

Open in app ↗



Search

Write



# On Oracle Extractable Value



thefett

7 min read · Sep 20, 2021



3



1



Ethereum and defi are continuing to push the boundaries of what's possible with financial engineering. Since most transactions are automated, transparent, and open for anyone to perform, the system quickly arrives at an equilibrium for any exchange, with degens and arbitrageurs leading the charge to hyper-efficient financialization.

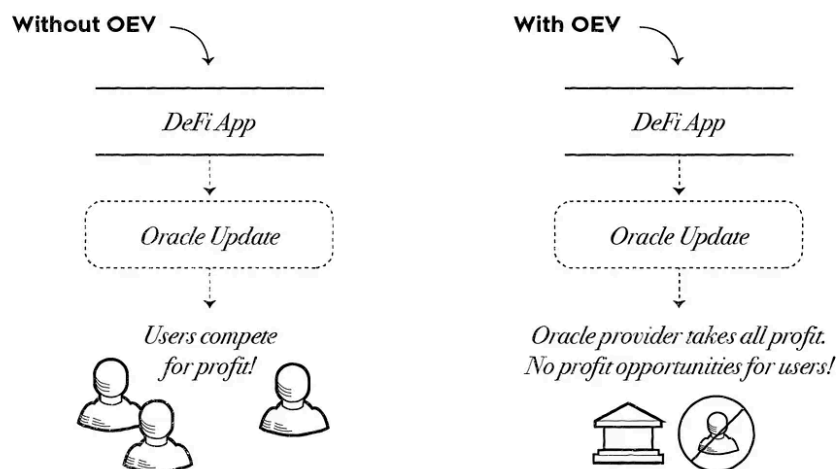
Miner Extractable Value (MEV), or the ability of miners to front-run transactions, has been discussed at length in the space and is a known problem (or feature) of the cutthroat reality that is the dark forest of decentralized finance. A similar issue however comes in the form of oracle extractable value (OEV). As with miners (a consensus chosen individual with special updating rights to the chain), oracle reporters are also parties who are tasked with updating something on-chain, the oracle specifically (e.g. price feed). This article will explain OEV, the pros, cons, and the fact that giving oracle reporters this special updating ability leads to arbitrage and eventually will be consumed by MEV (i.e. miners will be the oracles).

## What is OEV?

OEV in this article is defined as any value that is able to be extracted from the system ( set of smart contracts using (or connected to those using) the oracle) by the address that updates the oracle.

To give an example of OEV, imagine that a derivatives contract relies on a centralized oracle (one address is the oracle) and parties can be liquidated if their positions become undercollateralized, with a fee going to the party doing the liquidation. If a position is deemed undercollateralized by the oracle updates, the party who knows when and to what value the oracle will be updated to will be at an advantage. In fact it follows that all liquidations will be performed by the oracle operator. Since he knows exactly what the updated price feed will be and when it will move on-chain, he stands in a unique position to layer transactions in order to perform liquidations before other parties. The liquidation fees earned by his privileged position in the stack are the OEV.

Another, more devious, example would be rebasing tokens. Say you have a token that rebases each night to the result of an oracle feed. The oracle feed could be based on some 24hr avg price of the underlying rebasing token. The token prices itself throughout the day based upon what the expected rebase is going to be. If the oracle provider is able to add 1-2% to the rebasing price (very easy with the volatility of some of these coins), he could easily buy up underpriced coins. It leaves the oracle provider a fantastic opportunity to gain OEV before even submitting the price update to the miner. Some participants may catch on over time, but this is why a robust dispute mechanism and open oracle accessibility is crucial!

**Fig. 1**

## Is this a bad thing?

Like MEV, OEV is sort of unavoidable. If one party is in a privileged place to update the state of a contract that has financial repercussions, that party is at an advantage; and in the anonymous, unregulated world of crypto, there's little we can do about it. However, we can follow the guidelines that should be familiar to all free market economists, specifically that the system should strive for equality of opportunity if outcome is not possible. Just because something is unfair in the specific circumstance doesn't mean that it has to be unfair at the aggregate.

*OEV is dangerous and a problem solely when the oracles themselves are centralized.*

When oracles are centralized, a situation is created where oracle providers are given a payment that the projects may not be designed to handle. It creates a feeling of inequity in many defi protocols and more so ruins the idea of a neutral oracle party. If speed around oracle updates is important,

you need to be careful whether you're making your protocol to enrich a specific oracle provider.

The solution is as simple as how chains solve MEV: you sort of don't, but you democratize the process and work to ensure a distributed group of participants. By working to promote competition at the L1 level, a diverse set of miners with easy access to the same MEV software and ability to get started, networks can mitigate the negative externalities of MEV. In the same sense, creating an oracle that allows for anyone to be a provider and also developing open-source software to detect and take advantage of OEV, oracles and defi protocols can use OEV in a way that is both transparent and beneficial.

### **Is there anything positive about OEV?**

OEV can actually be viewed as a good thing! One of the big problems for oracles is actually paying for them. Gas costs on Ethereum can be staggering, often costing hundreds of dollars to simply update a price feed on-chain. By providing an alternate method for paying for updates, OEV allows the system as a whole to get more frequent updates.

