Making cryptocurrency payments fast and secure

April 29 2020, by Santina Russo

The Snappy team of Srdjan Capkun (r.). Credit: ETH Zurich / Martin Ruetsche

Trading in digital currencies such as Bitcoin or Ether has become an established practice but using them as a payment means is still a slow process. ETH Professor Srdjan Capkun and his team have now developed a system that makes cryptocurrency payments secure, fast and practical.

Cryptocurrencies such as Bitcoin, Ethereum or Ripple used to be nothing

more than an experimental platform for critics of the system, but this has long ceased to be the case. These currencies have now become an established investment strategy. Today, some 5,000 digital currencies are available. The most popular is Bitcoin, which now has over 18 million units in circulation—that's equivalent to more than 126 billion euros. Ethereum, or Ether for short, is the second-largest digital currency and has a total value of around 20 billion euros.

However, transactions with cryptocurrencies are still very slow and therefore not suitable for everyday purchases. Bitcoin users, for example, have to wait up to a whole hour for a payment to be approved. In the case of Ether, which was developed as a full-value substitute for conventional money from the outset, things move faster, with a payment taking three minutes to be confirmed. "This is still too long for many everyday purchases," says Srdjan Capkun, Professor of Information Security at ETH Zurich. "When people are shopping online or buying a coffee to go, not many want to wait a whole three minutes for their payment to process," he says. To address this issue, Capkun and his team have developed a system that speeds up transactions with Ether. They aptly named their solution "Snappy" because it enables payments to go through fast, like a snap of the fingers.

The nature of blockchain

But why is it that transactions with digital currencies still take so long? "It's down to the nature of the blockchains on which the cryptocurrencies are based," Capkun explains. In a blockchain, information is stored on a shared data register. The data isn't available on one centralised server; instead it is continuously synchronised on thousands of participating servers that form a huge worldwide network. That's why communication and the confirmation of transactions take a while. But what this does mean is that the data is transparent and secure: because the information is stored on so many servers at the same time, it is visible to all members

of the network and can't be manipulated by one party. In the blockchain, the same automated rules apply to everyone without the need for trusted authorities, such as banks, credit card companies, or governments, to act as intermediaries.

Some attempts have already been made to accelerate transactions with cryptocurrencies, but these involved removing the payment process from the blockchain and simply synchronising with the network beforehand and afterwards. Although this approach worked, it went against the ideas of security, transparency and freedom from authority that are inherent to blockchain. "We wanted to find a way to do the same thing but without removing the blockchain element," Capkun says.

Smart deposits and guarantees

Capkun and Vasilios Mavroudis, a doctoral student at University College London who was visiting Capkun's group at the time, designed a digital deposit system that runs in the background to the payment process. In addition to their purchase amount, customers place a deposit of the same value—but only for as long as it takes to confirm the payment. So, for the cryptocurrency Ether, the deposit would be held for three minutes—the latency of the Ethereum blockchain.

And because this deposit is active for only three minutes, it doesn't show in the user's own virtual wallet. "However, it allows the seller to immediately confirm the payment without running the risk of losing the sum," Capkun explains. After all, it's only after the blockchain's latency period has expired that the seller sees if the purchase price has been covered. This is where the deposit comes in. If there's something suspicious about the payment, the seller can retrieve the deposit instead. And owing to the fact that nothing can be manipulated within blockchain, the seller doesn't need to make a special claim—if something is amiss, it automatically shows in the blockchain and is plain

for everyone to see.

All eventualities covered

But not only do customers have to provide deposits when using Snappy—sellers do, too. The deposits they pay are higher than those of the buyers and are equal to the sum of all the individual sellers' transactions that take place in the same timeframe. For a small vendor, such as a kiosk, the deposit is low; for a large vendor, it is commensurately higher. Just like the customers' deposit, the deposit the sellers pay also serves as a safeguard against any malicious behaviour, this time on the part of the seller. In this way, Snappy protects against all risks. "And that's why our solution can process payments so quickly and yet securely," Capkun says.

When using Snappy, customers and sellers don't even notice the deposit security system running in the background. Everything is automated thanks to what are known as smart contracts—computer protocols that represent digital contracts. They define processes and rules that everyone in the blockchain automatically complies with.

To use Snappy, its algorithms and protocols can simply be deployed on the Ethereum blockchain. The system is not yet being used in practice, but Capkun envisages Snappy becoming a feature of smartphone apps. In shops or restaurants, for example, a connection to the seller's account could be established via a QR code. The payment process itself would be just as fast and straightforward as with a conventional payment app.

The appeal of new systems

In his working group, security expert Capkun is participating in a number of other projects on blockchain security and privacy. He is also

conducting research into trusted hardware. This involves developing computers and devices based on technology that is completely secure, impossible to manipulate and therefore completely trustworthy. Here, the idea is that people don't have to place their trust in a third party or the manufacturer.

Blockchain and trusted hardware are therefore both approaches that offer an alternative to the current system, which sees authorities acting as intermediaries—be it banks, economic giants or governments. Sitting in his tidy office with his diplomas hanging on the wall, Capkun doesn't look much like a system disruptor. Maybe he's just an anarchist at heart? "No, not at all," he responds with a smile, "it's just that I find these systems intellectually challenging." It perhaps comes as no surprise that he owns Bitcoin and Ether himself, but he's no crypto millionaire.

And that certainly wasn't his intention back when he wrote his doctoral thesis on communication systems. However, Capkun soon came to realize what a key role system and network security play. Since his appointment as a professor at ETH in 2006, he has co-founded two ETH spin-offs, both of which are developing products to improve network security.

Capkun is also prudent when it comes to online privacy and security in his private life. "I'm not a fan of social media," he says. Although Capkun does have a Twitter account, he's rather reluctant to curate it and tends to post only scientific contributions. When the topic of social media comes up with his two daughters, now aged 11 and 8, he'll take the time to talk to them about appropriate conduct in these networks. "Although the social media world appears to be very fast-paced, it's important to remember that once something has been posted online, it remains there forever," he says. "Many people still don't realise that."

More information: Snappy: Fast On-chain Payments with Practical

Collaterals: ethz.ch/content/dam/ethz/speci … s/pub2020/snappy.pdf

Provided by ETH Zurich

Citation: Making cryptocurrency payments fast and secure (2020, April 29) retrieved 17 April 2024 from https://techxplore.com/news/2020-04-cryptocurrency-payments-fast.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.