TLDR

- MEV from a transaction can be split into two types.

E

V

o

r

d

e

r

i

n

g

EV_{ordering}

E

V

or

d

er

in

g

(atomic arb) which extracts value by reordering transactions and

E

V

s

i

g

n

a

l

EV_{signal}

E

V

s

i

g

na

l

(stat arb) which requires information invisible to the blockchain to extract value.

- In 2022 on Ethereum, ~$133M was extracted via

E

V

o

r

d

e

r

i

n

g

EV_{ordering}

E

V

or

d

er

in

g

(excluding sandwiching), whereas the lower bound for

E

V

s

i

g

n

a

l

EV_{signal}

E

V

s

i

g

na

l

was ~$100M.

- In the last 4 months, 16.3% (

~$20M

) of Ethereum’s security budget was paid by CeFi-DeFi trades (a type of

E

V

s

i

g

n

a

l

EV_{signal}

E

V

s

i

g

na

l

), this value is extracted from AMM LPs.

- On-chain exchanges will see

E

V

s

i

g

n

a

l

EV_{signal}

E

V

s

i

g

na

l

as a

source of value leakage

and try to either reduce it on the protocol level or make it easier (RFQs) for LPs to capture it.

Introduction

In 1971 Jack Treynor (under the pseudonym Walter Bagehot) wrote an influential paper “

The only game in town

”, suggesting the difference between informed traders and uninformed traders. LPs (Market Makers) lose value to informed traders and recover their losses from uninformed traders. Even after 50 years, the model of informed traders has stood the test of time, and is frequently used both in theory and practice.

This article extends the concept of informed traders into the MEV space (we call them informed searchers), describes 3 most common types of on-chain informed trading strategies, surveys public articles to estimate a lower bound on Extractable Value (

EV

) from these strategies and makes predictions on how it will shape the

MEV

industry.

In the next section, we define

EV

from informed searchers (

E

V

s

i

g

n

a

l

EV_{signal}

E

V

s

i

g

na

l

) and compare it to ordering-based

EV

(

E

V

o

r

d

e

r

i

n

g

EV_{ordering}

E

V

or

d

er

in

g

) common in the

MEV

ecosystem today.

Types of Extractable Value (EV)

Suppose, at a given block number

n

n

n

, the blockchain has state

S

n

S_n

S

n

and

M

M

M

transactions

T

1

m

,

…

,

T

M

m

T^m_1, \dots, T^m_M

T

1

m

,

…

,

T

M

m

in its mempool. Some users

U

^

\hat{U}

U

^

have special permissions to update the state

S
n
S_n
S
n

to
S
n
+
1
S_{n+1}
S
n
+
1

by applying a bundle of transactions
T
b
l
o
c
k
(
n
+
1
)
=
[
T
1
,
T
2
,

…

,

T

l

]

T_{block(n+1)} = [T_1, T_2, \dots, T_l]

T

b

l

oc

k

(

n

+

1

)

=

[

T

1

,

T

2

,

…

,

T

l

]

from the mempool onto the state (

S

n

S_n

S

n

) in their preferred order. These permissions can be gained by performing the most work (POW consensus), staking assets (POS consensus) or having the authority to perform updates (POA consensus).

For a new transaction

T

*

m

T^m_*

T

*

m

entering the mempool,

MEV

is defined as the

M

aximal

E

xtractable

V

alue from this transaction, by any actor (not necessarily the transaction initiator). We propose that there are two types of value that can be extracted from

T

*

m

T^m_*

T

*

m

, i.e.:

M

E

V

=

E

V

o

r

d

e

r

i

n

g

+

E

V

s

i

g

n

a

l

MEV = EV_{ordering} + EV_{signal}

ME

V

=

E

V

or

d

er

in

g

+

E

V

s

i

g

na

I

- E

V
o
r
d
e
r
i
n
g
EV_{ordering}
E
V
or
d
er
in
g

: Instantaneous value extractable from a transaction (
T
*
m
T^m_*
T
*
m

) by inserting, removing, or reordering transactions in a bundle of confirmed transactions can be called
E
V
o
r
d
e

r

i

n

g

EV_{ordering}

E

V

or

d

er

in

g

- E

V

s

i

g

n

a

l

EV_{signal}

E

V

s

i

g

na

l

: Value extractable from a transaction when combined with an external piece of information (signal) from the point of view of the blockchain will be called

E

V

s

i

g

n

a

l

EV_{signal}

E

V

s

i

g

na

l

.

