Blockchain Private Pools and Price Discovery -Online Appendix

By Agostino Capponi and Ruizhe Jia and Ye Wang *

PROOFS OF PROPOSITION 1:

We first outline the three potential equilibrium outcomes for the informed traders' pool selection, and solve for the equilibrium fee bidding strategies. We then solve for the equilibrium venue selection strategies of the informed traders. The three potential equilibrium outcomes are: (1) Both informed traders choose the private pool; (2) One informed trader chooses the private pool, and the other informed trader chooses the public pool; (3) Both informed traders choose the public pool.

Case 1: Both informed traders choose the private pool.

We show that there is no pure strategy Nash equilibrium (PNE), and that there exists a mixed strategy Nash equilibrium (MNE) where both informed traders bid $g \in [0, c]$, with g following the probability distribution

$$P(g) = \begin{cases} \frac{1-p}{p} \cdot \frac{1}{c(1-\frac{g}{c})^2} & g \leq c \cdot p \\ 0 & g > c \cdot p \end{cases}.$$

Above, c is the revenue gain of the informed trader from exploiting the trading signal, and p is the probability that each informed trader observes the trading signal.

We prove the non-existence of a PNE in two steps. First, we show that there is no symmetric PNE using a contradiction argument. Second, we show that there is no asymmetric PNE.

Assume there exists a symmetric PNE where both informed traders bid the same transaction fee $f_{D_i} = f_{D_j} = g$. We will show that there exists an unilateral deviation which allows the informed trader i to increase their expected payoff. If $g < c$, the expected payoff of informed trader i is $A_i = (1-p) \cdot (c-g) + \frac{p}{2} \cdot (c-g)$. By changing their strategy to $f'_{D_i} = g + \delta$, where $\delta > 0$ is sufficiently small, informed trader i can increase their expected payoff to $A'_i = c - (g + \delta) > A_i$. If $g \geq c$, the expected payoff of the informed trader i is 0 or negative. In this case, trader i can deviate to a bidding strategy $f'_{D_i} = 0$, which results in an expected payoff $A'_i = (1-p) \cdot c > 0$. Therefore, there exists no symmetric PNE.

We next argue that there exists no asymmetric PNE. Assume there exists a PNE where $f_{D_i} < f_{D_j}$. We argue that one of the informed traders can improve their expected payoff by unilaterally deviating. If $f_{D_i} = g > 0$, the expected payoff of informed trader i is $A_i = (1-p) \cdot (c-g)$. Therefore, informed trader i can deviate to a bidding strategy $f'_{D_i} = 0$. In such a case, $A'_i = (1-p) \cdot c > A_i$. If $f_{D_i} = 0$ and $f_{D_j} = g > 0$, the expected payoff of informed trader j is $A_j = c - g$. Therefore, informed trader j can deviate to a strategy where $f'_{D_j} = \delta$, for some δ sufficiently small. In this case, $A'_j = c - \delta > A_j$. Therefore, there exists no asymmetric PNE.

We now discuss the constructed MNE. We show that there exists no profitable deviation for all informed traders. If both informed traders play the mixed strategy $P(g)$, trader i's expected payoff is

* Capponi: Columbia University, address1, ac3827@columbia.edu. Jia: Columbia University, address2, rj2536@columbia.edu. Wang: University of Macau, Avenida da Universidade, Taipa, Macau, China, wangye@um.edu.mo.

$$
\begin{aligned}
A_i &= \alpha(1-p)\cdot\int_0^{c\cdot p} P(t)\cdot(c-t)\mathrm{d}t \\
&+ \alpha p\cdot\int_0^{c\cdot p} P(t)\cdot(\int_0^t P(s)\mathrm{d}s)\cdot(c-t)\mathrm{d}t \\
&= \alpha(1-p)\cdot\int_0^{c\cdot p}\frac{1-p}{p}\cdot\frac{1}{(1-\frac{t}{c})^2\cdot c}\cdot(c-t)\mathrm{d}t \\
&+ \alpha p\cdot\int_0^{c\cdot p}\frac{1-p}{p}\cdot\frac{1}{(1-\frac{t}{c})^2\cdot c}\cdot\frac{(1-p)\cdot t}{p\cdot(c-t)}\cdot(c-t)\mathrm{d}t \\
&= \alpha(1-p)\cdot c,
\end{aligned}
$$

where α is the adoption rate of the private pool by validators.

Then we show that both informed traders cannot improve their payoffs by switching to a different strategy. We first consider the pure strategy where $f'_{D_i} > c\cdot p$. The informed trader i will always win the game by playing this strategy. However, $A'_i = \alpha(c - f'_{D_i}) < \alpha(1-p)\cdot c$, which indicates that the informed trader i is not better off deviating.

