Hathor's MEV protection
Don't be the greater fool

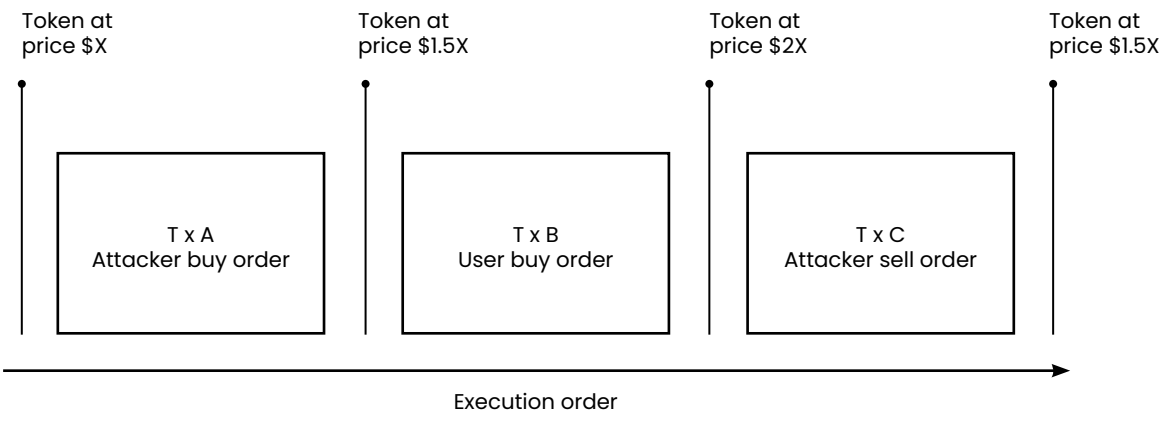
Hathor's Nano Contracts introduce groundbreaking technology to prevent MEV at the protocol level. Maximal Extractable Value (MEV) refers to the maximum amount of value that can be extracted from a given DeFi protocol or smart contract by a user or group of users.

To date, MEV has been responsible for more than $1.3 billion in lost value for Ethereum users alone. This number further increases if other networks are aggregated. To the average user, this translates into higher costs and lower profits. With Hathor's MEV protection, users can enjoy the network and its products without worrying about being exploited.

How MEV attacks works

Since each block can only contain a limited number of transactions, block producers have full autonomy in selecting which pending transactions they will include in their block. While block producers by default order transactions by the highest gas price (transaction fee) in order to maximize their profits, this is not a requirement by the network. As a result, block producers can extract additional value by taking advantage of their ability to arbitrarily reorder transactions.

For example, if a large trade is spotted, a front-running bot can copy the user's trade and create a transaction bundle where their transaction is processed first (Tx A) before the user's trade (Tx B). This moves the market price of the asset being traded, causing the user's trade to incur a larger amount of slippage - the difference between the expected price of a trade and the actual price. After the user's trade is processed (Tx B), the market price of the asset being traded further shifts in the frontrunner's favor, which allows them to take profits by selling their assets via a backrun trade (Tx C), resulting in what is commonly known as a "sandwich attack."



As a result, the user's trade is executed at a suboptimal exchange rate, increasing the costs of using decentralized exchanges in the form of an "invisible fee" where fewer tokens than initially expected are received. In the image above, the user would initially purchase tokens at price $X, but ends up purchasing at price $1.5X (numbers are just an example).

If you want to learn more about MEV, this is a good video.

Hathor's MEV protection

With Nano Contracts, Hathor is introducing an innovative solution to the MEV problem. Transaction execution order will not be determined by the block producers, but will happen in pseudo-random order. Therefore, no player can order transactions in a way that benefits them.

As a blockchain requires that all full nodes agree on the final state of the chain, transaction execution order cannot be entirely random as each node would reach a different state. All Hathor full nodes will shuffle transactions to determine the execution order using a common random number generator seed based on the latest block hash. That way, they can all arrive at the same shuffle order. If you want to learn more details about the solution, you can read the RFC.

In the sandwich attack example, an attacker cannot choose the order of execution of the transactions. So he may submit the frontrun and backrun transactions, but has no guarantee they will be executed in the required order. The user's buy order (Tx B) may be executed first, while Tx A and Tx C are executed later. This means the attacker is not able to exploit the user's buy order and will end up without profits while having to pay transaction fees.

Develop on Hathor Network

MEV protection is just one of Hathor's many innovations. If you're looking to push the boundaries of DeFi application development, consider building your next project on Hathor. Our public Nano Contracts testnet is open and ready for you to explore today!

Start developing Nano Contracts now!