AEA Papers and Proceedings 2023, 113: 253–256
https://doi.org/10.1257/pandp.20231030

Blockchain Private Pools and Price Discovery[†]

By Agostino Capponi, Ruizhe Jia, and Ye Wang*

Users who conduct financial transactions on a public blockchain are vulnerable to front-running attacks. Malicious actors can exploit information in pending transactions to unfairly extract profits from benevolent users (Daian et al. 2020). Front-running attacks can result in significant losses for users as well as inefficient allocation of blockspace. The transparent observability of pending transactions therefore poses a barrier to the broad adoption of blockchain-based financial services.

Private transaction pools, such as Flashbots Protect (see Flashbots 2021), have been designed to mitigate the risk of front-running attacks. Through these pools, users can send their transactions privately to validators and thus hide the transaction content from the rest of the network. However, as noted in the study by Capponi, Jia, and Wang (2021), private transaction pools may be monitored only by a fraction of validators and thus expose users to execution risk. Despite this risk exposure, it is shown in Capponi, Jia, and Wang (2021) that the presence of private transaction pools can improve the efficiency of blockspace allocation and the aggregate welfare in the ecosystem. There are two primary reasons explaining welfare improvement: first, private pools reduce the amount of blockspace inefficiently allocated to attackers' transactions, and second, they provide stronger incentives for users to submit financial transactions because front-running risk is absent.

The presence of private transaction pools on a public blockchain not only improves the efficiency of blockspace allocation and enhances welfare, but can also impact the price discovery process. In this paper, we use the model developed by Capponi, Jia, and Wang (2021) to study under which conditions and to what extent private pools hinder price discovery.

I. Model Setup

Our model consists of two informed traders. The timeline consists of three periods indexed by $t, t = 1, 2, 3$. Traders can submit transactions through two channels: the public pool and the private pool. The private pool is monitored only by a portion $\alpha < 1$ of validators, while all validators observe transactions submitted through the public pool. Transactions submitted through the private pool are only visible to the validators who have decided to monitor it. We normalize the minimal transaction fee required for transactions to be included in the block to 0.

In the first period, each informed trader has a probability p of receiving the same trading signal. If one informed trader can trade and exploit the signal before the other, they will earn a profit $c \geq 0$. After receiving the signal, each trader must decide which transaction submission channel to use: the private pool or the public pool. If an informed trader submits their transaction to the public pool, the other informed trader will learn the trading signal regardless of whether or not he received the signal directly.

In the second period, traders bid transaction fees for their orders. The transaction fee bidding mechanisms in the public and private pools are different. For traders who chose the public pool, the execution priority will be determined through the following variant of the English auction (often referred to as a priority gas auction). The public auction may last one or two rounds with equal probability, and in each round, only one informed trader is allowed to make a bid. The bid increment must be greater than a small constant ϵ. If both informed traders submit to the public pool, either of them can be the first mover with equal probability, and the other informed trader will only bid in the second round. In contrast, the execution priority in the private pool is determined by a sealed-bid first-price auction.

*Capponi: Columbia University (email: ac3827@columbia.edu); Jia: Columbia University (email: rj2536@columbia.edu); Wang: University of Macau (email: wangye@um.edu.mo).

[†] Go to https://doi.org/10.1257/pandp.20231030 to visit the article page for additional materials and author disclosure statement(s).

In the third period, a validator is chosen to append a new block of transactions to the chain. If the selected validator monitors the private pool (which happens with probability α) and sees at least one transaction in that pool, they will include the winning transaction in the new block. If there are no submitted transactions to the private pool, the validator will include the winning transaction from the public pool auction. If instead the selected validator does not monitor the private pool (which occurs with probability $1-\alpha$), then they will only include the winning transaction from the public pool auction. If there are multiple winning bids in either the private or public pool, the validator breaks the tie by randomly choosing one of the bids with equal probability.

The payoff function for informed trader j is given by

$$U_j = E\big[\mathbf{1}_{executed,j}\big(c - f_{executed,j}\big)\big],$$

where $\mathbf{1}_{executed,j}$ is the indicator function of the event "the order of informed trader j is executed" and $f_{executed,j}$ is the transaction fee paid by informed trader j. The goal is to solve for the Nash equilibrium of the game described above. The strategies of both informed traders include their pool selection and transaction fee bidding strategies.

