Auditing and Blockchains: Pricing, Misstatements, and Regulation

Sean Cao, Lin William Cong, and Baozhong Yang*

First Draft: June 2018; This Draft: September 2018

Abstract

To understand the implications of blockchains for financial reporting and auditing, we study in a unified framework auditor competition for clients, endogenous audit quality and client misstatements, and regulatory policy. We first 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. The technology disrupts conventional audit pricing: instead of pricing based on client size, auditors charge competitive fees dependent on clients' counter-parties' auditor association and corresponding transaction volume. Moreover, blockchain adoption reduces client incentive to misreport and that auditors can reduce sampling costs by focusing on off-chain transactions. Importantly, auditors' adoption of the technology exhibits strategic complementarity, leading to equilibrium multiplicity. A regulator can help select an adoption equilibrium that reduces misstatements as well as auditing and regulatory costs.

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 Yongtae Kim, Anya Kleymenova, James ("Robbie") Moon, Jr., Curtis Mullis, Baohua Xin, and conference and seminar participants at Ant Financial, Georgia State University Accounting and Finance Workshops 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 audit quality. The most costly activity in the auditing process is information acquisition and verification. Auditors need to learn about client transactions or those of their partners to verify transaction amounts. While each audit firm or audit team (also generically referred to as "auditor") possesses useful information that may significantly reduce other auditors' costs of information acquisition, its auditing process is traditionally independent from other audit firms because it is not customary to share proprietary information among audit firms. As a result, 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 laws concerning data privacy such as the General Data Protection Regulation (GDPR).

Meanwhile, blockchain technology has taken the central stage of technology innovation in business, and is widely believed to disrupt traditional practices in 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, "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). Consistent with this view, there is increased media and industry attention on the role of blockchains 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 industry and what auditors' new role would be with the emerging technology. (e.g., Raj

[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)).

(2017)).[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 document the potential 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 and its overall impact on capital markets; 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 has unique needs for blockchain technologies distinct 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 (e.g., http://www.blockchain.info or http://www.blockexplorer.com), they are not suitable in settings where client information privacy needs to be protected. Consequently many auditors develop permissioned private blockchains independently or simply upgrade their own data ecosystems. However, with the technological advancements brought by blockchains, it becomes possible to connect isolated audit processes across audit firms while preserving data privacy. This technology allows auditors to automatically verify whether their clients' transactions are consistent with information from other transaction parties. Examining records from both parties in a transaction is an efficient way of validating a record in the auditing process. Any inconsistency in transaction information between the two parties suggests

[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)). Given the recent efforts of accounting firms buiding in-house blockchain capabilities and services (e.g. Bajpai (2017), CNN (2018)), this study focuses on the latter.

unintentional errors or intentional misstatement. Therefore, this cross-party information verification can make the auditing process more efficient and reliable when detecting fraud, because such 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. Given the importance of cross-party verification, automated verification of clients' transactions in a federated blockchain using zero-knowledge protocol instead of *manually* confirming with clients' transaction parties reduces costs and alters the traditional concept of auditing sampling.[3]

Several features of blockchain technology allow auditors to collaborate to automate information verification of clients' transactions with minimal sharing of clients' private information. 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 not share any client transaction information except for providing confirmations to information requesters. Other auditors cannot infer any information about the clients or the transactions from the request or the confirmation due to blockchain encryption methods. Such zero-knowledge proof protocols have been well-developed and have led to recent applications to facilitate communications between banks (e.g., ING (2018)) and been applied in public blockchains such as Zcash and Ethereum. Lastly, theimmutable nature of blockchain also makes it easier for the PCAOB to inspect auditing processes and prevent audit firms or hackers to revise the original transaction data (See Section 2 for 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

[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 starndardized format onto the blockchain, the validation can be automated.

clients. Without blockchains, auditing firms compete for clientsthrough auditing fees and the anticipated auditing services they perform. Once a client is matched with an auditor, the client endogenously chooses the level of misstatement to tradeoff 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 volumeface greater misstatement risk and higher auditing fees.

When an auditor adopts a blockchain system, auditing costs of transactions among clients within the auditor are significantlyreduced, 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 federated blockchain disrupts auditing pricing because instead of being largely based on clients' total transaction size, it also crucially depends on the nature of transaction counterparties—the number of transactions the clients have with firms who are not in afederated blockchain, such as foreign/private firms, would drive the cost. On the client side, when both auditors adopt blockchain technology, clients report more truthfully for transactions recorded on blockchains, leading to a lower auditor risk and a lower fraction of costly auditing samples.

