The Value of Information in Blockchains: Maximal Extractable Value (MEV)

Frontrunning and Backrunning in Traditional Finance

During the days when stock market trades were made on paper, client orders were physically carried between desks to be processed. A broker who sees a large client order getting carried from one desk to another could have tried to run in front of the carrier, to get his trade executed before the client order. In another scenario, the broker could also try to get his trade executed right after the large order of a client (e.g., to be the first to sell some shares after the client's order drives up the price). These practices of the broker are referred to as *frontrunning* and *backrunning* respectively. They both depend on the fact that the broker has access to **non-public knowledge**.

Frontrunning and backrunning are prohibited practices as they are considered a form of market manipulation. The actors of these practices exploit non-public information (e.g., an order from a client) by taking positions according to it. If the actor is a broker working for a hedge fund, then, he/she will be committing fraud by prioritizing his/her interest above the client's interest.

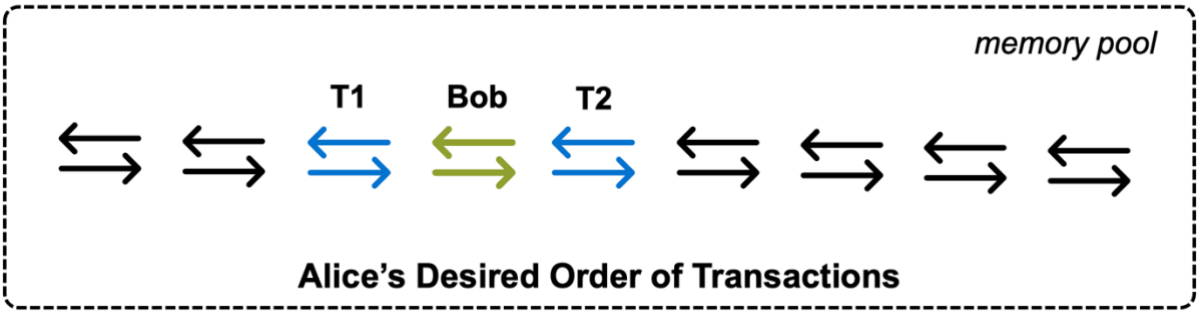
Value of Information

Value of information is a concept in decision science that deals with the utility gain of a decision-maker who acquires more knowledge before making a decision (i.e., reduces the unpredictability). Frontrunning and backrunning are techniques to capture the value of information in finance and especially in trading. Although they are considered illegal in traditional finance as they benefit from information not available to the public, this is not the case in public, permissionless blockchains.

Bitcoin and Ethereum are two of the most popular public, permissionless blockchains where the transactions are **transparent**. Every participant of the network can observe the transactions and access information about them before they are confirmed (i.e., placed in a block). Although not every transaction may provide a utility gain for observers (e.g., a transaction between two externally owned accounts (EOA)), a transaction interacting with a smart contract of a decentralized application (dApp) may yield valuable insight. Monitoring interactions with smart contracts of decentralized finance (DeFi) applications (e.g., decentralized exchanges, lending protocols, automated market makers, …) are especially valuable as they provide insight about trades that will take place (kind of like insider trading in traditional finance).

For example, let's assume Alice, a self-financed trader, is running a full node on the Ethereum blockchain and she can observe every transaction submitted to the network. One of the transactions she has seen was submitted by Bob, a crypto whale, buying a significant amount of ABC tokens. Alice knows that when Bob's transaction is confirmed and executed, it will drive up the price of ABC. Thus, she comes up with a plan to leverage the insight she has and submits two transactions to the network, respectively T1 and T2. While T1 buys a certain amount of ABC, T2 sells the same amount. Alice plans to make T1 get executed before Bob's transaction (*frontrunning*) and T2 right after it (*backrunning*).

Unlike in traditional finance, frontrunning and backrunning are not illegal practices in DeFi as transaction information is public and accessible by every member of the network. On top of that, no regulation exists to prohibit them. Thus, Alice can execute her plan by setting the correct transaction fees. Remember that, miners (or more generally block proposers) order the transactions in their unconfirmed transactions pool (i.e., memory pool) based on the fee they offer. If Alice submits T1 with a fee a little more than Bob's transaction fee, and T2 with a little less, she can possibly make the miner order the transactions in her desired way. If everything goes as planned, Alice will make a profit due to her access to information about transactions submitted to the network.



