Order-Fair Consensus

: Reducing MEV at the Consensus Layer

IC3

Follow

The Initiative for CryptoCurrencies and Contracts (IC3)

by Mahimna Kelkar

TL;DR

In current blockchain consensus protocols, a single miner or validator unilaterally controls the inclusion and ordering of transactions in a block. This form of temporary centralization is entirely at odds with the goals of decentralization. It also poses an acute problem for decentralized finance (DeFi). Arbitrageurs today are engaged in rampant collusion with miners to reorder transactions and extract profit at the expense of ordinary DeFi users. In the process of doing so, arbitrageurs are also participating in systemic bribery and even threatening the consensus stability of blockchains. So far in 2021, the impact of opportunistic transaction reordering — often called MEV or miner/maximum extractable value — has exceeded $550 million by one conservative estimate.

Our research initiates the first formal investigation into a powerful countermeasure to such transaction-order manipulation. We introduce and study transaction-order-fairness —

a new kind of consensus property that enforces strong guarantees on the final execution ordering of transactions. Order-fair consensus protocols are designed to make systems fairer for ordinary users by removing problematic forms of MEV.

What is fair ordering

and why is it important?

Before we consider fair ordering, let’s first look at how most existing protocols (both permissioned and permissionless) order transactions. In protocols like PBFT, Hotstuff, and even Nakamoto consensus, the leader (or miner) has complete control over the inclusion and order of transactions in the block that it proposes. There is no mechanism for other nodes in the network to check the transaction ordering in the proposed block. A malicious leader can outright choose the ordering that is most favorable to itself. It can also maliciously insert its own transactions or [sandwich

](/coinmonks/demystify-the-dark-forest-on-ethereum-sandwich-attacks-5a3aec9fa33e)

users to maximize its profit. Even rational leaders can be bribed to favor specific transaction orderings. We use order-manipulation

attacks to refer to the overarching class of attacks that profit from the selective censorship, inclusion, or reordering of transactions; MEV denotes the maximum profit that can be extracted from the system through these order-manipulation attacks.

To illustrate, let’s take a simple example for trading a hypothetical token T in a permissionless system. Suppose Alice wants to buy 1 token T for a maximum price of $110 and Bob wants to sell his T token for at least $100. A miner who observes both transactions can, instead of matching Bob’s and Alice’s transactions with each other, first buy Bob’s token itself and then quickly turn around and sell it to Alice for a $10 profit — -a profit taken directly out of the pockets of Alice and Bob.

During the last several decades, Wall Street has experienced a very similar kind of adversarial order-manipulation in spades. This is quite well known within the trading community and over the years multiple high-profile investigations by government agencies like the SEC have resulted in hundreds of millions of dollars in finesfor brokerages. Just recently, in December 2020, the popular mobile-app based brokerage Robinhood was charged with misleading its customers on best order execution and agreed to settle the charges for a $65 million fine.

In the past few years, order-manipulation practices have been observed on permissionless blockchains like Ethereum. In fact, Ethereum DeFi has encountered much more complex strategies, almost all of which would be heavily constrained or even outright illegal, in traditional financial markets. In the previous example for instance, a separate entity Eve could bribe the miner to finalize the transaction ordering of her choice, and extract the profit herself. This has striking similarities to payment-for-order-flow (PFOF), a controversial practice that is outright banned in Canada and the UK. While legal in the US, it is heavily restricted to ensure that user transactions are still provided the [best execution

](https://www.investopedia.com/terms/b/bestexecution.asp). While Wall Street firms need to answer to the SEC, blockchain platforms lack similar regulatory authorities. Moreover, authoritative regulation often conflicts with the key motive for blockchain decentralization which makes it necessary to provide mathematically sound solutions.

The line of work on order-fair consensus aims to prevent any malicious ordering manipulation directly at the consensus layer by designing new intrinsically

fair

protocols. Abstractly, a fair ordering protocol will guarantee that the final ledger ordering is determined by transaction arrival times in a fair

way rather than unilaterally at the will of individual miners; informally, the final transaction ordering should be influenced jointly

by a sufficiently large number of miners. For this first post, let's put aside the specific definitions of fairness and their tradeoffs and concentrate on the vision of fair ordering.

The Fair Ordering Vision

Owing to the recent rise of profit extraction through transaction order-manipulation, a number of ideas have been proposed as countermeasures. Popular financial instruments like decentralized exchanges (DeXs) can be redesigned to minimize MEV. Other techniques like hiding the transaction data before finalizing the ordering, or choosing a random ordering between transactions in the same time interval have also been experimented with; these strategies require only minor modifications and could be practical even today. While not all MEV-related problems may be solved (e.g., it's still challenging to get trustless and unbiased randomness), they're a step in the right direction of a vision for a world without unnecessary MEV.

Fair ordering protocols seek to tackle the order-manipulation problem at the core consensus layer, making them application-agnostic and therefore generically applicable. Fair ordering has distinct advantages over other techniques; it offers much stronger resistance to order-manipulation and protects against transaction spam attacks. Further, fair ordering definitions can be made general enough to include, and also integrate with other notions of MEV minimization.

Fairness itself has been a hotly debated topic in the crypto-twitterverse. A common strawman argument points out that there can't be a single notion of fairness for everyone, and therefore fairness is a lost cause — -a pipe dream

. That's like saying we can't prevent all security breaches, and so let's just not prevent any. Perfect is the enemy of good. It doesn't matter if all MEV cannot be completely removed. The hard truth is that *any*

definition of fairness proposed today provides fundamentally

better

security than existing systems where order-manipulation runs rampant. If DeFi is ever to level the playing field, it needs to learn from the mistakes of traditional finance. The choice is clear: our collective effort must be redirected to redesigning applications and protocols to minimize MEV.

This blog post will be the first in a series of posts onorder-fair consensus, likely also encompassing other techniques for MEV minimization. Subsequent posts will delve deeper into specific fair ordering protocols, and shed light on the tradeoffs for achieving different definitions of fairness. We'll draw comparisons of the order-manipulation problem to traditional finance, and explore the interactions between independent fair ordering protocols in an increasingly multi-chain and off-chain world.

We thank Sarah Allen

, IC3 Community Manager

,for her help in writing this blog post.

Image

[source

](https://commons.wikimedia.org/wiki/File:Take_a_Number,_(14495402297).jpg)