Zcash, the virtual money making its mark

May 8 2017, by Luc Olinga

After debuting in October Zcash hit an exchange rate of $1,000 per unit, putting it in league with the much better established Bitcoin, the virtual currency pioneer

Zcash, the latest virtual currency, has been a smash success since its launch seven months ago, drawing in new users with promises of unrivaled privacy protection.

But the new virtual money could face a tough battle integrating into the wider financial system.

After debuting on currency trading platforms in October, Zcash took off, hitting an exchange rate of $1,000 per unit, putting it in league with the much better established Bitcoin, the virtual currency pioneer created in 2009.

While its value has since come down to earth, Zcash is attracting the interest of Russian, Chinese, Venezuelan and, as of May 4, South African consumers.

Brazilians now use Zcash to pay taxes and electricity bills and make purchases.

To make its mark in the world of virtual currencies, Zcash boasts that it protects user privacy.

But because of that guarantee it does not offer the transparency demanded by authorities who want to prevent these new tender from being used in money laundering, financing terrorism, evading taxes or fraud.

Untraceable transactions

Zcash was developed by researchers at Johns Hopkins University and the Massachusetts Institute of Technology in the United States and Tel Aviv University and the Technion-Israel Institute of Technology in Israel. Only five of the six people who developed the cryptography have been publicly identified.

It is based on a technology dubbed zk-Snark, which allows untraceable transactions. The resulting data are encrypted but users are free to identify themselves.

Other cryptocurrencies such as Dash and Monero offer a level of

privacy, but Zcash goes further, even obscuring the origin of a payment.

This is the opposite of Bitcoin, which uses blockchain technology that publicly records transaction details including the unique alphanumeric strings that identify buyers and sellers.

"You don't expose all of your communications or all of your transactions to random people on the internet you barely know," said Zooko Wilcox, CEO of Zerocoin Electric Coin Company, which manages Zcash.

Virtual currencies are produced, or "mined," by banks of computers solving complex algorythms, an operation that can be expensive.

Wilcox told AFP he hoped the expanded privacy protection could overcome businesses' reluctance to adopt Zcash as a trustworthy alternative to traditional state-controlled currencies.

But Jonathan Levin, co-founder of Chainalysis, a start-up that helps banks and authorities trace the origins and destinations of virtual currency payments, doubts Zcash will find its place in the wider financial system.

"It is hard for existing financial institutions to integrate these types of crypto currencies as information on the origin of funds is very hard to ascertain," he said.

Financial institutions began to take an interest in Bitcoin, and in particular in its blockchain technology, once the darknet marketplace known as Silk Road was closed in 2013.

Silk Road facilitated Bitcoin transactions but was also platform for the sale of illegal drugs.

"Nobody has ever used Zcash for any kind of crime as far as anyone knows," Wilcox said, while conceding that "all technologies can be misused."

Hacking threat

Wilcox said he gave a presentation on Zcash to Canadian and US authorities in November and their attitude was "very pragmatic."

Virtual currencies are not regulated by any central bank. In the United States, trading is authorized by individual states which issues license to exchanges, and so far there is no regulation at the federal level.

Unlike central bank-issued demoninations, virtual currencies can be "mined" by anyone with sophisticated software skills to gather up the code.

Nevertheless, despite Zcash's efforts to protect users, the currency itself may be vulnerable to hacking or counterfeiting. In a June attack against another cryptocurrency called ether, hackers reportedly made off with 3.6 million units with a value of $50 million.

Cryptography consultant Peter Todd said in a November blog that Zcash's encryption could be weak, allowing hackers to crack the code.

"The threat here is that an attacker may be able to create fake zk-Snark proofs by breaking the crypto directly, even without having access to the trusted setup backdoor," he wrote.

Wilcox said Zerocoin Electric was alert to such risks and pays hackers to test the currency's security.

In total, Zerocoin Electric expects a maximum of 21 million Zcash units

will be mined, or produced, of which 10 percent will go to Zcash Electric shareholders, including founders, employees and investors.