulated auditing model, we assume the social planner's objective function is the same as that of the auditor since the auditor is the sole monitor of clients. In the regulated auditing model, the social planner's objective is the regulator's objective defined above (Equation (14)) plus the auditing costs, since a social planner also wants to decrease deadweight costs.

Proposition 6. *Assume there exist multiple equilibria, then*

1) In the unregulated auditing model, the social planner always strictly prefers the full adoption equilibrium to the no adoption equilibrium.

2) If the regulated auditing model, if the adoption cost c is sufficiently small, then the social planner 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 but the adoption cost is still non-trivial. For

example, PCAOB can impose regulatory standards or coordinate the development of the underlying infrastructure of blockchains.

Instead of directly influencing auditors' adoption of the new technology, a regulator can alternatively 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 can 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 extremely high. Although not explicitly modeled here, this channel is intuitive once added to 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.

5. Discretionary Accounts and Blockchains

In the models considered in previous sections, clients have transaction-based accounts. As we 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 trasaction-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

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

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 (19) 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 efforts for 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 blockchains, 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.

6. Conclusion

In this study, we analyze equilibrium outcomes of financial reporting and auditing in settings with and without the blockchain technology. 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 auditing in a transparent manner, we have abstracted away from 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 more future research about how technological advances impact financial

reporting and auditing.

Appendix

Proof of Proposition 1. The system of FOC equations are

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

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

Consider the two curves on the $s-p$ plane determined by Equations (A1) and (A2). Define $g(s) = \frac{2asT}{\mu^2}$ 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 $\frac{\partial p^*}{\partial a} > 0$. Similarly, from (A3), we have $\frac{\partial s^*}{\partial T} < 0$. (A3) then implies that

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

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

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

which is again increasing with 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),

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

also increases with 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 $C(T)$ and $F(T)$ as the second-stage utilities of the client and auditor, respectively. In other

words,

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

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

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 blockchains, when only the given auditor adopts blockchain, and when no auditor adopts blockchains, 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 (and potentially attract the client from the other auditor), the following client incentive condition has to be satisfied:

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

Therefore, the auditor's no-deviation condition is

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

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 blockchains, 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

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

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 blockchains, 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 utility $C(T_1)-f(T_1)-c$ while the other client has utility $C(T_0) - f(T_0)$. For the auditor with blockchain not to deviate, the condition is

$$C(T_1) - f(T_1) - C(T_0) + f(T_0) \geq c.$$

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

$$C(T_2) - f(T_2) - C(T_0) + f(T_0) \leq c.$$

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

In the full adoption equilibrium, the comparative statics of $s_T, p_T, s_T T$ and $p_T T$ 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 $C(T_2) < C(T_0)$. The auditor risk also decreases, by Proposition 2. Q.E.D.

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

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

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

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

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

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

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),

$$t^* = \frac{\lambda_r\mu^2}{2T}\frac{(1-s^*)p^*}{e} = \frac{\gamma\lambda_r\mu^2}{4\delta T^2}\frac{(1-s^*)^2}{es^{*2}} = c_1\frac{(1-s^*)^2}{\frac{(1-s^*)^3}{s^{*3}}} = c_1\frac{s^{*3}}{1-s^*},$$

where c_1 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

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

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

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

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

$$c_2(s^{*4}T^4) = \frac{(1-s^*)^3}{s^*},$$

for some constant c_2 independent of T. Since the right hand side increases with T, so does the left hand side and s^*T. Fom Equation (A11), $p^*T = \frac{\gamma\mu(1-s^*)}{2\delta s^{*2}}$ increases with T. From (A13) and (A14),

$$\begin{aligned} tT &= \frac{\lambda_r\mu^2}{2e}(1-s^*)p^* = c_3\frac{(1-s^*)^2}{s^{*2}T} = c_3\frac{(1-s^*)^2}{(s^{*5}T^4)^{\frac{1}{4}}s^{*\frac{3}{4}}} \\ &= c_4\frac{(1-s^*)^2}{(1-s^*)^{\frac{3}{4}}s^{*\frac{3}{4}}} = c_4\frac{(1-s^*)^{\frac{5}{4}}}{s^{*\frac{3}{4}}}, \end{aligned}$$

where c_3 and c_4 are independent of T. Therefore, $\frac{\partial(t^*T)}{\partial T} > 0$.

The auditing fee is given by

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

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, auditing fee will decrease. Q.E.D.

Proof of Proposition 6. In the unregulated model, by assumption, the social planner's utility is the same as that of the auditor. Since the full-adoption equilibrium exists, (A9) holds. Therefore,

$$F(T_0) - (F(T_2) + c) \geq C(T_0) - C(T_2) \geq 0.$$

The last inequality follows from the fact that $C(T)$ is increasing with T (Proposition 1 and Equation A5). This means that the auditor/social planner achieves a lower objective or higher utility under the full adoption equilibrium.

In the regulated auditing model, we only need to show that the social planner's equilibrium

objective without the blockchain adoption cost c,

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

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. From Proposition 5, s^*T and t^*T and hence the part after the first term increases with T. By (A11), the first term of (A18) is equal to

$$\lambda_r(1-s^*)(1-t^*)p^*T\mu^2 = c_5\frac{(1-s^*)^2}{s^{*2}}(1-t^*),$$

for some constant c_5 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),

$$t^* = c_6\frac{(1-s^*)^2}{s^{*2}T^2} = c_6\frac{(1-s^*)^2 s^{*\frac{1}{2}}}{(s^{*5}T^4)^{\frac{1}{2}}} = c_7\frac{(1-s^*)^2 s^{*\frac{1}{2}}}{(1-s^*)^{\frac{3}{2}}} = c_7\left((1-s^*)s^*\right)^{\frac{1}{2}},$$

with constants c_6 and c_7 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 $p_{bD}^* D = kp_b^* D < kp^* D = p_D^* D$, i.e., the client misstates less in

both nondiscretionary and discretionary accounts. We also have

$$s^*_{bD}D = s^*_bD > s^*D = s^*_DD, \tag{A25}$$

i.e., the auditor chooses a larger auditing sample for discretionary auditing. Equations (A24) and (A25) imply that $s^*_bT_{nb} < s^*T$, 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, Oct 22, 2018, ING bank launches zero-knowledge tech for blockchain privacy, *Coindesk*.

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.

Biais, Bruno, Christophe Bisiere, Matthieu Bouvard, and Catherine Casamatta, 2017, The blockchain folk theorem, *Working Paper*.

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

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.

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, 2017, From mining to markets: The evolution of bitcoin transaction fees, *Working Paper*.

Eyal, Ittay, and Emin Gun Sirer, 2014, Majority is not enough: Bitcoin mining is vulnerable, in *International Conference on Financial Cryptography and Data Security* pp. 436-454. Springer.

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

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

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

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

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

Howell, Sabrina T., Marina Niessner, and David Yermack, 2018, Initial coin offerings: Financing growth with cryptocurrency token sales, *Working Paper*.

Huberman, Gur, Jacob Leshno, and Ciamac C. Moallemi, 2017, Monopoly without a monopolist: An economic analysis of the bitcoin payment system, *Working Paper*, Columbia Business School.

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

Li, Jiasun, and William Mann, 2018, Initial coin offering and platform building, *Working Paper*.

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.

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.

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

Saleh, Fahad, 2018, Blockchain without waste: Proof-of-stake, *Working Paper*.

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

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, 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.

Sockin, Michael, and Wei Xiong, 2018, A model of cryptocurrencies, *Working Paper*.

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.

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.