Online Appendix: Distributed Ledgers and Secure Multi-Party Computation for Financial Reporting and Auditing

Sean Shun Cao, Lin William Cong, Baozhong Yang

IA.1. Model Extension: General Cost Functions

In this section, we show that our conclusions are robust to general convex forms of penalty/cost functions for the auditors and clients. We assume that the auditing cost for auditor j is given by

$$\lambda T(1-s)p\mu^2 + a_j(sT)^\alpha, \tag{IA1}$$

for $\alpha > 1$ and the client's utility given by

$$\gamma T(1-s)p\mu - \delta(psT)^\beta, \tag{IA2}$$

with $\beta > 1$.

Proposition 5. *For each auditor j and a matched client u, a unique equilibrium exists in the auditor and client's second-stage problem, with the strategies (s_j^*, p_j^*) characterized by*

$$s_j^* = \frac{1}{T}\left(\frac{\lambda p_j^* \mu^2}{\alpha a_j}\right)^{\frac{1}{\alpha-1}}, \tag{IA3}$$

$$p_j^* = \min\left(\left[\frac{\gamma\mu(1-s_j^*)T}{\delta\beta(s_j^*T)^\beta}\right]^{\frac{1}{\beta-1}}, 1\right). \tag{IA4}$$

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

Proof of Proposition 5. For simplicity of notation, we omit subscript j that indicates the

auditor in this proof. The system of FOC equations from (IA1) and (IA2) are

$$s = \min\left(\frac{1}{T}\left(\frac{\lambda p_j^* \mu^2}{\alpha a_j}\right)^{\frac{1}{\alpha-1}}, 1\right), \tag{IA5}$$

$$p = \min\left(\left[\frac{\gamma\mu(1-s_j^*)T}{\delta\beta(s_j^*T)^\beta}\right]^{\frac{1}{\beta-1}}, 1\right). \tag{IA6}$$

Consider the two curves on the $s-p$ plane determined by Equations (IA5) and (IA6). Define $g(s) = \frac{\alpha a_j (sT)^{\alpha-1}}{\lambda\mu^2}$ and $h(s) = \left[\frac{\gamma\mu(1-s_j^*)T}{\delta\beta(s_j^*T)^\beta}\right]^{\frac{1}{\beta-1}}$. The first curve is given by $p = g(s)$ when $0 \leq s \leq 1$. 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. Clearly, $h(s)$ is decreasing in s for $0 < s \leq 1$ and thus 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 (IA5) always holds since $s^* \in (0,1)$.

For comparative statics, we can focus on the interior solution. The equilibrium policy s^* satisfies the following equation derived from (IA5) and (IA6),

$$\alpha^{\beta-1}\beta a_j^{\beta-1}\delta T^{\alpha(\beta-1)}(s^*)^{\alpha(\beta-1)+1} = \gamma\lambda^{\beta-1}\mu^{2\beta-1}(1-s^*). \tag{IA7}$$

Taking derivatives of the equation and using the fact that $0 < s^* < 1$, one can then easily show that $\frac{\partial s^*}{\partial a_j} < 0$. Equation (IA6) then implies that $\frac{\partial p^*}{\partial a_j} = lh'(s^*)\frac{\partial s^*}{\partial a_j} > 0$, where l is a constant independent of a_j. For brevity of notation, when we derive comparative statics for a variable, we shall always use l to denote a quantity that is independent of the key variables in question. Therefore, l may represent different constants below in different contexts. Similarly, from (IA7), we have $\frac{\partial s^*}{\partial T} < 0$. (IA7) then implies that

$$s^*T = \left(\frac{s^{*\alpha(\beta-1)+1}T^{\alpha(\beta-1)}}{s^*}\right)^{\frac{1}{\alpha(\beta-1)}} = l\left(\frac{1-s^*}{s^*}\right)^{\frac{1}{\alpha(\beta-1)}},$$

increases with T, where l is independent of T. From (IA6) and (IA7),

$$p^* = l\left(\frac{1-s^*}{s^{*\beta}T^{\beta-1}}\right)^{\frac{1}{\beta-1}} = l'\left(\frac{1-s^*}{s^*}\right)^{\frac{\alpha-1}{\alpha(\beta-1)}},$$

which is again increasing with T, where l and l' are independent of T. p^*T thus also increases with T. Similarly, we have $\frac{\partial s^*}{\partial \gamma} > 0$ from (IA7). From (IA6) and (IA7),

$$p^* = l\gamma^{\frac{1}{\beta-1}}\left(\frac{1-s^*}{s^{*\beta}}\right)^{\frac{1}{\beta-1}} = l's^{*(\alpha-1)},$$

