CERIAS

The Center for Education and Research in Information Assurance and Security

Order but Not Execute in Order

Transaction Execution Reordering in Atomic Broadcast

Tiantian Gong, Aniket Kate

1. Motivation

Problem of Front-running in blockchains

- In general blockchain systems, validators consistently order and execute transactions submitted by users.
- In blockchains like decentralizes exchanges (DEXes), validators profit from ***inserting***, ***censoring***, and ***reordering*** transactions in a proposed transaction batch, called front-running.

Existing solutions

- Extend the security definitions of traditional Byzantine fault-tolerant (BFT) state machine replication (SMR) (or atomic broadcast (ABC)) problem to include batch order fairness and have order-fair ABC protocols[1,2,3] (Traditional BFT SMR/ABC problem studies maintaining a consistent transaction log among replicas in a distributed system. But traditionally, security requires **safety** and **liveness** but does *not* concern the explicit order of transactions or whether the proposer has inserted or deleted certain transaction(s))

: General order fairness is impossible (Condorcet paradox).

- Blind transactions through encryption[4,5,6], e.g., threshold encryption and delay encryption.

: Blinding does not eliminate MEV opportunities because the contents of transactions may be inferred, and front-running can be implemented in its traditional form, e.g., act before observing the explicit future actions of a victim splitting whale orders into small volumes.

- Proposer Builder Separation (PBS) / Tax the front-runners by charging priority fees[7]

: This does not solve front-running but leaves the market to reach equilibrium through actions carried out by interdependent players in an ever-changing environment.

2. Contribution

- Combing frequent batch auction (FBA) and or-ABC as a defense against front-running for DEX.
- Compare welfare loss in or-ABC under two common market designs, FBA and Continuous limit order book (CLOB), to support FBA as a market design response.

3. FBA VS CLOB

Prioritizes **time**

- CLOB executes ordered transactions one by one
- FBA match orders in a batch according to **price**, and all matched counterparties settle trades at the same price

Prioritizes **price**

4. Welfare comparison

- Solution concepts: Markov Perfect Equilibria (MPE) for CLOB and a weaker notion, Order Book Equilibrium (OBE) for FBA (since stationary MPE may not exist).
- In equilibrium, FBA imposes less welfare loss if

(1) public information (λ_{pb}) concerning an asset's fundamental value changes is released more often compared with **private information** (λ_{pr}). Because first, under FBA, market-makers have time to respond to public information and do not need to mark up the price. Second, under CLOB, an arbitrageur can front-run the liquidity providers in case of both public and private information releases, the market-maker then demands more markups in equilibrium to counter the risk.

(2) the batch auction frequency (I) is compatible with the arrival rates of different types of trading parties.

(3) smaller priority fees for submitting transactions into the blockchain system also increase the markups under CLOB. Because front-running market-makers is more profitable, resulting in the liquidity providers charging higher markups.

