Frontrunning

No Author Given

Concordia University

Abstract.

1 Introduction

2 Preliminaries

2.1 What is frontrunning?

Front-running is analogous to any course of action during which a person benefits from prior access to inside or confidential market information to upcoming transactions and trades. This problem can occur in both financial and non-financial systems, however, it is more noticeable within the trading and exchange systems as it was originated back in stock markets. In the old times, all the trades were executed on papers, so in case of receiving a large order from a client, the broker might say this loud and other people around the table could be informed. Therefore, a malicious trader would now run in front of that order and put his own transaction in between (before the trade was executed) and profit from the price increase of the stock. In other words, a group of market participants obtain non-public market information which allows them to front-run other users trades by putting their orders a head of those trades and benefit from advance knowledge of pending client orders. The two significant factors which cause the front-running practice to happen within the financial markets are (i) imperfect competition and (ii) liquidity uncertainty. **should I explain more?!** Any sort of front-running activity within the financial markets is considered as an unethical and illegal practice as it is unfairly beneficial for a few market participants who have the privilege of acting on this information and taking advantages at the expense of the investor.

2.2 Frontrunning in Blockchains

: One of the main discussion regarding regulations for exchanges on the topic of frontrunning, comes from the fact that information access is layered and some could be accessed only by insider actors, such as the broker, the IT administrator, *etc.*. In the blockchain world, anyone running a node of one blockchain could potentially have access to such information, hence it makes it is more susceptible for any actor to engage in frontrunning within applications running on the blockchain. Some other key differences are the fact that such actor can stay anonymous and also enforcing regulation is infeasible in traditional sense, however a decentral application could be designed in such a way to mitigate frontrunning attacks.

3 Related Work

As the traditional frontrunning was originated to trading financial instruments most of the literature are focused on financial aspects of the markets.

3.1 Historical Context / Classic Frontrunning

Frontrunning was first appeared on the Chicago Board Options Exchange (*CBoE*) [8], and was identified by *Securities Exchange Commission* in 1977 as the following:

> The practice of effecting an options transaction based upon non-public information regarding an impending block transaction[1] in the underlying stock, in order to obtain a profit when the options market adjusts to the price at which the block trades. [11]

On the years after there were ongoing discussions between self-regulatory exchanges (*e.g., CBoE*) and *SEC* to regulate, detect and define laws and regulations to deal with frontrunning [8], with *SEC* stating:

> It seems evident that such behaviour on the part of persons with knowledge of imminent transactions which will likely affect the price of the derivative security constitutes an unfair use of such knowledge. [2]

As defining what exactly is considered illegal front-running required more knowledge of how these new markets behave, *CBoE* and other exchanges (and brokers) issued educational circulars for their members asserting that frontrunning violates existing rules, with some examples of what is considered frontrunning. However difference of opinion regarding the unfairness o front running activities, insufficient exchange rules and lack of a precise definition in this area resulted in no action by self-regulator organizations citesec1978optionsmarket.

Further reading on the early details on the history and challenges of detecting and regulating frontrunning can be found in [8] .

Initially the frontrunning policies only applied to certain option markets, later on in 2002, the rule was refined to include the same prohibitions to security futures [3], which then in 2012 with the new amendment, FINRA Rule 5270, the frontrunning rule was extended to cover trading in an option, derivative, or other financial instruments overlying a security with some exceptions [4,**?**].

3.2 Recent Literature on Blockchain frontrunning

[7] [2] [**?**]

[1] Block in the stock market is large number of shares, 10 000 or more, to sell which will heavily changes the price

[2] Securities Exchange Act Release No. 14156, November 19, 1977, (Letter from George A. Fitzsimmons, Secretary, Securities and Exchange Commission to Joseph W. Sullivan, President CBoE).

4 (On) Blockchain Frontrunning

4.1 Who can frontrun?

All nodes connected to the network have the ability to front run specific transactions, however miners have special control on the blocks they happen to mine and hence more possible ways to frontrun.

Blockchain users/nodes

- **Higher GasPrice**: Monitor transactions, rebroadcast with higher GasPrice
- **Fully/well connected nodes**: Similar to HFT situation of faster connections to other nodes, for a higher chance of transaction inclusion, also Sybil attacks?
- **Noticable by the network**: More visible to the network as both transactions are broadcast to all the nodes

Miners

- **Their own mined blocks**: The can only frontrun transactions within the block they mine. This could be done by reordering the transactions within the blocks.
- **Less Noticable by the network**: Miners can include transactions within the blocks they happen to mine without broadcasting the transactions, hence less chance of being detected by the network participants.