We will assume that in the case of a tie, informed traders will choose the public pool. This assumption is justified by the fact that it usually requires more sophistication to submit transactions through private pools like Flashbots Protect.

II. Competition between Informed Traders

Informed traders must weigh the benefits and costs of using the private versus the public transaction submission channel. Submitting to the private pool guarantees privacy of the trading signal and reduces competition to exploit it, in addition to potentially providing prioritized execution. However, the private pool exposes the trader to the risk that their transaction is not observed by a fraction of validators, as observed in the study by Capponi, Jia, and Wang (2021). In equilibrium, informed traders account for these trade-offs when deciding whether to use the private or public pool. The following proposition (see the proof in the online Appendix) characterizes the pool choice of informed traders:

PROPOSITION 1 (Pool Choices): *There exist two critical thresholds* $0 < \alpha_1 < \alpha_2 \leq 1$, *such that:*

(*i*) *If* $\alpha \leq \alpha_1$, *the informed traders will submit to the public pool in equilibrium.*

(*ii*) *If* $\alpha_1 < \alpha \leq \alpha_2$, *then there exist two equilibria. In each equilibrium, one informed trader uses the public pool and the other uses only the private pool.*

(*iii*) *If* $\alpha > \alpha_2$, *then both informed traders use only the private pool in equilibrium.*

Informed traders' choice of the transaction submission channel (private or public pool) depends on the adoption rate of the private pool (α) by validators. As α increases, execution risk in the private pool decreases, which incentivizes informed traders to submit their transactions to the private pool. If the adoption rate is low, both informed traders use the public pool to avoid execution risk. If the adoption rate is high, both use the private pool to hide their trading signal and avoid competition. For intermediate values of adoption rate, there exist two equilibria, where one informed trader uses the private pool and the other uses both pools.

The following corollary (see the proof in the online Appendix) characterizes the sensitivity of informed traders' pool choices on the parameter p, keeping all other parameters fixed.

COROLLARY 1 (Sensitivity Analysis): *The thresholds* α_1 *and* α_2 *are both increasing in* p. *Moreover, if* $p = 1$, *then* $\alpha_2 = 1$*—that is, at least one informed trader does not submit through the private pool.*

As the probability p of receiving a trading signal increases, the value of hiding it decreases. This means that informed traders have reduced incentives to use the private pool to protect their information. As a result, the thresholds at which informed traders switch from the private to the public pool increase with p. If $p = 1$, the trading signal is known to both traders, and thus there is no benefit in using the private pool to protect privacy.

III. Delay in Price Discovery

In this section, we examine how the presence of private transaction pools affects price discovery. As shown in previous research (e.g., Capponi, Jia, and Yu 2022), trade flows in decentralized exchanges not only respond to public price innovations but also reveal private information, contributing to price discovery.

If informed traders submit their orders to the public pool, market participants such as market makers in centralized exchanges can learn their private information from the pending order flows and update prices in other exchanges, leading to improved price discovery. However, if informed traders only submit to the private pool, their orders will not be observed until the next block is added to the chain by a validator on the private pool. This can potentially lead to a delay in price discovery.

We propose two metrics to assess the impact of a private transaction pool on price discovery: the expected number of informed orders in the public pool (N) and the probability (q) that at least one informed trader's order is executed when a new block is generated. The expected number of informed orders in the public pool captures the amount of information revealed through *pending* orders, while the probability of execution measures the likelihood that informed traders' private information is revealed through *executed* orders. Both of these metrics are functions of the adoption rate (α) of the private pool. The following proposition (see the proof in the online Appendix) characterizes the impact of private pool adoption rate (α) on the price discovery metrics N and q.

PROPOSITION 2 (Price Discovery): *Let α_1, α_2 be the critical thresholds identified in Proposition* 1. *Let* $0 < \beta_1 < \alpha_1 < \beta_2 < \alpha_2 < \beta_3 < 1$. *The following statements hold in equilibrium:*

(*i*) $N(0) = N(\beta_1) > N(\beta_2) > N(\beta_3) = 0.$

(*ii*) $q(0) = q(\beta_1) > q(\beta_2) > q(\beta_3)$ *and* $\beta_3 q(0) = q(\beta_3)$.