The auditors' technology adoption decision exhibits strategic complementarity because the cost of auditing the cross-auditor transactions goes down when both auditors adopt. When clients value strongly the benefit of misreporting even after taking being detected into consideration, they would prefer to work with auditors not using blockchain, even though the auditor using blockchain can offer a lower auditing fee. Therefore when other auditors are not adopting, an auditorwould 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 using traditional auditing. 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. As such, there could be both a full-adoption equilibrium and a no-adoption equilibrium. Moreover, we find blockchain adoption could save regulatory costs. This implies that regulators such as the PCAOB have a potential role of coordinating an industry-wide adoption, which could reduce equilibrium misstatements and costs 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, it is important and novel to highlight its manifestation and implications in auditors' adoption of blockchain technology.

In sum, our study documents how blockchains could disrupt auditing industries. First, audit pricing becomes independent of clients' total transaction size but depends on the nature and volume of transaction counterparties. Second, such technology adoption improves the efficiency of audit sampling. Auditors can focus on transactions that cannot be automatically verified. Such on- vs. off-chain-based sampling is valuable for auditor sampling decisions given the current debate on the efficiency of audit sampling (PCAOB 2015). On the client side, the technology adoption will discourage clients' incentive to misreport. Importantly, 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 if regulators do not coordinate an industry-wide adoption. Therefore, coordination is needed in the technology adoption in order to reduce equilibrium misstatements and costs associated with auditing and its regulation. In addition, regulators also 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.

As a first study of blockchain implications for financial reporting and auditing, we have abstracted away from several realistic features observed in practice. For example, the federated blockchain in our model can automate audit processes of mainly transaction-based

accounts in income statements, but some discretionary accounts, such as bad debt expenses, may not be automatically verifiable because they still require auditors' experience-based discretion and industry expertise[4]. Moreover, we also omit the oft-discussed disruption in the auditor labor market and other costs of the technology due to imperfect designs. These features, albeit interesting, are not crucial for the economic insights our model delivers. In addition, many auditing jobs still remain for off-chain transactions and high discretionary accounts. Thus, the impact of these features may be more subtle (the auditing labor market may lose demand for less skillful auditors but expand demand for more skillful auditors) and warrant separate studies. Enriching our framework and empirically testing our model predictions once data are available evidently constitute interesting future research.

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 decentralization and the industrial organization of mining pools.

Concerning blockchain applications, Harvey (2016) discusses the applications of 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 user 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,

[4]For many firms, e.g., manufacturing firms, highly discretionary accounts do not constitute a large portion in their income statements (Stubben (2011)).

Niessner, and Yermack (2018)), and discusses blockchain economics and implications for investment professionals.

We differ from most earlier studies in our focus on permissioned blockchains, which means we largely abstract away from issues related to decentralization explored in Cong and He (2018) and Cong, He, and Li (2018). More importantly, our paper is among the first to explore the implications of blockchain technology and zero-knowledge proof algorithms in auditing and accounting.

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)), and joint auditing and quality (Deng et al. (2014)). Several studies propose theoretical models to study various issues regarding 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 are the first, to the best of our knowledge, to study the implementation and impact of blockchains on auditor pricing, auditor sampling, client misstating incentive, and regulators' role. We also lay out a framework for future empirical studies testing our model predictions as the technology matures and sees wider adoption.

2. Institutional Background

In this section, we explain the basic auditing process and how a customized federated blockchain can facilitate collaborative auditing against the backdrop of privacy concerns

without a central facilitating agency. In the process, 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.[5] 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 accounts payable purchases. The intuition is that 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. Therefore, this cross-party information verification can make the auditing process more efficient and reliable when detecting fraud because 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.

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

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. 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 uploaded to the private blockchain. Records on the private blockchains are synchronized on all the nodes to ensure immutability. In the private blockchain, only permissioned nodes can manage records and the nodes usually adopt a majority consensus that is efficient and scalable, and can avoid the costly mining process associated with public blockchains. 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.

