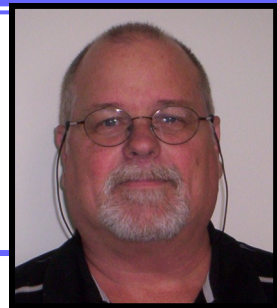


Dana's Desktop

by Dana C. Andrews, Grant County IT Technician



This special edition is to help users understand what Cryptocurrency is, how a 'coin' is made, and why this is impacting organizations.

Cryptocurrency Background

Cryptocurrencies, such as Bitcoin, Ethereum and Monero, have received increasing public attention over the past year. This is due, in part, to a rapid rise in the value of many cryptocurrencies in 2017 from their being legitimized by legal speculation (commodities trading). As legitimate activity associated with cryptocurrencies has increased, so has a variety of criminal activity, from fraudulent "initial coin offerings" to network intrusions. One way criminals receive cryptocurrency without buying it is through "mining."

Cryptocurrency "Mining" and "Mining Pools"

Cryptocurrency "mining" (or "cryptomining") generally uses one or more computers to perform a large number of calculations as quickly as possible. These calculations have a value to them. In order to encourage people to allow their computers to be used this way, cryptocurrency networks typically offer a reward of a percentage of the cryptocurrency value they create. These rewards go to the first miner to perform a calculation having a value that closely matches, but does not exceed, a specific target value.

As cryptocurrency grows more accepted, and transactions increase, more of these calculations are necessary. This means that the difficulty of arriving at the correct value usually increases as well. As of February 23, 2018, the "difficulty" of correctly computing the target value on the Bitcoin network is slightly more than three trillion. This means that correctly computing the target value for a block (another term for coins) as of February 23, 2018 is slightly more than three trillion times as hard as it was for the first Bitcoin block on January 3, 2009. This results in more computing work being required for less reward.

One method to increase the chance of being the first miner to discover the target value, and thereby generate more regular cryptocurrency rewards, is to harness a large number of computers to mine cooperatively. Since buying a large number of high-powered computers is cost prohibitive for most users, legitimate cryptocurrency miners will often form "mining pools" by voluntarily connecting their computers to a network of other computers (some may remember the SETI project where we all helped to try and discover aliens). Mining pools share any resulting rewards in proportion to the work performed on behalf of the group.

Criminal Activity In Cryptomining

However, criminals can take advantage of mining pools as well. They form their groups by compromising victim computers (hacking them) and configuring them to mine on the criminals' behalf as part of a pool. This results in loss of computing time and power for the legitimate user. When they can hack all the computers and servers in an organization, they vastly increase their computing abilities and speed with little or no cost to themselves.