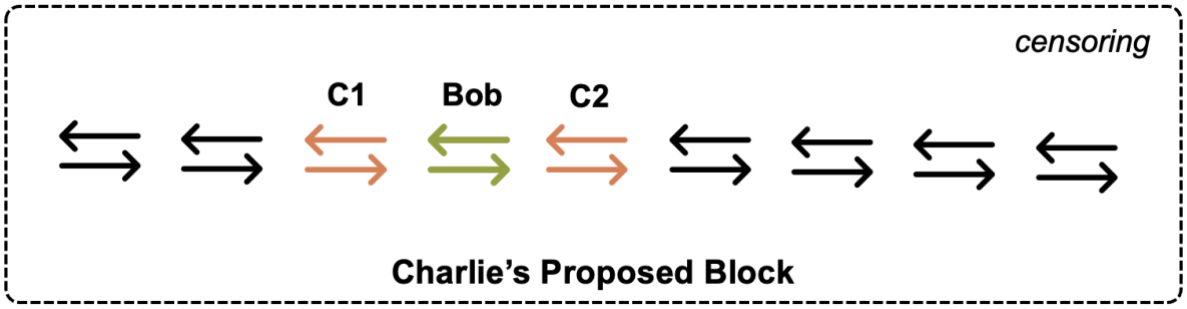
The Power of Block Proposers and Maximal Extractable Value

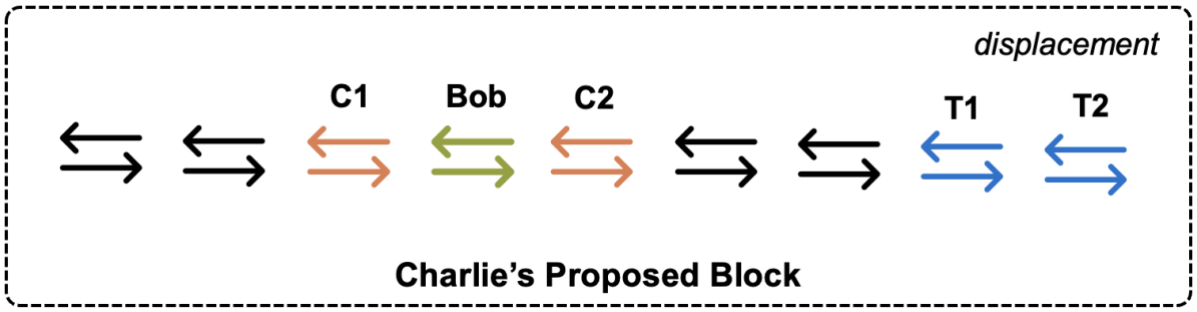
In public, permissionless blockchains, block proposers decide on the set of transactions that will be included in the next block and their respective order. Combining this with the fact that they can also observe the content of every transaction (like any other member of the network), they are considered to be in the most *powerful* position.

Let's jump back into the example where Alice tries to make a profit on Bob's transaction. The only scenario where Alice's strategy works is when T1 and T2 are placed in the correct order relative to Bob's transaction. Let's assume Charlie is a miner that solved the mining puzzle first, thus, has the right to propose the next block. He first orders the transactions in his memory pool by the fee they offer and includes the most profitable ones in his block. Since he is a *rational player,*[1] Charlie also simulates each transaction to see if there is any transaction that he can duplicate and increase his profits. He realizes that by duplicating T1 and T2 by Alice, he can leverage the opportunity created by Bob's transaction. At this point, Charlie can either:

- Leave out Alice's transactions and insert his transactions to correct positions (*Censoring*)
- Place Alice's transactions in meaningless (unprofitable) positions (*Displacement*)

[1] In game theory, rational players always aim to maximize their utility.