In the absence of a private pool ($\alpha = 0$), informed traders submit their orders to the public pool, which in turn maximizes the amount of information revealed through pending orders (N). This allows market participants to learn information from the pending order flow and improves price discovery.

As α increases, execution risk decreases, and informed traders are more likely to submit their orders to the private pool. If $\alpha_1 < \alpha < \alpha_2$, the public pool is chosen only by one informed trader. Hence, the probability that this informed trader observes the trading signal decreases, because he is alone in the pool and cannot learn the signal from the other informed trader who switches to the private pool. As a result, the total amount of information revealed through pending orders in the public pool (N) drops from $2\left(1 - (1-p)^2\right)$ to p. If $\alpha > \alpha_2$, both informed traders submit their orders to the private pool, and thus no information is revealed in the public pool. This slows down the price discovery process, because information may only become observable from executed trades at the time the next block is proposed.

Furthermore, if $\alpha > \alpha_2$, there is a probability $1 - \alpha$ that no information is revealed through the order included in the new block, which further hinders price discovery (q decreases). This is because both informed traders submit their orders to the private pool, but the validator of the next block may not even monitor the private pool. Hence, the execution risk faced by transactions submitted through the private pool also slows down the price discovery process, because information may not be revealed within the next few blocks.

IV. Improving Price Discovery

On the one hand, the presence of private transaction pools can negatively affect price discovery, as argued in the previous section. On the other hand, existing research has demonstrated that private pools can improve allocative efficiency of blockspace (see Capponi, Jia, and Wang 2021). In this section, we consider mechanisms that minimize the negative impact of private pools on price discovery while still guaranteeing efficiency in blockspace allocation.

One way to improve price discovery is to increase the probability q that information is revealed within one block. This can be achieved by increasing the number of validators monitoring the private pool, as suggested in Proposition 2. Recall from part 2 of the proposition that if $\alpha > \alpha_2$, then

$q(\alpha) = \alpha q(0) < q(0)$. As the number of validators monitoring the private pool approaches 1, the probability that information is revealed converges to its maximum value. This is because execution risk in the private pool decreases with the number of validators, resulting in a higher likelihood that information will be revealed through the newly proposed block.

A different mechanism to improve price discovery is to minimize the impact of reduced information revealed when orders are not submitted to the public pool (smaller N). This can be achieved, for instance, by decreasing the time between the generation of two consecutive blocks. Suppose that a new block is validated every ten seconds. If the informed traders submit their orders to the public pool, their pending transactions will be quickly observable after submission. However, if both informed traders submit through the private pool, then their information will only be revealed after a new block is proposed by a validator monitoring the private pool. This will take at least ten seconds. If instead a new block were generated every five seconds, the expected delay in price discovery would be reduced. The main point is that orders are publicly observed after execution regardless of whether they are submitted through the private or the public pool.

V. Conclusion

We have designed a model to highlight the trade-off between efficiency in blockspace allocation and price discovery. While private pools raise blockspace allocative efficiency, they may harm price discovery. This is because private pools limit the amount of information revealed through pending orders in the public pool and increase the execution risk of informed orders. However, a higher number of validators on the private pool or a reduction in the time elapsing between consecutive blocks can mitigate the negative impact of private pools on price discovery.

REFERENCES

Capponi, Agostino, Ruizhe Jia, and Ye Wang. 2021. "Allocative Inefficiencies in Public Distributed Ledgers." Unpublished.

Capponi, Agostino, Ruizhe Jia, and Shihao Yu. 2022. "Price Discovery on Decentralized Exchanges." Unpublished.

Daian, Philip, Steven Goldfeder, Tyler Kell, Yunqi Li, Xueyuan Zhao, Iddo Bentov, Lorenz Breidenbach, and Ari Juels. 2020. "Flash Boys 2.0: Frontrunning in Decentralized Exchanges, Miner Extractable Value, and Consensus Instability." In *2020 IEEE Symposium on Security and Privacy*, 910–27. Piscataway, NJ: Institute of Electrical and Electronics Engineers, Inc.

Flashbots. 2021. "Flashbots Protect Overview." https://docs.flashbots.net/flashbots-protect/overview.