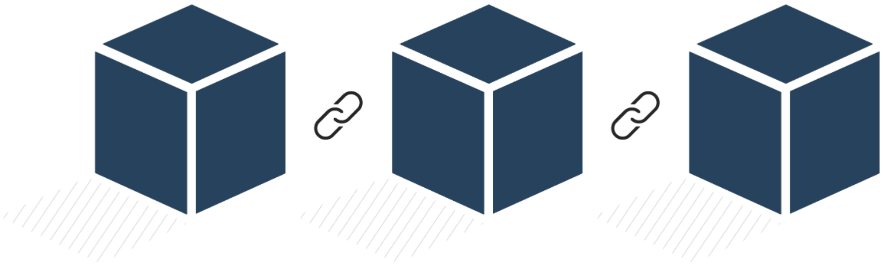
Prof. R. Wattenhofer

Fair Transaction Ordering

The inception of Bitcoin marked the creation of the first fully decentralized cryptocurrency relying on blockchain technology and electrified the world with its potential, namely the ability to securely execute financial transactions without having to rely on a central authority. In Bitcoin, transactions are ordered by the miners. Since then, various blockchains have emerged, and most also have the miners' order transactions. Ethereum is of particular interest as it first introduced smart contracts. Smart contracts allow blockchains to build decentralized applications and handle complex financial transactions. Thus, the Ethereum blockchain does not only process simple transactions but also complex financial transactions.

However, the smart contracts building these decentralized applications have introduced a new transaction ordering dependency to the Ethereum blockchain. This makes it possible for attackers to profit by including, excluding, and reordering the transactions in a block. As the miners currently control the transaction order, the profit that can be made is known as miner extractable value.



Multiple approaches to mitigate such transaction reordering manipulations have surfaced recently, but none have proven to be both effective and efficient [HW22]. In this project we want to explore a new approach to achieve fair transaction orderings on the blockchain.

Requirements: An interest and experience with blockchain is a plus. The project will be both theoretical and practical. 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

References

[HW22] Lioba Heimbach and Roger Wattenhofer. "SoK: Preventing Transaction Reordering Manipulations in Decentralized Finance". In: *arXiv preprint arXiv:2203.11520* (2022).