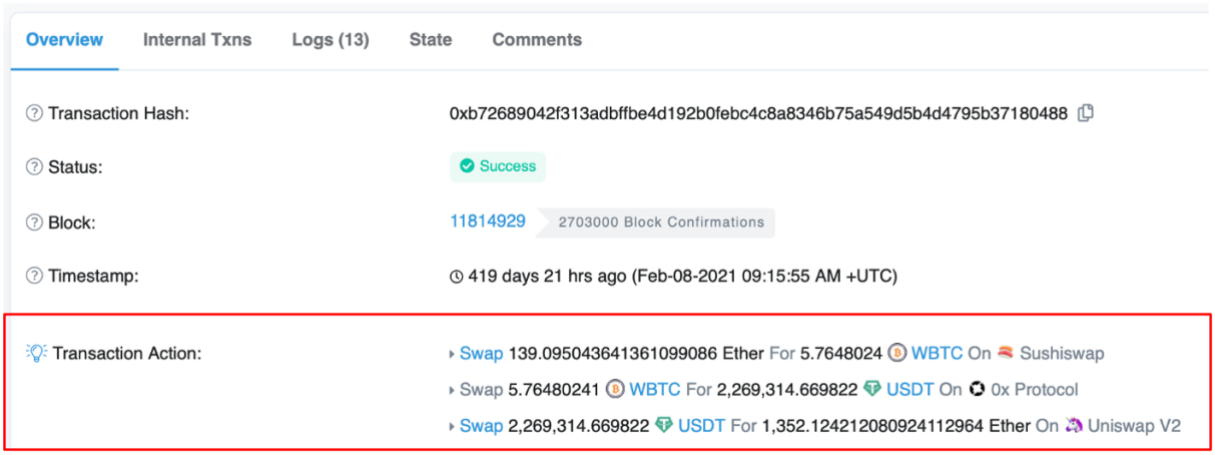
The potential profit that can be captured by Charlie in this scenario is defined as **Miner Extractable Value** (MEV). Although the term was first coined as "miner extractable value" by Phil Daian et al. in their seminal paper *Flashboys 2.0* (2019) soon it was changed to **Maximal Extractable Value**. There are two reasons for this renaming:

1. Miners are hesitant with collecting MEV since this may decrease the trust in the system. Instead, MEV is mostly collected by other network participants called *searchers*.
- *Like Alice, there are many searchers (bots) in the network that sniff the memory pool. Searchers competing for the same opportunity try to offer the most transaction fee to the miner, such that they can beat other searchers and be the first to leverage.*
2. In blockchains that don't adopt Proof-of-Work, there still exists block proposer nodes (e.g., validators, bakers) that have the right to order the transactions in a block.

On the official Ethereum website, MEV is defined as the maximum value that can be extracted from block production by including, excluding and re-ordering transactions in a block. While MEV has always been existing in public, permissionless blockchains, it has become more prominent since 2020 with the emergence of DeFi. Articles like *Ethereum is a Dark Forest* and *Escaping the Dark Forest* introduced MEV to a public audience and showed how dangerous the MEV game can be.[2] Although there exist harmful MEV strategies like Alice's,[3] which is called a *sandwich attack*, not every MEV capture is disruptive.

[2] Dangerous in the sense that there exist many highly complex bots which will try to profit from any possible opportunity exposed to the network via submitted transactions. These bots don't care about the disruptive impact on users.
[3] T1 and T2 sandwich Bob's transaction, making it buy ABC from a higher price as T1 drives the price up.

Arbitrage is one of the most common forms of MEV which contributes to enabling decentralized exchanges to offer the most accurate prices for their tokens. Arbitrage can be defined as the act of buying an asset from an exchange for a price and selling it on another exchange for a higher price in a single, atomic transaction. The following screenshot taken from Etherscan.io shows the details of an arbitrage MEV transaction. The arbitrageur initially swaps 139 Ether on Sushiswap for 5.76 wrapped Bitcoin (WBTC) and after a couple of swaps on different exchanges, ends with 1,352 Ether.



Forms of MEV

Arbitrages and sandwich attacks are two of the most popular forms of MEV. Another one is liquidations where searchers compete to be the first to liquidate a collateral in order to receive a reward. Since these MEV forms are easily detectable, there is a fierce race among the searchers for being the first to capture them. However, they are not much profitable as most of the captured MEV must be given as a transaction fee to the block proposer to outbid the other finders of the same MEV.

Besides the popular forms, searchers are also looking out for more secretive MEV opportunities. The long tail of MEV is where the real profit lies as there is much less competition. Nevertheless, finding them can be much more complex compared to detecting an arbitrage opportunity (check out this Twitter thread for an example).

