Virtual currency "Riecoin" uses computations to help solve math problem

February 27 2014, by Bob Yirka

Riecoin

Bitcoin has been in the headlines a lot lately due first to news that criminals have been using it for transactions, and more recently because of the collapse of its biggest currency exchange. Now comes news of a new type of virtual currency that offers an advantage over Bitcoin. Reicoin (named after Bernhard Riemann, a mathematician who studied the distribution of prime numbers) does everything Bitcoin does, but adds something new by taking advantage of the number crunching involved—it uses the peer-to-peer aspect of virtual currency generation to help solve a math problem by generating a series of prime numbers.

Bitcoin was the first widely known virtual currency—it's based on a peer-to-peer network where currency is generated when users agree to allow their computer to be used as a resource to the system—a process called

mining. Payments are recorded in exchange for transaction fees along with new bitcoins. The currency allows for conducting currency transactions anonymously—hence its use by criminals. Part of the process calls for processing hash functions—for public-key encryption. It's in this part of the process that Reicoin differs. Crunching hash functions by members of a network is resource intensive, and represents a waste of potential processing power.

The people behind Reicoin note that this likely represents work equivalent to multiple supercomputers all tied together. In this new approach, the researchers would like to harness that computing power to help test what is known in mathematical circles as the Riemann hypothesis—a possible method for revealing the pattern behind prime numbers. A proof of the hypothesis could net a million dollar prize from the folks at *Millennium Prize Problems*. The Reicoin project won't make that happen, but it could possibly lead to disproving the hypothesis, which would be of course, just as valuable.

By generating individual prime numbers as a by-product of coin generation, "constellations" of prime numbers could be amassed by the network. Constellations of prime numbers are sequences of numbers that contain prime numbers such that the distance between the first and last is minimized. If one is found in the Reicoin project that doesn't fit with the hypothesis, then the whole hypothesis is disproved.

With the unsettling news regarding Bitcoin, it's unclear if users will be willing to gamble on another type of cyber-currency—in order for Reicoin to be useful, it would need to attract a lot of users.

currency-riecoin-math-problem.html