4.2 Historical evidence

As blockchain records are immutably recorded, there is enough historical data to analyze for possible front running detection. For examples here we research some of the events of such attacks happening in the Ethereum blockchain applications.

Status ICO ICO, Initial Coin Offering, is one of the blockchain applications, specially blockchains such as Ethereum with smart contract capability. The common practice is to deploy a smart contract on the blockchain indicating the details of the ICO such as the trade ratio, when it starts and ends, and more details on how it will be capped. In June 2017, Status.im started their ICO and within 3 hours they reached the dynamic ceiling in place that triggered the end of the ICO, summing in 300,000 ether in funds, estimated at more than 200 million dollars at the time of their ICO. [10]. The idea behind Dynamic Ceilings is to make it more costly for larger contributors, in the form of transaction fees, which have to split their contributions to different addresses, with minimal impact to smaller contributors [12]. On the time of the ICO there were reports of Ethereum network being unusable and transactions were not confirming. Further study showed that some mining pools (: define mining pool) could have been manipulating the network for their own profit.

Bancor Bancor is an Ethereum-based application that allows users to exchange their tokens without any counterparty risk. This protocol aims to solve the cryptocurrency liquidity issue by introducing *Smart Tokens* [6]– ERC20 compatible tokens with a built-in liquidity mechanism that are always available to users. Smart Tokens can be bought and sold through the users smart contract at an automatically calculated price which displays supply and demand. Doing so, Bancor protocol provides continuous liquidity for digital assets without relying on an orderbook as there is no requirement to match sellers and buyers.
Front-running Bancor Recently, researchers have shown that Bancor is vulnerable to frontrunning attacks. Implemented on the Ethereum blockchain, when Bancor transactions are broadcast to the network, they sit in a pending transaction pool known as *mempool* waiting for the miners to mine them. Since Bancor handles all the trades and exchanges on the Ethereum blockchain (unlike other existing decentralized exchanges), these transactions are all visible to the public for 16s (the average Ethereum blocktime) before being included within a block. This leaves this blockchain-based decentralized exchange vulnerable to the blockchain race condition attack as attackers are given enough time to front-run other transactions and gain favourable profits [5]. Bancor frontrunning attacks can occur in two different ways:

- **Miner Frontrunning.** As mentioned, Bancor protocol uses an algorithm that automatically calculates the price of digital assets to provide better market liquidity. In the Bancor model, essentially buy orders increase the price of the tokens while sell order decrease it. Since the Blockchain miners are the only parties who can decide on the order of transactions within a block, they can easily intercept and reorder the pending transactions sitting in the mempool and profit from a guaranteed price-rise. For example, a miner learns about the pending *buy* transaction of 1000 Ether, based on the Bancor design, if this transaction goes through, it causes the price of Ether to increase. So the dishonest miner can step in front of this transaction and place his own buy order ahead of it. So he would simply create his *buy* of 1000 Ether and include it within a block and now he mines the previous *buy* transaction of 1000 Ether. Doing so, he would receive a better rate than other Bancor user, can sell the tokens he has received and gain a price advantage at the expense of others. Similarly, a dishonest miner can sell his tokens in front, if he sees a pending *sell* transaction.
- **Non-miner Frontrunning.** Researchers have also shown that a regular non-miner user can also front-run Bancor. In order for the Bancor transactions to be executed on the Ethereum Virtual Machine (EVM), users have to pay for the computations in small amount of Ether called *gas* [1]. The price that users pay for transactions (a.k.a. transaction fees) can increase or decrease how quickly they are executed and included within the blocks by the miners. This is because the Ethereum miners consume resources to process the transactions and so receive the transaction fees after creating the blocks. Once seeing two identical transactions with different transaction fees, profit maximizers miners are free to mine select the transaction which

offers the highest fee. Therefore, any regular non-miner users who run a full-node Ethereum client can modify the order of pending transactions by paying a more amount of gas *i.e.,* by monitoring the network, upon seeing a pending *buy* transaction which will further increase the price of the asset, a font-runner user can pay a higher gas price and send his transaction a head of that. By doing so, he achieves a better rate from any other Bancor users.

