

Is your computer secretly mining Bitcoin alternatives? A guide to 'cryptojacking'

19 December 2017, by Bill Buchanan, The Conversation



What's going on in your computer? Credit: Shutterstock

Nothing comes for free, especially online. Websites and apps that don't charge you for their services are often collecting your data or bombarding you with advertising. Now some sites have found a new way to make money from you: using your computer to generate virtual currencies.

Several [video streaming sites](#) and the popular file sharing network [The Pirate Bay](#) have allegedly been "cryptojacking" their users' computers in this way, as has the free wifi provider in a [Starbucks cafe in Argentina](#). Users may object to this, especially if it slows down their computers. But given how hard it is for most companies to make money from online advertising, it might be something we have to get used to – unless we want to start paying more for things.

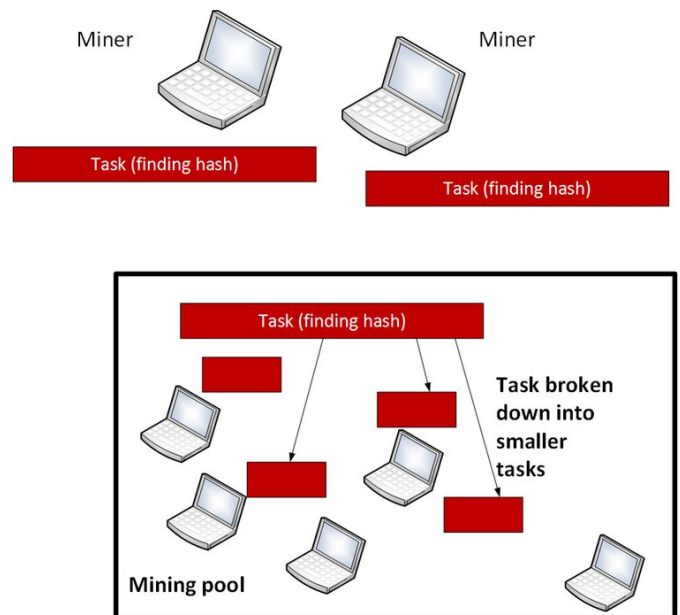
Units of cryptocurrencies such as Bitcoin aren't created by a central bank like regular money but are generated or "mined" by computers solving complex equations. Cryptojacking involves using someone's [computer](#) without their knowledge, perhaps for just seconds at a time, to mine a cryptocurrency.

In the case of Bitcoin, mining requires specialised hardware and consumes masses of energy. For

example, each Bitcoin transaction takes enough energy to boil around 36,000 kettles filled with water. In a year, the whole Bitcoin mining network consumes [more energy than Ireland](#).

But Bitcoin is not the only show in town and there are many competing cryptocurrencies. One of the most successful is Monero, which builds a degree of privacy into transactions (something Bitcoin doesn't do). Currently it requires no specialised hardware for mining, so anyone with computing power to spare can mine it.

Mining usually takes the form of a competition. Whichever computer solves the equation the fastest is rewarded with the money. With Monero and other similar cryptocurrencies, a pool of computers can work together and share the reward if they win the competition. This allows individual computers to work on a just small part of the mining task. The larger the pool, the more chance there is of winning the reward.



Mining pool.

When a computer is cryptojacked, it is added to a pool for to work on the task. This is often done using a commercially available piece of software, [such as Coinhive](#), which can be written into what looks like an ad using the common website language JavaScript. As the ad runs in the background, the computer is added to a pool.

This means the website or internet provider doing the cryptojacking can mine cryptocurrency with little cost to themselves. [One estimate](#) is that 220 of the top 1,000 websites in the world are conducting cryptojacking, making a total of US\$43,000 over a three week period. This might not be very much but file-sharing sites in particular have been searching for new business models in order to support their operations and cryptojacking could grow into a new income source.

The problem for the computer's owner is that this takes up processor power, making other operations take much longer. Pirate Bay users have complained that their processors have been using [up to 85%](#) of their capacity compared with less than 10% for normal operations. This can be accompanied by a large battery drain. The Pirate Bay has since said this high processor usage was a bug and the system should normally use between [20% and 30% of processing power](#).

How do you avoid being cryptojacked?

Coinhive strongly advises the websites that deploy it that they should inform users they are being cryptojacked. But it's common for the code to run without users realising and without a way to opt out of it. If you want to prevent your computer from being cryptojacked you need a software tool which checks the code as it runs such as an ad-blocker.

But you might feel that allowing a site to use a little bit of your computer's processing power is a better alternative to being bombarded with advertising. Whatever you do, you'll likely end up paying for "free" services somehow.

This article was originally published on [The](#)

[Conversation](#). Read the [original article](#).

APA citation: Is your computer secretly mining Bitcoin alternatives? A guide to 'cryptojacking' (2017, December 19) retrieved 1 December 2020 from <https://techxplore.com/news/2017-12-secretly-bitcoin-alternatives-cryptojacking.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.