E

V

o

r

d

e

r

i

n

g

EV_{ordering}

E

V

or

d

er

in

g

Instantaneous value extractable from a transaction by reordering, inserting or removing transactions in a bundle of confirmed transactions can be called

E

V

o

r

d

e

r

i

n

g

EV_{ordering}

E

V

or

d

er

in

g

(

Flash Boys 2.0

).

E

V

o

r

d

e

r

i

n

g

EV_{ordering}

E

V

or

d

er

in

g

is commonly known as atomic arbitrage. All the information available in the blockchain state (

S

n

S_n

S

n

) and mempool transactions (

T

1

m

,

…

,

T

M

m

T^m_1, \dots, T^m_M

T

1

m

,

…

,

T

M

m

,

T

*

m

T^m_*

T

*

m

) is

sufficient

to extract value by ordering. Examples of this include:

- Defi atomic arbitrage
- Sandwiching of user orders (exploiting high slippage), or
- Liquidations of unhealthy loans

Users who identify and package transactions to extract value are commonly known as searchers. A searcher can package a single transaction (

T

*

m

T^m_*

T

*

m

) with their transaction or combine multiple transactions from the mempool to extract value. In the diagram above we can see that a searcher reorders transactions and the bundle in green which has a higher

EV

gets included in the block by the validator. According to

flashbots

in 2022 on Ethereum, ~$133M (excluding sandwiching) has been extracted via

E

V

o

r

d

e

r

i

n

g

EV_{ordering}

E

V

or

d

er

in

g

. Note, $133M is the

extracted value

the theoretical upper bound of

extractable value

(EV)

via ordering is much higher.

E

V

s

i

g

n

a

l

EV_{signal}

E

V

s

i

g

na

l

EV

from a transaction when combined with an external piece of information (

signal

) will be called

E

V

s

i

g

n

a

l

EV_{signal}

E

V

s

i

g

na

l

.

E

V

s

i

g

n

a

l

EV_{signal}

E

V

s

i

g

na

l

is commonly known as statistical arbitrage. The information is not visible to the blockchain i.e. does not exist either in the blockchain state (

S

n

S_n

S

n

) or the mempool transactions. This is equivalent to the value extracted by informed traders from Market Makers in traditional finance. Examples of this include:

- CeFi-DeFi arbitrage
- Order flow trading by aggregating orders from multiple private or public mempools, or
- Copy trading aka Whale watching (buying tokens bought by influential addresses)

Users who extract value from external signals will be called

informed searchers

. In the above diagram, we can see that an informed searcher executes one side of the arbitrage on-chain but the second side of the arbitrage on Binance. Neither the price of the arbitrage nor the trade is visible to the blockchain. Currently, cross-chain MEV is a type of

E

V

s

i

g

n

a

l

EV_{signal}

E

V

s

i

g

na

l

, if a higher order system exists which can provide cross-chain information and guarantee cross-chain atomic execution then cross-chain MEV will convert into

E

V

o

r

d

e

r

i

n

g

EV_{ordering}

E

V

or

d

er

in

g

.

E

V

s

i

g

n

a

l

EV_{signal}

E

V

s

i

g

na

l

is trickier to estimate since we only know the on-chain transaction and not the signal that triggered it. In the next section, we take a closer look into common signal-based strategies and estimate the lower bound of

E

V

s

i

g

n

a

l

EV_{signal}

E

V

s

i

g

na

l

based on them.

Informed strategies and their

E

V

s

i

g

n

a

l

EV_{signal}

E

V

s

i

g

na

l

In this section, we will describe the three most common on-chain informed strategies, look at their external signals and try to estimate the lower bound of their

E

V

s

i

g

n

a

l

EV_{signal}

E

V

s

i

g

na

l

.

CeFi-DeFi arbitrage

CeFi-DeFi arbitrage is the most well known on-chain informed strategy. The external

signal

is the price of the asset on a centralized exchange. Tim Roughgarden et. al have

derived a theoretical estimate

of

E

V

s

i

g

n

a

l

EV_{signal}

E

V

s

i

g

na

l

(called

LVR

in the paper) from these trades and have shown that for Constant Product AMMs (eg. Uni V2),

E

V

s

i

g

n

a

l

EV_{signal}

E

V

s

i

g

na

l

is proportional to the square of the pools price volatility. In the formula below,

σ

\sigma

σ

is the price volatility of the AMM pool, and

P

o

o

l

V

a

l

u

e

PoolValue

P

oo

l

Va

l

u

e

is the value of tokens in the pool.