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

IA.2. Model Extension: Endogenous Choice of Transaction Partners

In this section, we derive some details regarding the solutions to the model extension in Section 4.1, which allows clients' endogenous choice of their transaction partners. In this setup, each client is unaware of its type at the beginning and thus makes a choice to maximize the ex-ante expected utility,

$$E[CU] = \int_0^1 CU_{u,j(u)}du = \int_0^1 (W_{j(u)} - d|u-u_j| - P_{j(u)})du,$$

where $j(u) \in \{1,2\}$ is the auditor choice of client u. Given the solution of the first-stage equilibria in Proposition 2, we have

$$CU_{u,1} = W_1 - d|u-u_1| - P_1 = \frac{2(W_1-Z_1)+W_2-Z_2}{3} - d(1+u),$$
$$CU_{u,2} = W_2 - d|u-u_2| - P_2 = \frac{(W_1-Z_1)+2(W_2-Z_2)}{3} - d(2-u).$$

Therefore, letting $t^* \in [0,1]$ be the client indifferent between auditors 1 and 2,

$$\begin{aligned} E[CU] &= \int_0^{t^*} CU_{u,1} du + \int_{t^*}^1 CU_{u,2} du \\ &= t^* \frac{2(W_1 - Z_1) + W_2 - Z_2}{3} + (1 - t^*) \frac{(W_1 - Z_1) + 2(W_2 - Z_2)}{3} - d(\frac{3}{2} - t^* - t^{*2}). \end{aligned}$$

The clients then make their optimal choice of private share of transactions m in a Bayesian perfect game sense. Given this choice, the auditors and clients play out the blockchain adoption equilibria described in Proposition 3. The optimal choice m does not have a closed-form expression, but we analyze different scenarios in Section 4.1.

IA.3. Model Extension: Discretionary Auditing and Blockchains

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

$$\min_{s, s_D \in [0,1]} \lambda E \left[\int_0^T (\hat{x}_i(s) - \tilde{x}_i)^2 di + \int_T^{T+D} (\hat{x}_i(s_D) - \tilde{x}_i)^2 di \right] + x_j (sT + k s_D D)^2 + b, \quad \text{(IA8)}$$

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 effort. Equation (IA8) can be rewritten as

$$\min_{s, s_D \in [0,1]} \lambda \mu^2 (T(1 - s)p + D(1 - s_D)p_D) + a_j (sT + k s_D D)^2 + b. \quad \text{(IA9)}$$

Similarly, the objective for the client is generalized to

$$\max_{p\in[0,1]} \gamma\mu \Pr(\hat{x}_l = x_l > \tilde{x}_l | l \in [0, T+D])(T+D) - \delta \left(\Pr(\hat{x}_l = \tilde{x}_l < x_l | l \in [0, T+D])(T+D)\right) \tag{IA10}$$

or

$$\max_{p,p_D\in[0,1]} \gamma\mu \left(T(1-s)p + D(1-s_D)p_D\right) - \delta(spT + s_D p_D D)^2. \tag{IA11}$$

We have the following result about the second-stage reporting and auditing game between the auditor and client.

Proposition 6. *Assume a client has selected an auditor j. Then there exists a unique second-stage equilibrium with equilibrium strategies $(s_j^*, s_{j,D}^*)$ for the auditor and $(p_j^*, p_{j,D}^*)$ for that client that satisfy*

$$p_j^* = \frac{p_{j,D}^*}{k}, \quad s_j^* = s_{j,D}^*.$$

Furthermore, (s_j^*, p_j^*) are the same as the second-stage equilibrium strategies for the model with only transaction-based accounts (as in Proposition 1) and transaction volume $T + kD$.

Proof of Proposition 6. We omit the subscript j for auditor j in the proof for simplicity of notation. The FOCs for s and s_D from the auditor's objective (IA9) are as follows:

$$-\lambda\mu^2 pT + 2a(sT + ks_D D)T = 0, \tag{IA12}$$

$$-\lambda\mu^2 p_D D + 2a(sT + ks_D D)kD = 0. \tag{IA13}$$

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

$$\gamma\mu T(1-s) - 2\delta(spT + s_D p_D D)sT = 0, \tag{IA14}$$

$$\gamma\mu D(1-s_D) - 2\delta(spT + s_D p_D D)s_D D = 0. \tag{IA15}$$

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 (IA12) and (IA14), 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.