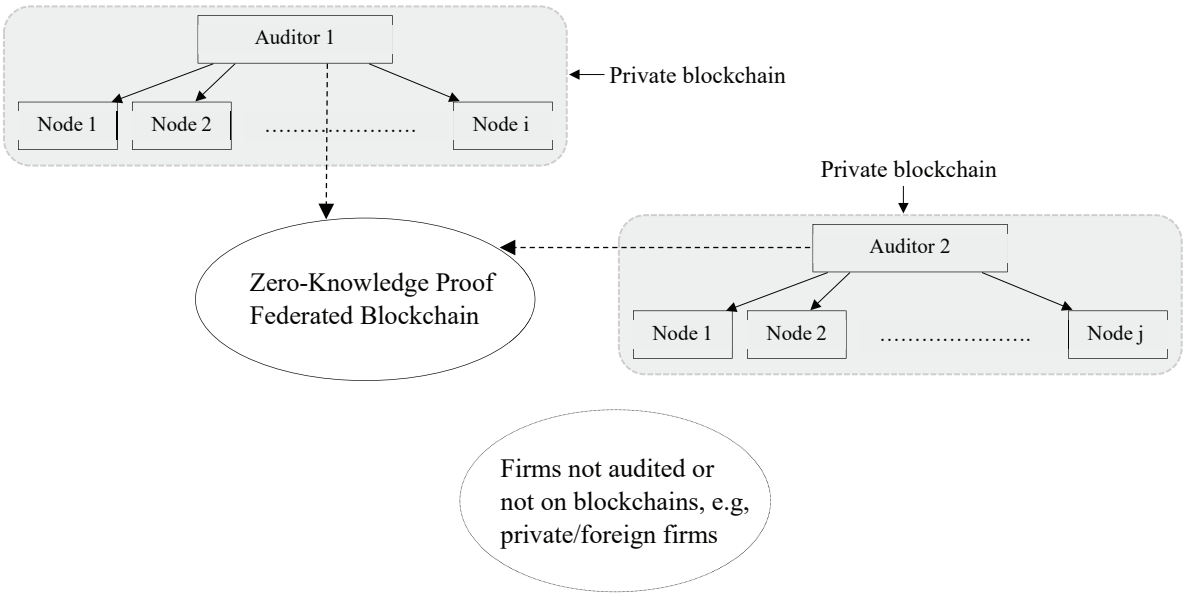

Figure 2: **Structure of the Federated Blockchain**

We illustrate the details of the transaction verification process on the federated blockchain in Figure 3. Developed in cryptography, a *zero-knowledge proof* protocol is an 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. Zero-knowledge proof protocols have seen recent applications to communications between banks (e.g., ING (2018)) and in public blockchains such as Zcash and Ethereum.[6] 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. 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

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

of a centralized party. Once the blockchain protocol is set up, this verification process can be automated so that no human intervention is needed. Therefore, this cross-party information verification can make the auditing process more efficient because an auditor does not have to contact the transaction counter-party directly to request records and manually verify the information.

