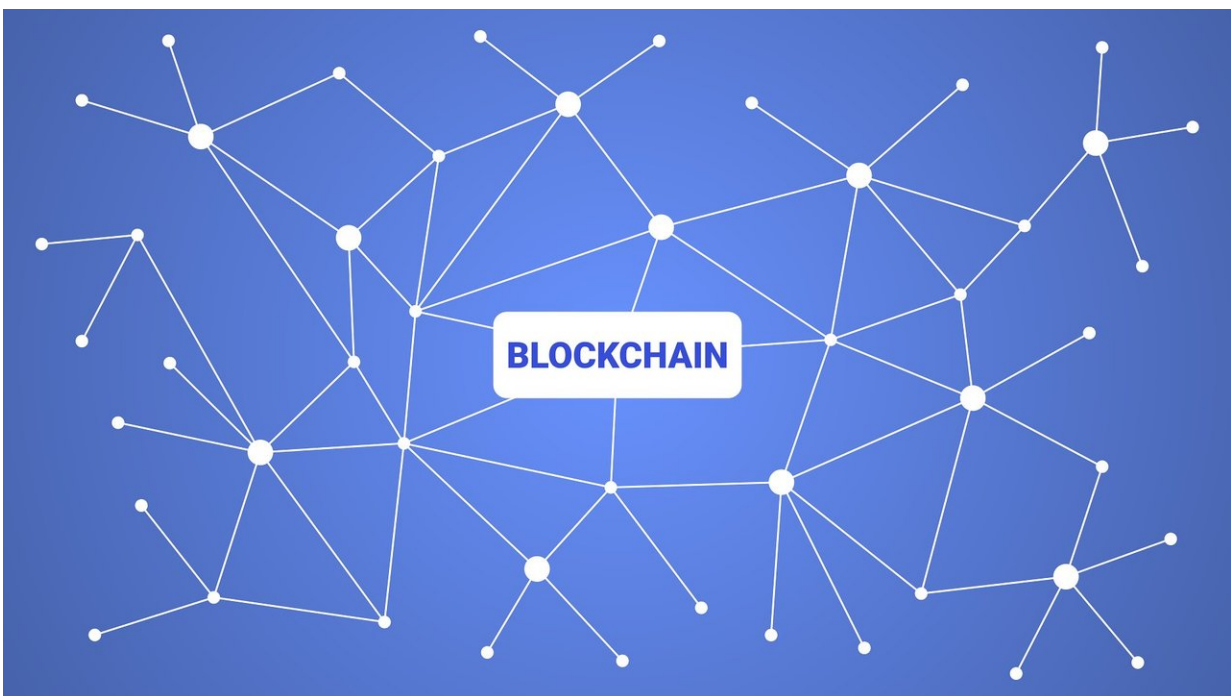


Setchain, an application that multiplies by a thousand the number of transactions per minute in any blockchain

September 26 2022



Credit: CC0 Public Domain

Researchers Margarita Capretto, Martin Ceresa (IMDEA Software), Antonio Fernández Anta (IMDEA Networks), Antonio Russo (IMDEA Networks) and César Sánchez (IMDEA Software) presented Setchain, a new data structure that improves the scalability of blockchains, allowing

a greater number of transactions per block, which leads to a reduction in risk and costs for users, at the 2022 IEEE International Conference on Blockchain.

Modern blockchains employ smart contracts, programs that describe the functionality of transactions. With them, users can observe the details of a transaction from start to finish, generating not only greater confidence but also greater efficiency, as well as more opportunities.

The introduction of the Byzantine consensus algorithm to avoid attacks generated a limitation in the number of transactions inserted in the chain. Hence, there is a growing interest in improving the scalability of blockchains (i.e., improving the performance of the blockchain network to face of a high number of transactions).

In this sense, the research team of IMDEA Software and IMDEA Networks has carried out a joint work that is reflected in the paper "Setchain: Improving Blockchain Scalability with Byzantine Distributed Sets and Barriers," and in the development of the Setchain application. The study is the result of a collaboration agreement between IMDEA Software, the Tezos Foundation and Nomadic Labs, with the aim of meeting the needs of the ecosystem and contributing to the development of the Tezos technology.

According to Margarita Capretto, a pre-doctoral researcher at the IMDEA Software Institute, "right now a blockchain like Ethereum only allows 8,000 transactions per minute while VISA, for example, reaches 100,000. The difference is abysmal. That is why we have worked to create an application that allows us to achieve a breakthrough in this aspect and that can also be applied to any blockchain, not just Tezos."

"The main advantage of Setchain versus a classical blockchains is the scalability," explains Antonio Fernández Anta, Research Professor at

IMDEA Networks Institute. The result of their research shows that if barriers (a conceptual visualization of the boundary between blocks) are not needed too often (no more than once per second), "Setchain allows millions of new transactions to be added, whereas blockchains can usually only add thousands."

He adds, "Setchain allows to store transactions permanently and reliably, introducing order between transactions when it is indispensable. It can be used instead of blockchains when total order between records or transactions is not required, as order in this application is enforced when it is essential to introduce barriers between sets of records." Setchain achieves ordering of the blocks within the chain without requiring the transactions within the blocks to be ordered. The process works more efficiently and saves money for [blockchain](#) users.

Next steps

The authors of the study believe that Setchain can be used to implement a solution to so-called front-running, which is the action of observing a transaction request and maliciously injecting another one just like it before the observed ones are executed, in order to make a profit. This is achieved by paying a higher fee to a miner. Mempools are in charge of encoding the information of what is about to happen in the blockchains, so, anyone observing this data can predict the following transactions and act in their favor.

Fernández Anta warns that, although Setchain's application "are systems used by multiple entities that have to collaborate and may have conflicting interests, Setchain will provide them with a repository that allows them to share data without the risk of any of them manipulating it to their advantage."

The IMDEA Software and IMDEA Networks research team believes

that their application can detect front-running and act as a mechanism to build a more efficient Mempool that encrypts [transaction](#) requests using multi-signature. Research Professor Antonio Fernández Anta comments that the main conclusion they have reached is precisely that "in blockchains the total order requirements are often too restrictive, when most applications do not need them. Relaxing these requirements can lead to huge performance gains."

More information: Paper:

dspace.networks.imdea.org/handle/20.500.12761/1602

Conference: www.blockchain-ieee.org/

Provided by IMDEA Networks Institute

Citation: Setchain, an application that multiplies by a thousand the number of transactions per minute in any blockchain (2022, September 26) retrieved 5 May 2024 from <https://techxplore.com/news/2022-09-setchain-application-thousand-transactions-minute.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.