The intuition of the proposition is that if $p_j^* \neq \frac{p_{j,D}^*}{k}$, say, $p_j^* > \frac{p_{j,D}^*}{k}$, then the marginal benefits of auditing transaction-based accounts is higher than that of auditing discretionary transactions. This implies that auditors would spend more effort on transaction-based auditing, and thus, it is not an equilibrium. Similarly, in equilibrium, the auditors must set $s_j^* = s_{j,D}^*$. Otherwise, the clients would have an incentive to misstate more in one of the two pools of transactions.

When auditors adopt blockchain, the volume of a client's transaction-based accounts that need to be verified by conventional methods shrinks to $T_b < T$. Discretionary accounts, meanwhile, still need to be audited in the traditional way. We have the following characterization of the equilibrium with blockchains:

Proposition 7. *In the full adoption equilibrium with discretionary account auditing and blockchains, compared with the equilibrium in the traditional world, the clients misreport less in both the discretionary and transaction-based accounts, and auditing fees decrease.*

Proof of Proposition 7. From Proposition 6, 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 $T_b + kD$. Let (s^*, s_D^*, p^*, p_D^*) be the equilibrium strategies without blockchains. By Propositions 3 and 6,

$$s_b^* > s^*, \quad p_b^* < p^*.$$

Therefore, $p_b^* T_b < p_b^* T < p^* T$ and $p_{bD}^* D = k p_b^* D < k p^* D = p_D^* D$, i.e., the client misstates less in both nondiscretionary and discretionary accounts. Given the mapping of the equilibria with discretionary auditing to the equilibria with only nondiscretionary auditing with modified total volumes ($T_b + kD$ and $T + kD$), Proposition 3 implies that the auditing fees decrease. Q.E.D.

IA.4. Model Extension: Blockchain Adoption Costs Paid by Clients

In this section, we consider a model in which the client firms share the operating costs of a blockchain, as discussed in Section 4.3. To focus on client choices, for simplicity, we consider a single auditor who sets the auditing price equal to marginal costs. The auditor provides service to a continuous measure of client firms with mass 1. Because the auditor cannot force its existing client to convert to the blockchain, it can offer incentives to clients, e.g., lower fees for clients to switch to the blockchain system. But at the same time, the auditor offers two choices to any client: 1) pay the blockchain cost, and a potentially lower auditing fee, 2) do not adopt blockchain, and pay a potentially higher auditing fee. We consider equilibria in which a mass $n \in [0, 1]$ of clients adopt blockchain. The following proposition implies that there exist multiple equilibria, but the number of possible equilibria is very limited.

Proposition 8. *If $\gamma < \lambda\mu$ and $c > 0$ is sufficiently small, then all clients adopting blockchain is an equilibrium, then there exists a unique critical mass $0 < n_0 \leq 1$, such that there exists three and only three equilibria:*

1) No-adoption equilibrium: No clients adopt blockchain.

2) "Knife's edge" equilibrium: A mass of n_0 of clients choose to adopt blockchain.

3) All-adoption equilibrium: All clients adopt blockchain.

This proposition shows that there is a coordination problem when clients need to decide whether to adopt blockchain. Essentially, there needs to be a critical mass n_0 of clients who decide to switch, in which case, the system either stays at the knife's edge equilibrium or

the full adoption equilibrium. Otherwise, the network benefits of blockchain adoption are insufficient to cover the cost of adoption, and the equilibrium is no one will adopt. This coordination problem is related to the coordination among different auditors but is more severe because there are many more clients to coordinate with.

Proof of Proposition 8.

Recall that if the number of transactions to be manually verified for a client is T, then the client's second-stage utility is given by

$$W(T) = \gamma T(1-s)p\mu - \delta(psT)^2. \tag{IA16}$$

and the auditor's second-stage auditing cost is

$$R(T) = \lambda T(1-s)p\mu^2 + as^2T^2 + b. \tag{IA17}$$

For a mass n of blockchain-adopting clients, let T_n be the off-chain transaction amount for each such client. T_n is strictly decreasing in n. Note that if a mass n of clients adopting is an equilibrium, then (based on the assumption that marginal cost equals price) the auditor offers $P(adopt) = R(T_n)$ to adopting clients, and $P(non\text{-}adopt) = R(T_0)$. An adopting client's first-stage utility is thus $W(T_n) - R(T_n) - c$ and a non-adopting client $W(T_0) - R(T_0)$. Since $\gamma < \lambda\mu$, the proof of Proposition 2 implies that $W(T) - R(T)$ is strictly decreasing in T. Therefore, if the blockchain operating cost c is sufficiently small, $W(T_1) - R(T_1) - c > W(T_0) - R(T_0)$, which implies that if all clients adopt, then no client has the incentive to deviate, i.e., all-adoption is an equilibrium. In this case, there exists a unique n_0 such that $W(T_{n_0}) - R(T_{n_0}) - c = W(T_0) - R(T_0)$, which implies that in the knife's edge case, each client is indifferent between adopting and not adopting blockchain, which is also an equilibrium. Finally, if no clients are adopting, then the deviation payoff of a single agent is $W(T_0) - R(T_0) - c < W(T_0) - R(T_0)$, and thus no-adoption is always an equilibrium (note that the clients are atomic and thus a single agent adopting does not bring benefits of blockchain). Q.E.D.