More recently

0xfbifemboy

,

thiccythot

and

0x94305

have been using markout analysis to estimate

E

V

s

i

g

n

a

l

EV_{signal}

E

V

s

i

g

na

l

on Uniswap V3. Markout analysis compares the execution price of a trade with a price in the future (markout). If the

price in the future changes

then the trade contained some information content, that is not priced into the market at execution time but is sufficient to move the price.

As shown by the image above, in the last year for the Uni V3 ETH/USDC pair, they estimate ~$20M worth of value extracted from the LPs for a 5-minute markout price on the Uni V3 pool. Note, we take the 5-minute markout since it's the most conservative estimate. For all the pairs combined

E

V

s

i

g

n

a

l

EV_{signal}

E

V

s

i

g

na

l

is estimated to be

~$100M

in the last year. Note, this strategy has significant execution risk and requires lots of capital both on-chain and off-chain.

Order flow trading

Searchers who have access to private and public mempool transactions can aggregate these transactions and predict how the price will move in the future. The

signal

here is access to private order flow and does not require the capability to execute the trade on-chain. Note, that the knowledge of the intent to transact and confidence in its eventual settlement is sufficient enough for

E

V

s

i

g

n

a

l

EV_{signal}

E

V

s

i

g

na

l

0.

In traditional finance order flow is a big source of revenue, the 12 largest US brokerages earned

[$3.8B in revenue from order flow trading in 2021] alone. Traders use order flow as a short-term strategy to accurately time their trade while Market Makers use order flow to model information content from incoming orders and readjust their prices and spreads.

Selling order flow is still a nascent market in DeFi and we don’t currently have numerical estimates on its

E

V

s

i

g

n

a

l

EV_{signal}

E

V

s

i

g

na

l

. It is a topic of increasing interest for wallets and dApps looking for monetization and is likely to be one of the major narratives of 2023. Several teams are building solutions which aim to capture parts of the market with a range of designs.

Whale watching

Whale watching or copy trading refers to tracking public addresses of successful traders and buying the same assets as these addresses. Due to the nature of the blockchain, it is easy to calculate the historical performance of an address and

know

which assets they have bought and are buying. The

signal

here is the set of whale addresses,

DeBank

and

Nansen.ai

are the most common tools to identify and track these addresses. Nansen has also productized this signal via their smart money dashboards.

Although there are no numerical estimates on the

E

V

s

i

g

n

a

l

EV_{signal}

E

V

s

i

g

na

l

from these trades, analysis by

Nansen

and

defi_mochi

show that during the bull run, there were opportunities for a 100x return if the correct whale addresses were followed.

Future predictions

In this section, we make predictions on how the

MEV

space will evolve as sophistication and opportunity for

E

V

s

i

g

n

a

l

EV_{signal}

E

V

s

i

g

na

I

trading increases.

As time progresses, more and more signals will become common knowledge (i.e. lose their alpha) and become heavily contested. In the remaining section, we will focus on CeFi-DeFi arbitrage to make future predictions, since it's the most publicly known signal.

Rise of informed searchers

One leg of the CeFi-DeFi arbitrage happens on a Centralized Exchange (CeFi) while the second leg happens on-chain (DeFi). On the CeFi side, informed searchers will fight to get lower fee tiers and faster data from exchanges. In parallel on the DeFi side, they will compete for inclusion on-chain. We predict a rise of informed searchers leading to a race to the bottom for on-chain inclusion. Informed searchers who have better connections with exchanges will be able to keep some value but most of the

EV

from these trades will end up being captured by validators.

Interestingly informed searchers are already incentivizing block builders for CeFi-DeFi trades. In the above charts, we compare the monthly payments going to the validators by CeFi-DeFi trades vs other types of transactions (

code here

). Total validator rewards are measured by combining priority fees and direct transfers to the coinbase address, whereas a transaction is classified as CeFi-DeFi if it contains a single swap and makes a direct transfer to the coinbase address in the same transaction. A caveat, this approach does not cover all the edge cases for CeFi-DeFi trades like money sent to validators via gas fees or other means but is satisfactory enough to estimate a lower bound without introducing significant false positives.