Domain Name Registration Although frontrunning attacks have been more showcased in the context of decentralized exchanges and trading systems, they are are not yet limited to the financial markets. Frontrunning can occur within other blockchain based applications such as naming systems. Blockchain-based namespaces have been introduced to eliminate the role of central parties *i.e.,* domain name system (DNS) which introduces single point of failures in the entire web. One such system is Ghazal, an Ethereum-based naming and PKI system [9]. Ghazal users rely on the Ethereum blockchain to register their `.ghazal` domain names and bind certificates to those names. In Ghazal model, a user would register domain name by executing the *registerdomain* function from the Ghazal smart contract with the domain name in plain text as the function argument. As mentioned before, These transactions will sit in the mempool so that it would be mined by Ethereum miners and included in the block. During this period in which the transaction is not yet confirmed, frontrunning attack can occur by (i) dishonest miners and/or (ii) regular non-miner user. In the first case, a miner would intercept the *registerdomain* transaction and register that name ahead of the user. A regular non-miner node in the Ethereum network can frontrun other user's *registerdomain* at a good profit by paying higher transaction fees. In both cases the adversarial party could sell the domain name to the users for higher price.

5 How to stop frontrunning?

Traditional Frontrunning Prevention Methods. regulations/enforcement/broker education/sealed order

Blockchain Frontrunning mitigation/prevention. The traditional methods of preventing frontrunning are based on regulation and restrictions applied to the brokers and actors within the markets, such methods do not apply to blockchains, no enforcement methods, ...

There are two main approaches to prevent front running, one to design a blockchain that is frontrun-resistent , and the other to design the application logics in a way that front running is not possible.

5.1 Frontrun-resistent Blockchain

What does this mean to have a frontrun-resistent blockchain? There are technical difficulties to achieve such solutions as there are unknown factors within such network designs (corner/edge cases).

- **Privacy Preserving Blockchians**: Shielded transactions in ZCash do not reveal the sender, receiver, the amount and the data included in the transactions, hence they cannot be seen by network participants to be frontrunned. Although this limites the functionality of the blockchain/smartcontracts/-dapps
- textbfLoopring/Dual Athoring: Talk about this possible solution

5.2 Application design to prevent frontrunning

Applications, in this case Dapps, could be designed in a way to prevent frontrunning.

- **Commit/Reveal**: describe. General solution to prevent data leaks of the transactions. although it does not hide the participatory factor (it shows the actor participated in the application but hides the details, obvious participation(commit))
- **Submarine sends**: describe. General solution similar to commit and reveal. This is to solve the participatory factor of the commit and reveal solution.
- **Application logic specific solution**: Depending on the use case of the Dapp or the application, it could be designed in a way to deincentives some actors to frontrun the transactions or prevent them from doing so. As an example on desiging a decentral orderbook, it could be said that a miner could front run orders for financial gain on price improvement, however if the fees of the orders are sent to the miner of the block, it deincentiveses the miner to front run the orders as they already gain enough financial benefit from including the correct order of transactions. Another example for decentral orderbook design could be using call market design instead of time-sensitive orderbooks. In such design the arrival time of the order does not matter as they are executed in batches.

6 Concluding Remarks

References

1. Account types, gas, and transactions ? ethereum homestead 0.1 documentation. `http://ethdocs.org/en/latest/contracts-and-transactions/account-types-gas-and-transactions.html#what-is-gas`. (Accessed on 06/14/2018).
2. R. T. Aune, A. Krellenstein, M. OHara, and O. Slama. Footprints on a blockchain: Trading and information leakage in distributed ledgers. *The Journal of Trading*, 12(3):5–13, 2017.
3. F. I. R. Authority. *IM-2110-3. Front Running Policy.* 2002.
4. F. I. R. Authority. *5270. Front Running of Block Transactions.* 2012.
5. P. D. Emin Gn Sirer. Bancor is flawed. `http://hackingdistributed.com/2017/06/19/bancor-is-flawed/`, 2017. (Accessed on 06/14/2018).
6. E. Hertzog, G. Benartzi, and G. Benartzi. Bancor protocol. 2017.
7. K. Malinova and A. Park. Market design with blockchain technology. 2017.

8. J. W. Markham. Front-running-insider trading under the commodity exchange act. *Cath. UL Rev.*, 38:69, 1988.
9. S. Moosavi and J. Clark. Ghazal: toward truly authoritative web certificates using ethereum.
10. C. Petty. A look at the status.im ico token distribution. `https://medium.com/the-bitcoin-podcast-blog/a-look-at-the-status-im-ico-token-distribution-f5bcf7f00907`, 2017. Accessed: 2018-06-10.
11. SEC. 96th cong, 1st sess, report of the special study of the options markets to the securities and exchange comission. *Comm. Print 1978*, pages 183–189, 1978.
12. S. Team. The status network, a strategy towards mass adoption of ethereum. `https://status.im/whitepaper.pdf`, 2017. Accessed: 2018-06-10.