A new protocol for faster, safer crypto transactions

June 18 2021

Credit: CC0 Public Domain

Researchers from 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) have jointly developed a protocol that makes more secure and faster transactions in cryptocurrencies like Bitcoin.

Nowadays in cities like Tokyo we can subsist with cryptocurrencies like Bitcoin. Buying a coffee, going shopping, taking the bus, paying a taxi or even buying a meal are all accessible if you only have Bitcoin in your (electronic) wallet. This may seem strange for some European countries—even though there are many cryptocurrencies in the market like ATM and coinradar (Spanish market)—but we are moving at a steady speed to that model that may or may not co-exist with our bank cards in the future.

The popularity of cryptocurrencies is increasing very fast due to the many advantages compared to, for example, Mastercard or Visa. Transactions are usually anonymous, decentralized and global.

But there is still work to do in security, privacy and efficiency. Fraud can be possible, users can discover information about other users that should be kept secret, the number of transactions is limited, and sometimes delays occur.

The researchers from the IMDEA Software Institute, TU Wien, and Purdue University, aware of these problems, have developed an improved protocol. The article, in which these ideas are based on, will be presented at the USENIX Security Symposium 2021, one of the best IT security conferences worldwide.

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 Aumayr. "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 at the end of this series of transactions is there an official entry in the blockchain.

As demonstrated by other works of Moreno-Sanchez), the apparent privacy gain of the Lightning Network due to off-chain payments isn't real. In fact, previous work of Moreno-Sanchez has demonstrated that payment intermediaries can learn who pays what to whom. This is an issue that needs to be solved for a system like Lightning Network to become widely used.

A second big issue is that "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 time it will take" says Moreno-Sanchez.

Mathematically ruling out vulnerabilities

"This project has advanced the state of off-chain payments both theoretically and practically. From the theory point of view, we have provided a formal model of the new payment system, proving mathematically its correctness and security against an adversary. Moreover, while current Lightning Network requires two rounds of communication across all participants in a payment, Blitz (the new protocol) reduces it to a single round of communication. This is a milestone result since Lightning Network and other approaches proposed

so far where all using two rounds and it was unknown whether we could beat this barrier" in the IMDEA Software researcher's words.

"In practice, a single round of communication implies great benefits in practicality," says Aumayr "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"

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 the number of attacks and fraud attempts, the new protocol results in a factor of 4 to 33 fewer failed transactions than with the conventional Lightning network.

Moreno-Sanchez and Aumayr are putting efforts on disseminating the results with the Lightning Network developers as well as other Bitcoin organizations. One of the most attractive points so far is that Blitz is totally backwards compatible with currently deployed technologies and could be immediately deployed as a more secure and faster alternative for off-chain payments.

Provided by IMDEA Software Institute