IA.5. Model Extension: Heterogenous Transaction Sizes

In this section, we consider an extension of the auditor-client monitoring-restatement model to allow heterogeneous transaction sizes, which has been discussed in Section 4.4. Given the focus of this section is to study the impact of transaction size on the misstatement and auditing strategies, we assume that there is a single auditor and one client (as in the second-stage game analyzed in Section 3.1).

The client reports a continuum of transactions $i \in [0, T_1 + T_2]$. T_1 and T_2 represent the volume of small- and large-sized transactions, respectively. Each small transaction $i \in [0, T_1)$ has a true value of $\tilde{a}_i \in (-S_1, S_1)$, and each large transaction $i \in [T_1, T_1 + T_2]$ corresponds to a true value $\tilde{a}_i \in (\infty, -S_2) \cup (S_2, \infty)$, where $S_2 > S_1 > 0$. The client but not the auditor observes the true value of transactions. For each small transaction $i \in [0, T_1)$, the client reports to the auditor the following transaction amount:

$$x_i = \tilde{x}_i + \varepsilon_i, \tag{IA18}$$

where

$$\varepsilon_i = \begin{cases} 0, & \text{with probability } 1 - p_1, \\ \mu_1, & \text{with probability } p_1, \end{cases} \tag{IA19}$$

and p_1 is the client manager's tendency to overstate a small transaction's value. For large transactions, we assume that the error equals μ_2 with a probability p_2, where $\mu_2 > \mu_1$, indicating that the client has a larger room to misstate large transactions. For tractability, we assume that $S_1 + \mu_2 < S_2$, i.e., small and large transactions do not change their label even after misstatement.

The auditor's problem is:

$$\min_{s_1, s_2 \in [0,1]} \lambda \left[T_1(1 - s_1) p_1 \mu_1^2 + T_2(1 - s_1) p_1 \mu_1^2 \right] + a(s_1 T_1 + s_2 T_2)^2 + b. \tag{IA20}$$

where s_1 and s_2 are the monitoring intensity for small and large transactions, respectively.

The client's problem can be written as

$$\max_{p_1,p_2\in[0,1]} \gamma\left[T_1(1-s_1)p_1\mu_1 + T_2(1-s_2)p_2\mu_2\right] - \delta(p_1s_1T_1 + p_2s_2T_2)^2. \tag{IA21}$$

The following proposition characterizes the equilibrium strategies $(s_1^*, s_2^*, p_1^*, p_2^*)$ of the auditor and client.

Proposition 9. *Assume that an equilibrium exists in the auditor and client's problem set up in* (IA20) *and* (IA21)*, with the equilibrium strategies* $(s_1^*, s_2^*, p_1^*, p_2^*)$*. Then*

$$s_1^* < s_2^*, \quad p_1^* > p_2^*. \tag{IA22}$$

Proof of Proposition 9.

The first order conditions for (IA20) and (IA21) are

$$-\lambda T_1 p_1 \mu_1^2 + 2a(s_1T_1 + s_2T_2)T_1 = 0, \tag{IA23}$$

$$-\lambda T_2 p_2 \mu_2^2 + 2a(s_1T_1 + s_2T_2)T_2 = 0, \tag{IA24}$$

$$\gamma T_1(1-s_1)\mu_1 - 2\delta(p_1s_1T_1 + p_2s_2T_2)s_1T_1 = 0, \tag{IA25}$$

$$\gamma T_2(1-s_2)\mu_2 - 2\delta(p_1s_1T_1 + p_2s_2T_2)s_2T_2 = 0. \tag{IA26}$$

Simplifying (IA23) and (IA24), we obtain

$$p_1\mu_1^2 = p_2\mu_2^2 \Rightarrow \frac{p_1}{p_2} = \frac{\mu_2^2}{\mu_1^2} > 1. \tag{IA27}$$

Similarly, from (IA25) and (IA26),

$$\frac{(1-s_1)\mu_1}{s_1} = \frac{(1-s_2)\mu_2}{s_2} \Rightarrow s_1 < s_2. \tag{IA28}$$

Q.E.D.