What is a Sandwich Attack?

Sandwich attacks occur when a user's transaction gets trapped, or "sandwiched," between two hostile transactions - one before and one after. As a result, the original transaction executes at a much higher price than necessary, leading to an inflated price for the original trader and a profit for the malicious trader placing the two extra trades (known as a "searcher").

How a sandwich attack works

When a searcher spots an opportunity to sandwich a transaction, they place a trade before (known as "frontrunning") and a trade after (known as "backrunning") the transaction in order to manipulate the price of the trade.

Due to the design of Automated Market Makers (AMM) such as Uniswap, these trades strategically manipulate the price of the assets, leaving room for profit. To really understand how sandwich attacks work, though, we first need to understand some core concepts.

Core concepts at play

- Automated Market Makers (AMM):
- Automated Market Makers are trading mechanisms that allow traders to buy and sell assets in real time. Unlike traditional "orderbook" trading, which relies on counterparties for every transaction (you need a seller in order to buy and a buyer in order to sell), AMMs work by maintaining a constant ratio between the prices of two assets. For example, ETH and COW. AMMs use the formula "x*y = k" to determine a fair price based on the ratio between two assets (x and y) in the liquidity pool. Any time a trade alters this ratio by depleting the supply of one asset and increasing the other, the prices of the assets adjust in order to preserve the established ratio. For instance, if a trader buys COW and sells ETH, the COW price rises, and the ETH price falls. The opposite happens when traders sell COW and buy ETH.
- Slippage Tolerance:
- When placing a trade, traders set a "slippage tolerance" for their transactions, which represents the maximum price difference they're willing to accept for their trade. For example, if ETH is trading at 2,000 and you place an order to buy ETH with a 5% slippage tolerance, you're willing to buy ETH at up to 2,100. If ETH goes above 2,100, however, your trade will fail, as it's outside your slippage tolerance. Some slippage tolerance is always necessary because the prices of crypto assets are constantly fluctuating, so by the time your trade executes, the price may have moved. Setting your slippage tolerance too high, however, leaves room for searchers to sandwich your trades.
- Price Impact:
- Crypto markets, like all markets, are based on supply and demand. AMMs maintain "liquidity pools" of assets that they use to fill trades. Each trade drains some amount of this liquidity, moving the price of the asset. This price movement is known as "price impact." The larger the trade, the bigger the price impact. A trade of 100 ETH will not move the price of ETH very noticeably, since it makes up a tiny fraction of the available liquidity. A trade of 1,000,000 ETH however, will noticeably move the price of ETH.
- Transaction Reordering:
- Blockchain transactions do not always enter the block in the order that they were submitted. Searchers can "bribe" the validator responsible for creating the block to have them arrange transactions in a specific sequence. This transaction reordering is what makes all of MEV, including sandwich attacks, possible.

The sandwich attack: Step by step

Let's examine a sandwich attack through a step-by-step example. In this example, we're trading ETH and COW.

1. Bessie wants to buy COW using her ETH. She goes to a decentralized exchange (DEX) like Uniswap, and places an order for 4,000 COW. This should cost her around 1 ETH, but due to significant market volatility, Bessie decides to set a 10% slippage tolerance. This means she's willing to pay up to 1.1 ETH for 4,000 COW.
2. Bessie's trade enters the Ethereum mempool (the pending order queue), and a lurking searcher spots an opportunity. Springing into action, the searcher places a trade just before Bessie's large enough to push the COW price up to her slippage tolerance. In this case, the searcher buys 4,000 COW for exactly 1 ETH. As a result of this first trade's price impact, Bessie's 4,000 COW purchase now costs 1.1 ETH - the maximum she's willing to pay.
3. Once the searcher's transaction clears, Bessie's transaction also goes through and she receives her 4,000 COW in exchange for 1.1 ETH. The searcher takes advantage of this price impact and sells their original COW at this new rate - 4,000 COW for 1.1 ETH. In the end, the searcher buys 4,000 COW for 1 ETH and sells it for 1.1 ETH, earning a profit of 0.1 ETH (before gas and fees) for not much effort.

It's easy to see how lucrative sandwich attacks are!

Bessie, on the other hand, ends up with a bad deal. She could have purchased 4,000 COW for just 1 ETH, but her slippage tolerance left room for a sandwich attack that forced her to pay an extra 10% for her trade. Edit this page Previous What is Frontrunning? Next What is Backrunning?