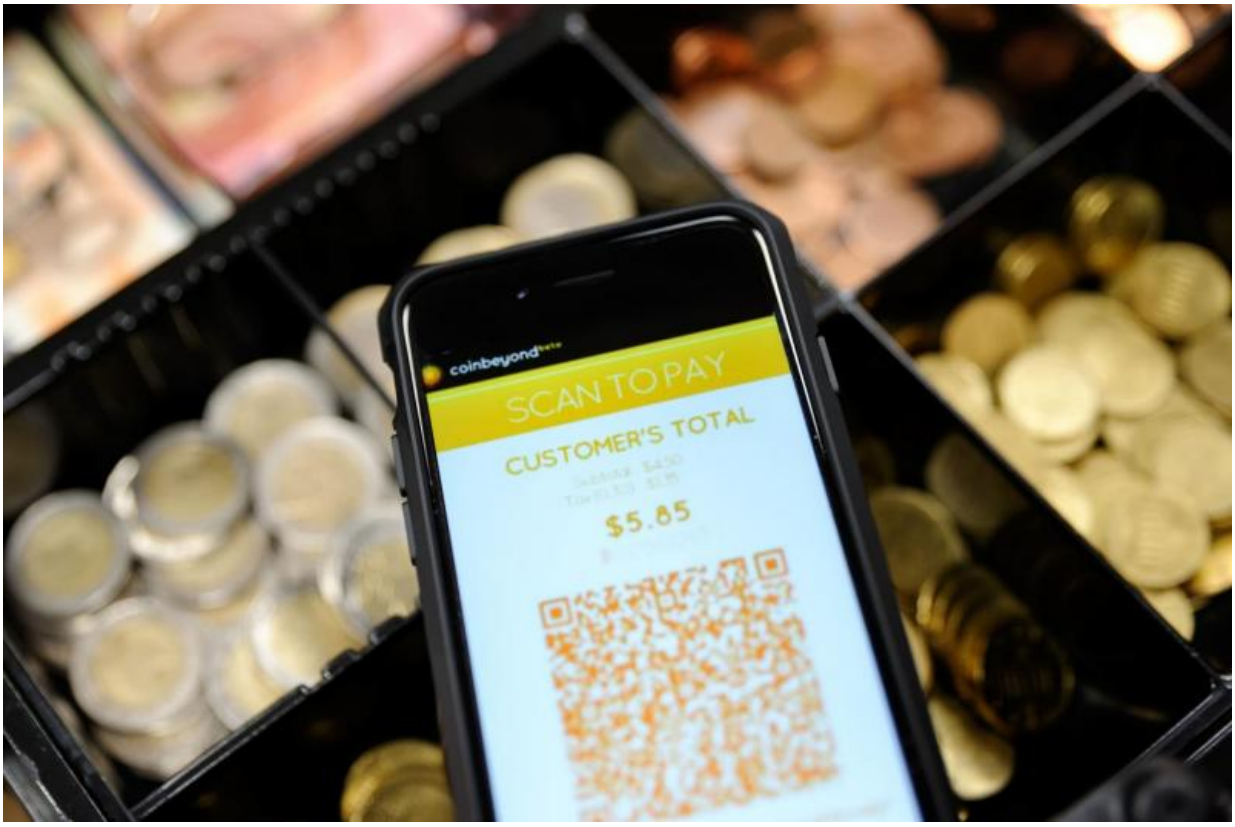
Energy-efficient security mechanisms for digital currency

June 28 2016



In some places, customers have the option to pay using the digital currency Bitcoin. Credit: RUB, Schirdewahn

IT experts at Ruhr-Universität Bochum have developed a new cryptographic puzzle that might one day be used as a security mechanism

for digital currency such as bitcoin. It consumes significantly less energy than the method used to date. The science magazine Rubin reports about their results.

Cryptographic puzzle as security mechanism

A challenge when dealing with digital currency is to make it impossible for users to spend their virtual money twice. This is why the bitcoin system is equipped with a sophisticated security mechanism. Dedicated users, so-called miners, check all transactions that are carried out. The system is considered secure as long as 50 per cent of the computing power in the network is controlled by honest miners.

In order to validate transactions, they currently have to solve a cryptographic puzzle that requires enormous computing power. This mechanism prevents users from gaining control over a bitcoin network by setting up several identities on a computer, because the power users have in the network is measured by their share of computing power.

Energy consumption extremely high

"Experts estimate that the bitcoin network currently has a higher computing power than Google due to this proof-of-work method – which means that it is anything but environmentally sound," says Prof Dr Sebastian Faust from Horst Görtz Institute for IT Security in Bochum. Together with a research group at the Institute of Science and Technology Austria in Vienna and the University of Warsaw, he has come up with an energy-saving alternative, namely the proof-of-space puzzle. It is based on storage space rather than computing power.

New puzzle based on storage space

The user has to initialise the puzzle in a CPU-intensive manner; in the process, a huge portion of the storage space on the hard disk is used. Subsequently, he can solve the puzzle without any considerable computational cost. However, this is only possible as long as the storage space is actually available.

Conceptually, the system works as follows: the puzzle solver has to sort a string of digits in ascending order and save the sorted list. When he wishes to publish the puzzle, he is asked to name the figure in a certain position in the list. If he had saved the sorted list as required, he can read the answer in no time. "This is the basic idea, but in order to build a secure puzzle several technical challenges have to be solved," explains Sebastian Faust.

Method already in use

A group at the Massachusetts Institute of Technology in Boston and at the Institute of Science and Technology Austria has enhanced the proof-of-space concept and introduced a new digital currency based thereon.

Provided by Ruhr-Universitaet-Bochum