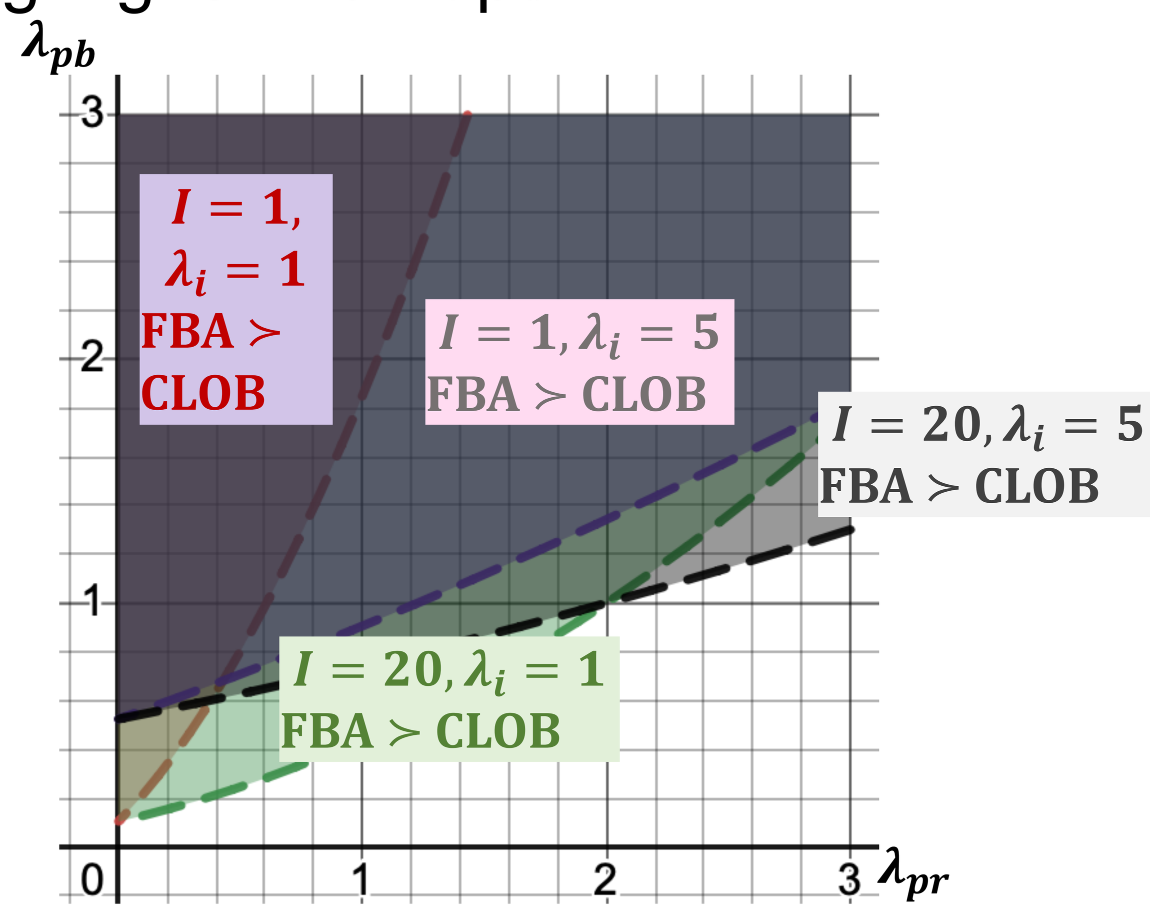

Fig 1. Example regions where FBA has less welfare loss, truncated at $\lambda_{pr} = \lambda_{pb} = 3$. An interactive graph for tuning parameters can be found here[8].

References

[1] Kelkar, M., Zhang, F., Goldfeder, S., Juels, A.: Order-fairness for byzantine consensus. In: Annual International Cryptology Conference. pp. 451–480. Springer (2020)
[2] Cachin, C., Micic, J., Steinhauer, N.: Quick order fairness. In: International Conference on Financial Cryptography and Data Security. Springer (2022)
[3] Kelkar, M., Deb, S., Long, S., Juels, A., Kannan, S.: Themis: Fast, strong order-fairness in byzantine consensus. Cryptology ePrint Archive (2021)
[4] Malkhi, D., Szalachowski, P.: Maximal Extractable Value (MEV) Protection on a DAG. arXiv e-prints pp. arXiv–2208 (2022)
[5] Momeni, P.: Fairblock: Preventing blockchain front-running with minimal overheads. Master's thesis, University of Waterloo (2022)
[6] Bebel, J., Ojha, D.: Ferveo: Threshold decryption for mempool privacy in bft networks. Cryptology ePrint Archive (2022)
[7] Daian, P., Goldfeder, S., Kell, T., Li, Y., Zhao, X., Bentov, I., Breidenbach, L., Juels, A.: Flash boys 2.0: Frontrunning in decentralized exchanges, miner extractable value, and consensus instability. In: IEEE Symposium on Security and Privacy. pp. 910–927. IEEE (2020)
[8] https://www.desmos.com/calculator/gf3fdufsan

PURDUE UNIVERSITY

CERIAS