Paper 2023/1868

COMMON: Order Book with Privacy

Albert Garreta, Nethermind Research
Adam Gągol, Aleph Zero Foundation,Cardinal Cryptography
Aikaterini-Panagiota Stouka, Nethermind Research
Damian Straszak, Aleph Zero Foundation,Cardinal Cryptography
Michal Zajac, Nethermind Research

Abstract

Decentralized Finance (DeFi) has witnessed remarkable growth and innovation, with Decentralized Exchanges (DEXes) playing a pivotal role in shaping this ecosystem. As numerous DEX designs emerge, challenges such as

Archived copy · cryp2nova.com

price inefficiency and lack of user privacy continue to prevail. This paper introduces a novel DEX design, termed COMMON, that addresses these two predominant challenges. COMMON operates as an order book, natively integrated with a shielded token pool, thus providing anonymity to its users.
Through the integration of zk-SNARKs, order batching, and Multiparty Computation (MPC) COMMON allows to conceal also the values in orders.
This feature, paired with users never leaving the shielded pool when utilizing COMMON, provides a high level of privacy.
To enhance price efficiency, we introduce a two-stage order matching process: initially, orders are internally matched, followed by an open, permissionless Dutch Auction to present the assets to Market Makers. This design effectively enables aggregating multiple sources of liquidity as well as helps reducing the adverse effects of Maximal Extractable Value (MEV), by redirecting most of the MEV profits back to the users.

Metadata

Available format(s)

PDF

Category

Cryptographic protocols

Publication info

Preprint.

Keywords

private order bookprivacyDEXZK-SNARKbatchingDutch auctionMPCsmart contractsMEVthreshold encryption

Contact author(s)

albert @ nethermind io
adam gagol @ cardinals cc
aikaterini-panagiota @ nethermind io
damian straszak @ cardinals cc
michal @ nethermind io

History

2023-12-06: approved
2023-12-05: received
See all versions

Short URL

https://ia.cr/2023/1868

License

Creative Commons Attribution
CC BY

BibTeX Copy to clipboard

Archived copy · cryp2nova.com

```
@misc{cryptoeprint:2023/1868,
      author = {Albert Garreta and Adam Gągol and Aikaterini-Panagiota Stouka and Damian Straszak and Michal Zajac},
      title = {{COMMON}: Order Book with Privacy},
      howpublished = {Cryptology {ePrint} Archive, Paper 2023/1868},
      year = {2023},
      url = {https://eprint.iacr.org/2023/1868}
}
```



Note: In order to protect the privacy of readers, eprint.iacr.org does not use cookies or embedded third party content.

Archived copy · cryp2nova.com