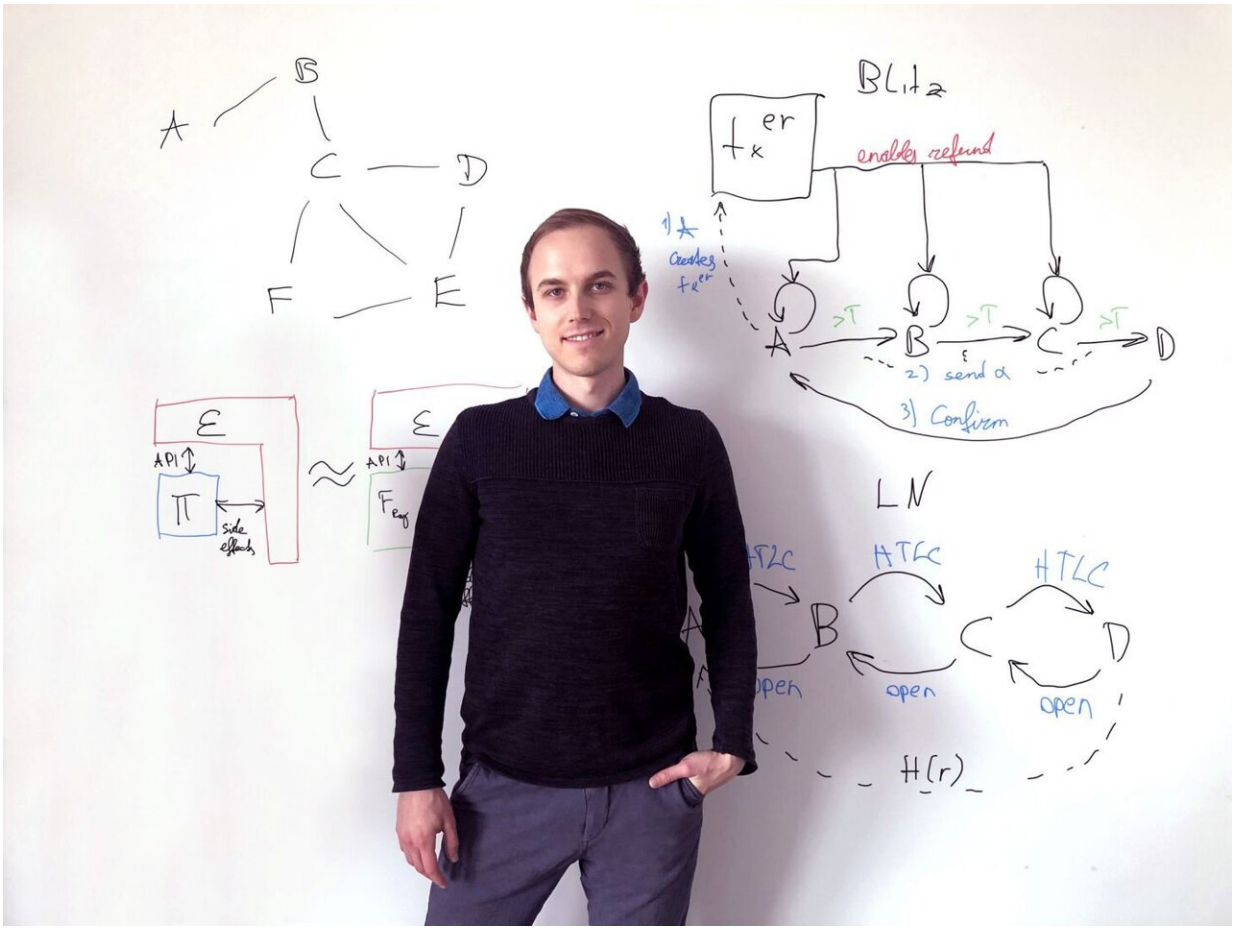
New protocol makes Bitcoin transactions more secure and faster than Lightning

May 4 2021



Lukas Aumayr. Credit: Vienna University of Technology

Cryptocurrencies like Bitcoin are becoming increasingly popular. At first

glance, they have many advantages: Transactions are usually anonymous, fast and inexpensive. But sometimes there are problems with them. In certain situations, fraud is possible, users can discover information about other users that should be kept secret, and sometimes delays occur.

The research unit "Security and Privacy" at TU Wien (Lukas Aumayr and his supervisor Prof. Matteo Maffei) in collaboration with the IMDEA Software Institute (Prof. Pedro Moreno-Sanchez, previously postdoc at TU Wien) and the Purdue University (Prof. Aniket Kate) analyzed these problems and developed an improved protocol. It has now been published and will be presented this year at the USENIX Security Symposium—one of the "Big Four" IT security conferences worldwide, which are considered very prestigious.

The bottleneck of Bitcoin

"It has long been known that Bitcoin and other blockchain technologies have a scalability problem: There can only be a maximum of ten transactions per second," says Lukas Aumayr of the Security and Privacy research unit at TU Wien. "That's very few compared to credit card companies, for example, which perform tens of thousands of transactions per second worldwide."

An approach to solve this problem is the "Lightning Network"—an additional network of payment channels between blockchain users. For example, if two people want to process many transactions in a short period of time, they can exchange payments directly between each other in this way, without each individual transaction being published on the blockchain. Only at the beginning and end of this series of transactions is there an official entry in the blockchain.

These "side branches" of the blockchain can also be made relatively complicated, with chains of multiple users. "Problems can arise in the

process," says Lukas Aumayr. "In certain cases, users can then get hold of data about other users. In addition, everyone in this chain has to contribute a certain amount of money, which is locked as collateral. Sometimes a transaction fails, and then a lot of money can remain locked for a relatively long time—the more people involved, the longer."

Mathematically ruling out vulnerabilities

The research team at TU Wien analyzed how this transaction protocol can be improved and developed an alternative construction. "You can analyze the security of such protocols using formal methods. So we can mathematically prove that our new protocol does not allow certain errors and problems in any situation," says Aumayr.

This makes it possible to rule out very specific security-critical attacks that were previously possible, and also to prevent long-term money blocking: "Previously, two rounds of communication were necessary: In the first round, the money is locked, in the second round it is released—or refunded if there were problems. That could mean an extra day of delay for each user in that chain. With our protocol, the communication chain only has to be run through once," explains Lukas Aumayr.

Simulation proves practicality

However, it is not only the fundamental logical structure of the new protocol that is important, but also its practicality. Therefore, the team simulated in a payment channel network how the new technology behaves compared to the previous Lightning network. The advantages of the new protocol became particularly apparent: depending on the situation, such as whether or not there are attacks and fraud attempts, the new protocol results in a factor of four to 33 fewer failed transactions

than with the conventional Lightning network.

The TU Wien team is already in contact with the Lightning network's development organizations. "Of course, we hope that our technology will be quickly deployed, or at least offered as a more secure alternative to the current technology," says Lukas Aumayr. "Technically, this could be implemented immediately."

More information: Blitz: Secure Multi-Hop Payments Without Two-Phase Commits. www.usenix.org/conference/usen … /presentation/aumayr

Provided by Vienna University of Technology