Bitcoin faces biggest threat yet: a miner takeover

June 17 2014, by Peter Svensson

In this April 7, 2014 file photo, a man arrives for the Inside Bitcoins conference and trade show in New York. The Bitcoin digital currency system is in danger of losing its credibility as an independent payment system because of the growing power of a group that runs the some of the computers behind it. (AP Photo/Mark Lennihan, File)

The Bitcoin digital currency system is in danger of losing its credibility as an independent payment system because of the growing power of a group that runs some of the computers behind it.

In recent weeks, a British-based "mining pool" called GHash has amassed nearly half of the Bitcoin computing power and has briefly gone over 50 percent. Miners operate the computers that keep track of bitcoins and create additional coins.

Miners pool their computing power to spread the financial risk of their operations. If GHash amasses more than half of the computing power devoted to Bitcoin, it could in theory control the flow of transactions, freeze people out of the network and keep all future bitcoins for itself.

Although GHash says it's committed to preserving Bitcoin as a trustable technology, the mere fact that one player can amass majority control could undermine trust in the currency, which is worth only what people are willing to pay for it.

"The entire premise of bitcoin relies on the fact that no single authority would control the majority of the mining power," said Ittay Eyal, a Cornell University researcher who studies bitcoin vulnerabilities.

The value of bitcoins has fallen 6 percent in a week to around $600 as the threat posed by GHash has become clearer, although the decline is within the range of normal fluctuations for the volatile currency.

Bitcoins allow people to send money over the Internet without going through banks. This means transaction costs are low, but it also means they're useful for illegal activities such as money laundering and drug sales. Bitcoins have also become a target of speculators betting on a continued run-up in the currency. Its value has grown a hundredfold over two years.

From a technical standpoint, bitcoins are sequences of numbers, painstakingly produced by computers churning through millions of calculations. Bitcoin transactions are recorded in a virtual public ledger,

known as the blockchain. Miners are in charge of maintaining the blockchain. As their computers perform the calculations to do that, the process rewards them with newly minted bitcoins.

A single mining computer might take years to produce a single block of coins, and there's no way to know when that might happen. In pools, miners divide the bitcoins they create among themselves in proportion to the work done, providing with them with a steadier stream of income. The pools aren't created to threaten the trust placed in bitcoin; it's a side effect of the pool's growth.

GHash is controlled by a British company, CEX.IO Ltd. The company said in a statement Monday that it wants to protect Bitcoin, but it doesn't want to turn away people from the pool or impose other temporary solutions to back away from the 50 percent threshold.

GHash said it's arranging a "round table" meeting of key players in the Bitcoin system in July to "with the aim of discussing and negotiating collectively ways to address the decentralisation of mining as an industry."

Eyal said the problem needs to be fixed in "a very drastic fashion" to reduce the incentive to create pools. That will probably with an update to the software the underlies the system, he said.