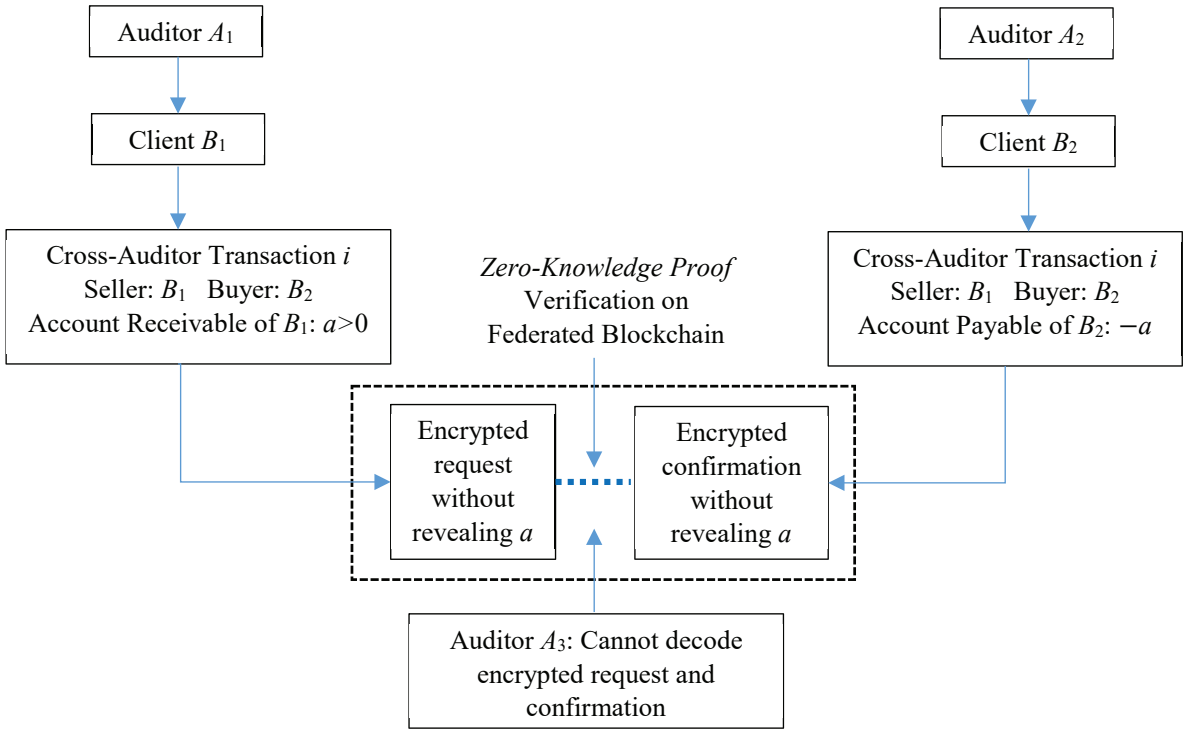

Figure 3: **Transaction Verification on a Peer-to-Peer Federated Blockchain**

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 in Case 1 is done manually; that is, audit teams manually check the information of the two parties in the transaction. However, auditor teams can 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. If a client's transaction counterparty in a transaction is not on the blockchain; for example, when it involves a private or foreign firm that is unaudited, we call such a transaction an *off-chain* transaction. 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 benefits of blockchain can contribute 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 all nodes on the federated blockchain. In Section 3, we will 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 asan 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. What is relevant for our discussion is whether an auditor has access to transaction details on the blockchain. We also want to point out that while other technologies (such as centralized databases) can also help to facilitate communication among auditors, federated blockchains

with zero-knowledge proof provide systematic and ready-to-use algorithms and infrastructure with key benefits such as privacy protection, decentralization, and immutability.

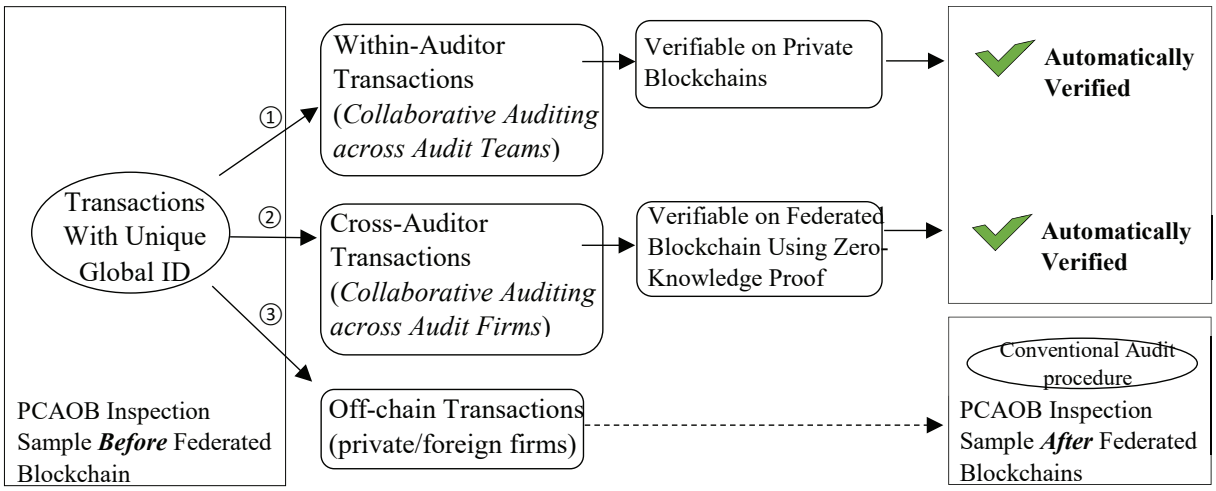

Figure 4: **Auditing Transactions with the Blockchain**

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 size K_1 and K_2. The total amount of transactions scales with the size of the economy, and is given by $(K_1 + K_2)^2$. There are two auditing firms, A_1 and A_2. Firm B_i would report K_i^2 internal transactions, and $K_i K_{-i}$ cross-firm transactions. For simplicity, we assume $K_1 = K_2$, that auditors are identical in their utility and technology, and all clients have the same utility functions.[7]