Next, we consider a deviation to strategy $f'_{D_i} \leq c{\cdot}p$. We can write the expected payoff of informed trader i as

$$
\begin{aligned}
A'_i &= \alpha(1-p)\dot{(}c - f'_{D_i}) \\
&+ \alpha p\cdot(c - f'_{D_i})\cdot\int_0^{f'_{D_i}} P(t)\mathrm{d}t \\
&= \alpha(1-p)\cdot c.
\end{aligned}
$$

Therefore, the deviation to f'_{D_i} cannot increase the expected payoff of informed trader i.

To sum up, any combination of pure strategies will not result in a profitable deviation.

Case 2: one informed trader chooses the private pool, and the other informed trader chooses the public pool.

Since there is no competition for execution in the private pool, the informed trader will bid the 0 in the private pool when he observes an arbitrage opportunity. The informed trader in the public pool also bids 0, because he is the only informed trader in this venue.

Case 3: both informed traders choose the public pool.

Let ϵ be the minimum increment in the public auction. It is clear that the informed trader who moves first in the public pool auction will always submit an opening bid of 0. This is because if the auction lasts only for one round, the informed trader who submits the opening bid will win the auction. However, if the auction lasts for two rounds, the other informed trader who moves second will also have a chance to bid and win the auction. Therefore, the payoff of the first mover is $c - g$, and the optimal strategy is to open with a bid of 0. Similarly, the informed trader who moves second will only bid ϵ.

We then calculate the expected equilibrium payoff of each informed trader for all three cases, and construct the payoff matrix. (See Table 1)

We begin by solving for the equilibrium pool selection strategy of informed traders.

If $\alpha > \alpha_2 = \frac{1}{2-p}$, then the condition $\alpha p(1-p)c > (1-\alpha)pc$ must be satisfied, which ensures the unique equilibrium to be such that both informed traders choose the private pool.

If $\alpha \leq \alpha_1 = \frac{1}{2} - \frac{\epsilon}{4c}$, then the condition $\alpha(1-(1-p)^2)c \leq (\frac{c}{2} - \frac{\epsilon}{4})(1-(1-p)^2)$ must be satisfied. Using the tie-break rule and the aforementioned condition, the unique equilibrium is that each informed trader chooses the public pool.

If $\alpha_2 \geq \alpha > \alpha_1$, the following two conditions must be satisfied: $\alpha(1-(1-p)^2)c > (\frac{c}{2} - \frac{\epsilon}{4})(1-(1-p)^2)$ and $\alpha p(1-p)c \leq (1-\alpha)pc$. These conditions ensure that one informed trader chooses the public pool, while the other informed trader chooses the private pool.

PROOF OF COROLLARY 1:

It is easy to verify that $\alpha_1 = \frac{1}{2} - \frac{\epsilon}{4c}$ and $\alpha_2 = \frac{1}{2-p}$ both (weakly) increase in p. Moreover, $\alpha_2 = 1$ if $p = 1$.

PROOF OF PROPOSITION 2:

Let α_1, α_2 be the critical thresholds identified in Proposition 1. Let $0 < \beta_1 < \alpha_1 < \beta_2 < \alpha_2 < \beta_3 < 1$.

As shown in Proposition 1, if $\alpha < \alpha_1$, both informed traders choose the public

Table 1—: Payoff Table

A_1, A_2	Private	Public
Private	$\alpha p(1-p)c$, $\alpha p(1-p)c$	$\alpha(1-(1-p)^2)c$, $(1-\alpha)pc$
Public	$(1-\alpha)pc$, $\alpha(1-(1-p)^2)c$	$(\frac{c}{2}-\frac{\epsilon}{4})(1-(1-p)^2)$, $(\frac{c}{2}-\frac{\epsilon}{4})(1-(1-p)^2)$

pool. As a result, for $0 < \beta_1 < \alpha_1$, the expected number of informed orders in the public pool is $N(\beta_1) = N(0) = 2(1-(1-p)^2)$. This is equal to the probability that at least one informed trader receives the trading signal, multiplied by the total number of orders submitted by both informed traders, which is two. The probability of revealing information is $(1-(1-p)^2)$, because the validator that appends the next block will surely observe and execute the winning order submitted through the public pool (no execution risk).

If $\alpha_1 < \alpha < \alpha_2$, the public pool is chosen only by one informed trader. As a result, if $\alpha_1 < \beta_2 < \alpha_2$, the expected number of informed orders in the public pool is $N(\beta_2) = p$. This is equal to the probability that the informed trader using the public pool receives the trading signal. The probability of revealing information is $q(\beta_2) = p + \alpha p(1-p)$, because the order of the informed trader submitted to the public pool is always observable, but the order of the informed trader submitted to the private pool has only a probability α of being executed by the next validator.

If $\alpha > \alpha_2$, both informed traders choose the private pool. As a result, if $\beta_3 > \alpha_2$ the expected number of informed orders in the public pool is $N(\beta_3) = 0$. The probability of revealing information is $\alpha(1-(1-p)^2)$, because all informed traders' orders are submitted through the private pool, and have probability α of being observed by the validator who appends the next block.