Quantifying MEV

Flashbots, the primary research group working on MEV, developed a dashboard, MEV-Explore, which displays statistics about arbitrage and liquidation MEV extracted on the Ethereum blockchain. According to it, **$663M** MEV has been extracted since January 1st, 2020 with 99.12% of the MEV transactions capturing arbitrage opportunities. Although the amount detected is significant, as Flashbots also indicates, this can only be a *lower bound* for the total amount of MEV extracted on Ethereum as MEV-Explore only covers single transaction opportunities (e.g., no sandwich attacks) executed on a certain set of DeFi protocols.

Quantifying MEV on Ethereum is not a trivial task. Even if Flashbots' MEV-Explore covered every existing DeFi protocol, their quantification would still only constitute a lower bound.

The main reason for this is the long tail of MEV forms. Since MEV can be exposed in many different ways, we cannot know about every existing form. Thus, the tools we develop can only attempt to cover the forms we know about and even that cannot be done completely as we have seen in MEV-Explore. Furthermore, the long tail of MEV that the Ethereum community is aware of and extracting is still only a proportion of the actual *extractable value*.

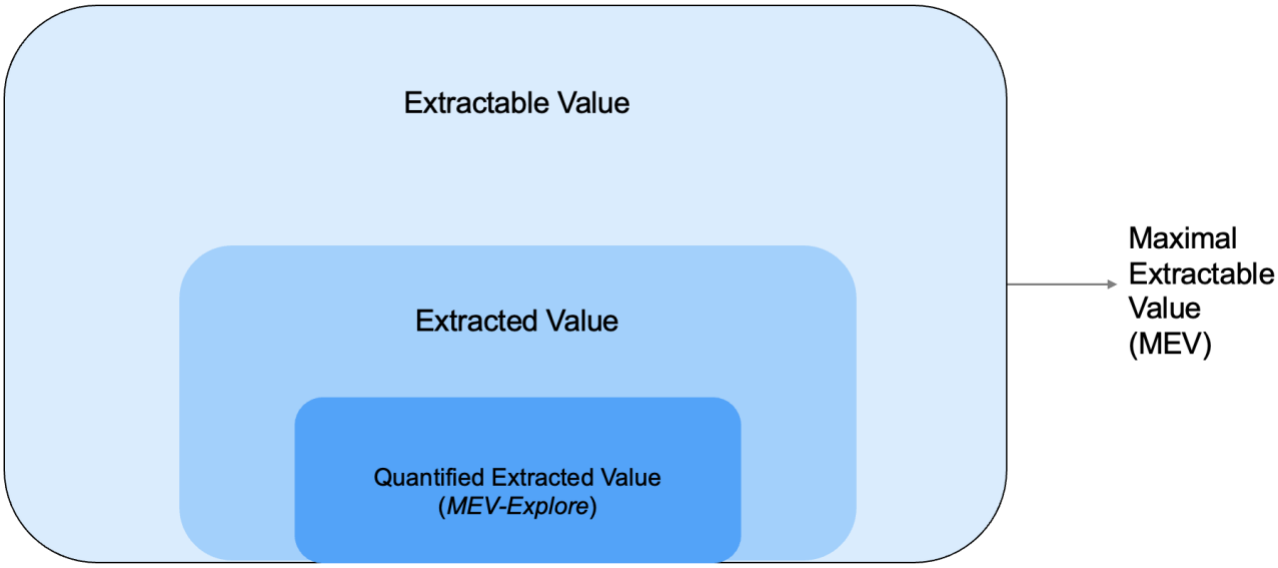


Figure inspired from Alex Obadia (Flashbots).

MEV in Bitcoin

Theoretically, Bitcoin also has MEV (e.g., ordering transactions from Lightning channels). However, compared to Ethereum or other Ethereum-based chains, the amount of MEV exposed is significantly less due to the difference in the complexity of the application-layer behavior. As Bitcoin is much more conservative in its approach to DeFi and applications running on it, the MEV exposure is by default less prominent. This may change in the future with the growing DeFi ecosystem built on Bitcoin.

Final Words

Since its realization, MEV has changed the game in Ethereum and other Ethereum-based chains. It has affected almost every component of the network, from the full node implementations (check out MEV-Geth) to block proposer incentives (according to the official Ethereum website, MEV may become more significant than the block reward for block proposers in the near future). MEV-resistant applications are being developed to offer a better user experience (see CowSwap). The Ethereum Foundation is now working together with Flashbots to democratize the MEV scene in ETH 2.0 (see mev-boost). As participants of the blockchain community, we should be aware of MEV as it will continue to exist and potentially grow with the expanding ecosystem.