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

[7]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.

auditing quality or misstatement level). We solve the model backward and first analyze the second stage of the game whereby 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 an intrinsic/true value of $\tilde{a}_i \in (-\infty, \infty)$. For example, accounts receivable and accounts payable items correspond to the cases $\tilde{a}_i > 0$ 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

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

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.

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-auditor transaction.[8] To fix ideas, 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 found to report erroneously/commit fraud (which damages the reputation of the firm and entails regulatory penalty). We assume that the client maximizes the following second-stage utility function,

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

[8] 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.

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 found to commit 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:

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

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

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

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

(7) and (8) 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 cost parameter* a *and transaction volume* T *while the auditing intensity* s^* *is weakly decreasing in* a *and* T*. Further, the sampling size* s^*T *and the misstatement size* p^*T *are increasing in* T*.*

It is interesting that 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 a smaller sample with a larger volume to process. We are interested in the interior solution when K and thus T are very large such that

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

and 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.[9] The auditors compete for clients by posting auditing fees. Now when the auditors' market is perfectly competitive, the zero profit condi-

[9]In an earlier draft, we solved the case where there is a cost associated with switching auditors. The main intuition and qualitative results carry through.

tion 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 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 cost for each inspection and can only randomly sample due to resource constraints. Blockchain technology allows 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 blockchain. 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. When c is large, not adopting blockchain is an equilibrium.

To see this, supposing everyone is playing the equilibrium characterized in Proposition 2, the incentive for one auditor to deviate to acquire blockchain capacity is that 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 if the other client of size K stays with the other auditor who chooses not to adopt blockchain, and would be 0 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

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

Solving this, we have the optimal overstatement probability equal to

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

(11) and (12) form a system from which we can solve the equilibrium strategies (s_b^*, p_b^*) of the auditor and client. If the auditor can attract both clients, then the fee it charges in the sub-game equilibrium would be

$$b + \frac{c}{2} \leq F(s^*) \leq \lambda E\left[\int_0^{K^2} (\hat{a}_i(s^*) - \tilde{a}_i)^2 di\right] + as^{*2}K^4 + b + c.$$

We note that the first-stage objective of a firm is $\frac{\gamma^2\mu^2}{4\delta}\frac{(1-s^*)^2}{s^{*2}} - F$ is decreasing in T. Therefore, for sufficiently large γ, δ, μ relative to λ, a, b, and c, the decrease in the first term

when $T_{nb} = 0$ 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. 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 $b + c$ as an auditing fee. 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, if there are transactions with private firms that are off-blockchain, 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.

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*

$$s^*T > s_{ib}^* T_{nib} > s_b^* T_{nb}, \quad p^*T > p_{ib}^* T_{nib} > p_b^* T_{nb},$$

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 consider an extension of the model that incorporates 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

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

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.[10] The regulator's objective function is simplified to

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

Because the regulator can find a deviation of a transaction from its true value, the au-

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

ditor'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

$$L = \lambda t T E\left[\int_0^1 (\hat{a}_i - \tilde{a}_i)^2 di\right]. \tag{15}$$

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

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

This can be simplified to

$$\min_{0\le s\le 1} \lambda t(1-s) p\mu^2 + a s^2 T^2 + b. \tag{17}$$

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 are identical with 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* (14), (17), *and* (8). *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 auditing quality. Another implication of the proposition is that lower regulatory costs lead to greater auditor independence since auditors have to exert more effort, *ceteris paribus*. However, 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. Again, let T_{nb} be the number of off-chain transactions. Both the auditor and the regulator only incur costs for 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

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

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 in the case without blockchains. Auditing fees and misstatement risk also decrease.

Therefore, the adoption of blockchains can help to 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 probem 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 is lower in the full adoption equilibrium (whether we count regulator cost or not), it is a dominant policy for the regulator to coordinate adoption. The following proposition formalizes this intuition.

