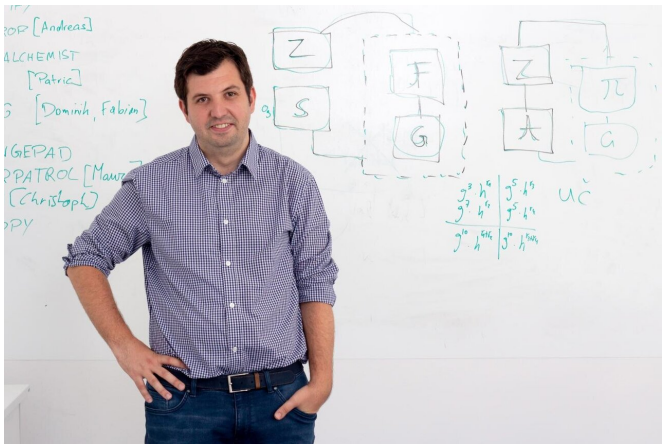
Making blockchain transactions secure and private

25 July 2019, by Florian Aigner



Pedro Moreno-Sanchez, head of the Blockchain lab at TU Wien (Vienna). Credit: TU Wien

Blockchains have become an important part of internet technology. They are used for cryptocurrencies such as Bitcoin, but also for other security-sensitive tasks, such as managing supply chains for high-tech factories. Although blockchains were initially thought to be the holy grail of security and privacy in public information exchange, it turned out that that they actually fall short of keeping that promise.

Given this state of affairs, the Security and Privacy Group at TU Wien (Vienna) launched a blockchain research lab in September 2018. In the past few months, the lab has already been extremely successful: Pedro Moreno-Sanchez, the lab leader, who joined TU Wien in 2018 after receiving his Ph.D. from Purdue University, has raised 820,000 Euros from some of the world's leading blockchain companies; he has won the prestigious FWF Lise Meitner Fellowship; and, perhaps most importantly, he came up with fundamental scientific breakthoughs: Two major security and privacy problems in blockchain technologies have been solved through new cryptographic techniques developed at TU Wien. These solutions have already been implemented by the leading providers of Bitcoin software and are being used to perform thousands of transactions every day.

Coinshuffle and Lightning Networks

Every Bitcoin transaction is published on the blockchain, which can be read by everybody. This is important to make sure that all transactions are verified and, ultimately, all participants agree on which amount of money belongs to whom. But this is at odds with privacy. "In principle, the Bitcoin blockchain is anonymous, as it does not contain any names, just user IDs," says Moreno-Sanchez. "But if I find out which Bitcoin ID belongs to you, I can easily see what you did in the past, and I can monitor your transactions in the future."

A retailer who delivers goods to his customers' home addresses and is paid with Bitcoin can easily match names, addresses and Bitcoin-IDs. "There are even companies that offer this kind of tracking as a paid service," says Moreno-Sanchez.

But this is about to change: Moreno-Sanchez and his team have developed "Coinshuffle," a software tool that can easily be added to existing blockchain technologies, such as Bitcoin. Coinshuffle collects several transactions from different users and merges them, creating one single Bitcoin transaction, while making sure that all participants receive the correct amount of money.

After the transaction, the complete list of IDs that took part in this transaction shows up in the published blockchain, but nobody can tell, who sent money to whom. "We were able to provide a formal proof that this technology is secure," says Pedro Moreno-Sanchez. "Not even the people sharing the single Bitcoin transaction have a chance to break anonymity—this is a mathematically proven fact."

Another problem that Bitcoin faces is scalability:

The sheer number of transactions can hardly be handled any more. Therefore, the Lightning network has been developed: It is a technology that enables business partners who frequently exchange Bitcoins to handle these transactions privately among themselves, without creating a Bitcoin transaction that has to be published all around the world. Only when the two partners agree to end their series of transactions, the remaining balance is settled using a standard Bitcoin transaction.

"Everyone used to think that this improves privacy," says Pedro Moreno-Sanchez. "But we found out that this is not true. The system could even be exploited to steal money from others." But the team at TU Wien was quick to identify and solve this problem, proposing an innovative cryptographic protocol that has been already integrated in the Lightning network.

Turning Basic Research into Working Solutions

Both Coinshuffle and the new cryptographic protocol for Lightning networks have quickly raised the attention of leading blockchain companies. "Just like there are several big companies developing internet browsers, there are several big providers of blockchain software. We talked to them and they have already implemented our solutions," says Moreno-Sanchez. "So thousands of Bitcoin transactions are performed every day all around the world, using the security and privacy-enhancing technologies designed and developed here at TU Wien."

"We are very happy to have our own blockchain research lab here at TU Wien, and it is astonishing how quickly it took off and produced quite amazing results," says Professor Matteo Maffei, leader of the Security and Privacy group at the Institute for Logic and Computation at TU Wien. "Pedro Moreno-Sanchez and his team have not only been incredibly successful raising money from tech companies and delivering useful solutions, they have also earned international acclaim in academia. Their results have been presented at the most prestigious scientific conferences in security and privacy."

Provided by Vienna University of Technology