Since data on a blockchain can be read by other contracts, one oracle feed can be used for many different applications (e.g. one ETH/USD feed should work for several stablecoins, derivatives, etc.). Rather than have each application need to pay for its own feed and the costs to put it on-chain, by utilizing OEV from each dapp, the feed as a whole gets updated more frequently and with a lesser (or even no) cost directly from the contract using the oracle. For each new application providing OEV on a specific feed, you get more security and faster updates. The diversity of each application's

needs can even help ensure that one party cannot pull the specific price in one direction without being noticed or punished.

## The Game Theory of OEV — why OEV will become MEV

Assume:

- Open access to becoming an oracle provider,
- A system which provides OEV

In this scenario, the party who will receive the OEV will be the party that can best win the race conditions provided on the network. So now you will have two sets of miners: those who get MEV and those who get MEV/OEV. Since competition will put those who do not accept OEV at a material disadvantage, this will eventually lead to miners doubling as oracle reporters, and conversely all oracle reporters will be miners as they will have the advantage in race conditions. Naturally, like MEV and even more broadly block rewards, competition will drive profits to a risk-adjusted zero. The ending oracle system will churn being solely operated and monitored by competing L1 validators. By pushing the OEV to the outer edges of trust, you get a system where the oracle is close to perfect given the operating conditions of a chain. The trust assumptions and centralization concerns of your oracle will be identical to the assumptions and concerns you have at the base L1 level. If you have a diverse set of validators (who compete and are vigilant checking other validators), your oracle problems are an afterthought.

Assume:

- Whitelisted list of oracle provider,

- A system which provides OEV

In this scenario, unlike in the first scenario, there are no race conditions. Having a cartel as your oracle leads to two outcomes depending on the L1. If the L1 is closed as well, the cartel will simply capture the OEV. You'll have each defi protocol disadvantaged in different ways as cartel members are always subject to bribes, coercion, and different levels of OEV extractions in which they pull value away from actual community members. Their ability to maintain profitability on the OEV (no market conditions leading to a minimized profit) mean that the underlying protocols do not even receive the benefits of OEV such as faster or cheaper updates. This is the scenario most people envision with OEV, but it's actually not even the worst.

If the L1 is open (no closed set of validators) it actually leads to an even worse problem than OEV on a centralized chain; the eventual capture of the L1 validators. As in any efficient market, L1 validation competition leads to profits driving toward zero (e.g. the hashpower of Bitcoin will increase until electricity costs for miners equal rewards). As with Bitcoin, this means that the parties that can provide validation in the most profitable fashion will win (either by reducing costs (e.g. electricity) or increasing rewards (MEV/OEV)). Since the OEV will subsidize cartel validators, if OEV gets large enough, the cartel validators can become miners/validators themselves and dominate the system. This means that a widely used but centralized oracle network can actually lead to centralization risks at the L1 level!

## How to prepare

If you're an application/protocol developer using oracles, you need to select an oracle that allows for OEV to be captured by anyone with the eventual plan that it will be rolled directly into MEV. The maximum security of an

oracle can come from a wide variety of usage and scrutiny on any given data feed. Users too should work to become good stewards of the L1 and work to develop oracle usage with the goals of decentralization in mind.

Oracles can also be leveraged through OEV to become vigilant watchers of defi contracts. In many cases, protocols expect arbitrageurs and users to take advantage of profitable conditions and things break when they don't (e.g. maker auctions). Since oracles by their nature monitor the chain for profitable opportunities on when to submit data, linking your contract to their profitability is a perfect way to help guarantee that arbitrage will be executed.

## Conclusion

Oracle extractable value is here. It is very similar in nature to the game theory being played out currently with miner-extractable value and will eventually be coupled directly with it. Ensuring equitable access in an oracle system is of vital importance if the space is going to avoid having a super class of validator/oracles that can control the state of the chain. The good news is that structures are being created and parties are beginning to heed the warnings of oracle manipulation/ front-running. Systems built on decentralized networks do not follow the same rules as traditional systems, but we're quickly figuring out what works and makes sense as the space removes the privilege and roles given to middle men.

[Ethereum](#)[Blockchain](#)[Defi](#)[Mev](#)[Oev](#)



## Written by thefett


[Edit profile](#)

183 Followers

CTO Tellor. Economics, crypto, regulation, and the revolution. [twitter.com/@themandalore9](https://twitter.com/themandalore9)

### More from thefett



 thefett

### Social Flex #2- Dangers


LST's, restaking, systemic risks, parasites, greed, and a protocol's journey to death

8 min read · Dec 20, 2023

 2 

 ...



 thefett

### blue shell strategy—a path for removing centralization from the...

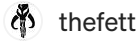
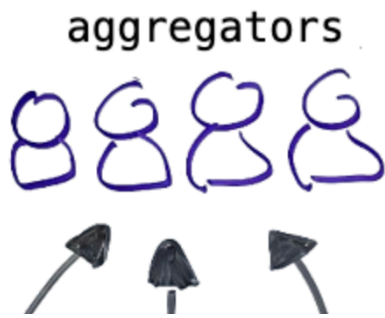
make a list of centralized people...ignore that list. the more overlap we have in our list, the...