In the last 4 months, ~$20M (15.7k ETH), or 16.3% of validator payments were paid by CeFi-DeFi trades. In the month of Nov-2022 when there was high volatility the contribution of CeFi-DeFi trades to validator rewards was ~20%. This value is leaked by AMM LPs and captured by informed searchers and block validators. As CeFi-DeFi competition continues to increase, validators are poised to capture an increasing share of the value.

Future of On-Chain exchanges

Although one leg of the CeFi-DeFi arbitrage happens on AMMs, neither AMM protocols nor their LPs are able to capture this value. We predict that AMMs will see CeFi-DeFi arbitrage as a source of value leakage and develop ways to mitigate it.

Rise of MEV-aware AMMs

AMMs will treat

E

V

s

i

g

n

a

l

EV_{signal}

E

V

s

i

g

na

l

as a source of

value leakage

and design new protocols which can capture it more effectively. Much like a liquidation system can

auction liquidation rights

, an AMM can auction off arbitrage rights. In fact, a

few

designs

have already been proposed which enable capturing CeFi-DeFi

EV

on the protocol level. The core idea of these designs is that block producers auction off the right to capture

E

V

s

i

g

n

a

l

EV_{signal}

E

V

s

i

g

na

l

at the start of the block and this auction value is then captured by the protocol.

AMMs will treat

E

V

s

i

g

n

a

l

EV_{signal}

E

V

s

i

g

na

l

as a source of

value leakage

and design new protocols which can capture it more effectively. Much like a liquidation system can

auction liquidation rights

, an AMM can auction off arbitrage rights. In fact, a

few

designs

have already been proposed which enable capturing CeFi-DeFi

EV

on the protocol level. The core idea of these designs is that block producers auction off the right to capture

E

V

s

i

g

n

a

l

EV_{signal}

E

V

s

i

g

na

l

at the start of the block and this auction value is then captured by the protocol.

Rise of RFQ-based exchanges that capture signal value

RFQ-based exchanges work similarly to how a Central Limit Order Book works. Users submit orders using signed messages to an RFQ-based exchange, while professional Market Makers take these messages and execute them on-chain. In this approach Market Makers behave as both the LPs and searchers (compared to AMMs) and are in the best position to reduce value leakage (

E

V

s

i

g

n

a

l

EV_{signal}

E

V

s

i

g

na

l

) while providing better prices to end users. Live examples of this approach are HashFlow, 0x API and even OpenSea.

RFQ-based exchanges work similarly to how a Central Limit Order Book works. Users submit orders using signed messages to an RFQ-based exchange, while professional Market Makers take these messages and execute them on-chain. In this approach Market Makers behave as both the LPs and searchers (compared to AMMs) and are in the best position to reduce value leakage (

E

V

s

i

g

n

a

l

EV_{signal}

E

V

s

i

g

na

l

) while providing better prices to end users. Live examples of this approach are HashFlow, 0x API and even OpenSea.

It is difficult to say which of the two types of on-chain exchange design will dominate the market in the coming years but we can say that the AMM design space as it stands today is ripe for disruption.

In this article, we define a new type of

E

xtractable

V

alue (

E

V

s

i

g

n

a

l

EV_{signal}

E

V

s

i

g

na

l

) which requires information invisible to the blockchain to extract value. Actors who extract such value are called

informed searchers

. In 2022 on Ethereum, ~$133M was extracted via

E

V

o

r

d

e

r

i

n

g

EV_{ordering}

E

V

or

d

er

in

g

(excluding sandwiching), whereas the lower bound for

E

V

s

i

g

n

a

l

EV_{signal}

E

V

s

i

g

na

l

was ~$100M. Interestingly, 16.3% (

~$20M

) of Ethereum’s security budget was paid by AMM LPs via CeFi-DeFi trades. This is the price CeFi-DeFi traders were willing to pay to get their swaps quickly included on-chain. In the future, on-chain exchanges will see

E

V

s

i

g

n

a

l

EV_{signal}

E

V

s

i

g

na

l

as a

source of value leakage

and try to either reduce it on the protocol level or make it easy for active LPs to stop this leak.

Acknowledgments

Special thanks to

Rajiv

,

Jai

,

Alexander

and Robin for reviewing the article.

References