Proposition 6. *In both the unregulated and regulated auditing models, the regulator strictly prefers the all-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 mature. For example, PCAOB can help to set up regulatory

requirements and standards as well as coordinate the development of the underlying infrastructure of blockchains.

5. 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. The technology adoption disrupts conventional audit pricing and have implications for audit sampling. 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 the strategic complementarity in utilizing the technology to reduce equilibrium misstatements and costs associated with auditing and its regulation.

To capture the key 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 technology is not the only one 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. Consider the system of equations

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

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

Consider the two curves on the $s-p$ plane determined by the 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 of the two curves at $0 < s^* < 1$ such that $g(s^*) = \min(h(s^*),1)$. Note that in equilibrium the strict inequality in (A1) holds.

For comparative statics, we can focus on the interior solution or solution to the following equation

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

By taking derivatives of the equation and using the fact that $0 \leq s < 1$, one can then easily show $\frac{\partial s^*}{\partial a} < 0$. Equation (A2) then imply that $\frac{\partial p^*}{\partial a} > 0$. Similarly, we have $\frac{\partial s^*}{\partial a} < 0$. Multiplying both sides of ((A3)) by T, we obtain an equation in s^*T. Taking derivatives w.r.t. to T, we can then obtain $\frac{\partial(s^*T)}{\partial T} > 0$. Q.E.D.

Proof of Proposition 3. The system of equilibrium equations are

$$s = \min\left(\frac{\mu^2 p}{2aT_{nb}}, 1\right), \tag{A4}$$

$$p = \min\left(\frac{\gamma\lambda\mu(1-s)}{2\delta s^2 T_{nb}}, 1\right). \tag{A5}$$

Comparing this with the equilibrium conditions in Proposition 1, we see that when $T_{nb} = T$, it reduces to the benchmark case without blockchains. Therefore, we only need to study the comparative statics of (s, p) with respect to T_{nb}, which has been established in Proposition 1. Q.E.D.

Proof of Proposition 5. First-order conditions to the client's, auditor's, and regulator's problems are

$$p^* = \min\left(\frac{\gamma\mu(1-s^*)}{2\delta s^{*2} T}, 1\right), \tag{A6}$$

$$s^* = \min\left(\frac{\mu^2 p^* t^*}{2aT}, 1\right), \tag{A7}$$

$$t^* = \min\left(\frac{\mu^2(1-s^*)p^*}{2eT}, 1\right). \tag{A8}$$

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^*, we obtain

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

Taking derivatives on both sides and noting that $0 \leq s < 1$, we see that $\frac{\partial s^*}{\partial e} > 0$. Equations (A6) and (A8) then imply that $\frac{\partial p^*}{\partial e} < 0$ and $\frac{\partial t^*}{\partial e} > 0$. 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

$$p_b^* = \min\left(\frac{\gamma\mu(1-s_b^*)}{2\delta s_b^{*2} T_{nb}}, 1\right), \tag{A9}$$

$$s_b^* = \min\left(\frac{\mu^2 p_b^* t_b^*}{2aT_{nb}}, 1\right), \tag{A10}$$

$$t_b^* = \min\left(\frac{\mu^2(1-s_b^*)p_b^*}{2eT_{nb}}, 1\right). \tag{A11}$$

Comparing these equations to (A6), (A7), and (A8), 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 $\frac{\partial(t^*T)}{\partial T} > 0$.

References

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, July 5, 2017, "Big 4" Accounting Firms are Experimenting with Blockchain and Bitcoin, *Nasdaq.com*.

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.com, March 17, 2018, Big Four Giant PwC Announces Blockchain Auditing Service.

Cohn, Michael, December 6, 2016, Get Ready for Blockchain's Big Impact, *Accounting Today*.

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

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

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.

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.

Raj, R. Vittal, November 2, 2017, Will External Audits Vanish in the Blockchain World?, *IFAC*, available at https://www.ifac.org/global-knowledge-gateway/audit-assurance/discussion/will-external-audits-vanish-blockchain-world.

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.

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, March 15, 2018, How blockchain might affect audit and assurance, *Journal of*

Accountancy.

Vetter, Amy, May 7, 2018, Blockchain is Already Changing Accounting, *Accounting Today*.

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

Zhao, Wolfie, July 19, 2018, All "Big Four" Auditors to Trial Blockchain Platform for Financial Reporting, *Coindesk*.