7 min read · Apr 5, 2024

 ...





thefett

## addressing systemic risks— discouragement attacks against...

Note: this is the fourth of a series of articles on social slashing of systemic risks. The first...

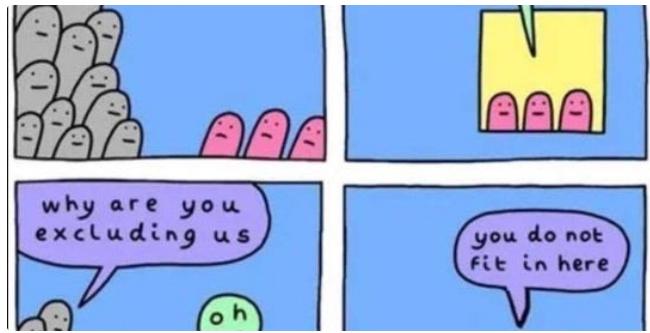
8 min read · Mar 22, 2024



2



...



thefett

## social flex #1 — values

why values matter –social flexing in crypto

9 min read · Dec 7, 2023



31



1

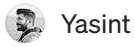


...

See all from thefett

## Recommended from Medium





Yasint

## Redstone

The integration of oracles into decentralized applications (dApps) and smart contracts is ...

3 min read · Jan 30, 2024



79



2



## MEV 101 : How to dive into MEV

10 min read · Dec 5, 2023

### Lists



#### data science and AI

40 stories · 139 saves



#### Modern Marketing

129 stories · 595 saves



#### My Kind Of Medium (All-Time Faves)

81 stories · 302 saves

omev									
search for block / tx hash / account									
contains \$-36.30 in user losses from mev and a \$3098.72.									
delay transactions were delayed by 6 secs avg and 13 secs max before being included at 2024-04-19 13:06:13.									
network p2p latency was measured at 315 ms by 3									
as order fair order									
all info toxic other									
mev	impact	action	tx hash	arrival time	from	to	value (Eth)		
Swap	+	+	0x72fb2a927d03b...	2024-04-19 13:06:03.556	0xc8f580c968e3a4...	0x7a250d5630b4cf...	2		
Swap	+	+	0x5cb3d0be4cc8c6...	2024-04-19 13:06:13.004	0x71c3f87c011401...	0x3328774a1d1c5...	0.226		
Swap	+	+	0x51b20d2c4ca570...	2024-04-19 13:06:13.004	0x842e95275c57ef...	0x3328774a1d1c5...	0.22		
Swap	+	+	0x2cfd588617c6...	2024-04-19 13:06:13.004	0x7088659e96e5dc...	0xc6fecdf760af24...	0		
Swap	+	+	0x58f254d4f0b044...	2024-04-19 13:06:13.004	0xc8d11a5953aa71...	0x51c72848c68a96...	0		
Swap	+	+	0xcbbcbdd3f35861...	2024-04-19 13:06:13.004	0x2a0ef9797bb6829...	0x73a8a6d5d9762e...	0		
Swap	+	+	0x46400d5ba8428...	2024-04-19 13:06:13.004	0x55c5003b5cd8c6...	0x80a64c6d7f12c4...	0.2		
Swap	+	+	0x2bf3319e83bd0...	2024-04-19 13:06:13.004	0xaf827c7dedf534...	0x3328774a1d1c5...	0.2		
Swap	+	+	0x5376a130eaa773...	2024-04-19 13:06:13.004	0x503e4b31a107f...	0x80a64c6d7f12c4...	1		

Atis E

## Anatomy of CEX/DEX Arbitrage

This article looks at the mechanics of CEX/DEX arbitrage trading, focusing on the...

15 min read · Apr 22, 2024

35



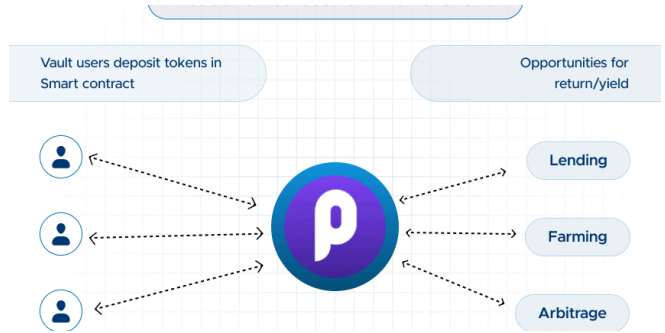
Neon EVM

## Neon EVM Quests are Live on Galxe —Join Now!

Welcome, Neonauts, to an exhilarating journey where every move you make counts,...

3 min read · 6 days ago

3



Oodles Blockchain in Coinmonks

## Exploring ERC-4626: The World of Vault Tokenization

Introduction

4 min read · Apr 17, 2024

32 1



Sergio Arrighi

## Decoding a Solana token program transaction from mempool using...

I decided to write this article as it took me ages to complete this apparently easy task! I...

4 min read · Jan 28, 2024

60

See more recommendations