Just in Time Liquidity and Sandwich Attacks

The inception of Bitcoin marked the creation of the first fully decentralized cryptocurrency relying on blockchain technology. Almost a decade later, Ethereum introduced the concept of smart contracts, which allowed for most parts of the financial system to be rebuilt in a decentralized manner using the blockchain. Decentralized Finance (DeFi) is the umbrella term for these financial applications running on the blockchain (mainly Ethereum), and their usage has been growing dramatically.

Decentralized exchanges (DEXes) are notable DeFi applications. They allow for transactions to take place on the blockchain without an intermediary. Most decentralized exchanges replace traditional order books with an automated market maker mechanism, whereby the liquidity of two cryptocurrencies is aggregated in what is referred to as a liquidity pool. This liquidity pool then facilitates trading between the pool’s two cryptocurrencies. The exchange ratio is controlled by an algorithm and generally depends on the amount of reserved liquidity, as well as the ratio of the reserves.

Both just in time liquidity\(^1\) and sandwich attacks\(^2\) are very common on DEXes. In this thesis we want to empirically analyze the prevalence and impact of both on DEXes.

Requirements: Ability to work independently and interest in conducting new research. An interest and experience with decentralized finance is a plus. This is a practical project, Python experience is required. We will have weekly meetings to discuss open questions and determine the next steps.

Interested? Please contact us for more details!

Contact
- Lioba Heimbach hlioba@ethz.ch, ETZ G95

---

\(^1\)https://blog.uniswap.org/jit-liquidity
\(^2\)https://medium.com/coinmonks/defi-sandwich-attack-explain-776f6f43b2fd