

Ransomware attack reveals bitcoin as an accessory to cybercrime: Don Pittis

Cryptocurrency has become the new hidden suitcase full of unmarked bills

By Don Pittis, [CBC News](#) Posted: May 16, 2017 5:00 AM ET Last Updated: May 16, 2017 5:00 AM ET

Many good things can be turned to evil uses.

While the anonymous electronic currency bitcoin may have found its first support in the broad community of digital libertarians, the digital payment system has revealed itself as a dangerous tool of criminal oppression.

That has not been good for the cryptocurrency's value.

In a world where big government and giant corporations seem to have an unshakable grip on our lives, the libertarian sentiment that favours anonymity has attracted a justifiably wide following, especially among the high-tech crowd.

But the latest attack by the ransomware program WannaCry, which freezes the victim's computer and threatens to wipe out the data it contains, has been a high-profile demonstration that bitcoin has a dark side.

That is because the substantial ransom demanded by the malware must be paid to the cybercriminals in bitcoins.

No counterculture cheers

Bitcoin has suddenly overtaken the ignominious role in public perception formerly held by a suitcase full of unmarked currency in small denominations left in a secret location.

Perhaps if the attack had been on The Man — on some sort of oppressive corporation or secretive government body — WannaCry would have attracted the counterculture cheers that WikiLeaks has garnered for revealing tax cheats and political hypocrites.

Cyberduffers using old software were a soft target. Targeting them was the work not of Robin Hood but of cyberbullies.

The most oppressive corporations and government departments are the well funded ones best equipped to deal with cyberattacks. In fact, the National Security Agency, a traditional hate object of cyber-libertarians, appears to have [invented key parts of the system](#) used in the ransomware attack.

Victimizing the poor and sick

Some of the victims have been larger corporations. But to date the most prominent casualty is Britain's strapped National Health Service, and the majority of people who have been hurt are by no means rich oppressors.

So far there are no reports of deaths specifically attributed to the attack, but certainly the people who will suffer the most from damage in the attack on the NHS are the poorer and sicker, not the rich, who in the

British system can use money to bypass public health wait times.

Bitcoin uses something called blockchain technology to create two sets of data, one secret and one public. The public information provides a record of the encrypted data that proves each unit of the currency is real and valuable, but owners of those encrypted currency units can remain anonymous.

That makes studying who is using the cryptocurrency difficult. But techniques discussed in a book released last week called [Everybody Lies: Big Data, New Data, and What the Internet Can Tell Us About Who We Really Are](#) offer a partial route around that anonymity.

Using methods he says are similar to those described in the book, University of Kentucky economist Aaron Yelowitz discovered some revealing information about the thinking of people with an interest in bitcoin.

Criminals, not libertarians

[Mining Google search data](#), he tested the thesis that people were using bitcoin on political principle. To oversimplify, he looked for data that showed bitcoin information was being searched because the searchers were libertarians.

"We found that did not matter at all," says Yelowitz.

Instead, he found one other very strong correlation — with illegal activity.

"Google will spit out how much interest there is state-by-state and [we] related that to interest in bitcoin, and what we found was that interest in this illegal activity absolutely did explain quite a bit of the interest in bitcoin," says Yelowitz.

Enabling crime

Effectively, Yelowitz says, bitcoin has become an enabler of illegal activity such as the ransomware attack.

"If you didn't have bitcoin all you could do is ruin people's files," he says. "What's interesting about this ransomware is that unless you had something like bitcoin — a way to profit from it without it being traced — this ransomware stuff would be hard to do."

Cash continues to dribble into the bitcoin accounts associated with the malware, but yesterday White House security adviser Tom Bossert said there is little evidence that people who paid the ransom have had their computers restored.

I'm watching 3 [#ransomware](#)-associated wallets that have received 92 bitcoin payments totaling \$26,407.85 USD. [#wcrypt](#) [#wannacrypt](#)

— [@actual_ransom](#)

Bitcoin has been an amazing invention, creating reliable value-in-exchange from bits and bytes. Last week its value soared to record highs, putting the value of bitcoins in circulation at about \$25 billion US.

But since the ransomware attack, the cryptocurrency has seen a sharp fall.

Yelowitz says that even if the world's governments wanted to get rid of the currency, it would not be easy. Some would like to try.

The latest ransomware attack will only arm bitcoin's critics.

Then of course if the huge publicity over the attacks means the cryptocurrency becomes indelibly associated with criminals and suffering, the sign "Bitcoin Accepted Here" could well lose its trendy commercial appeal.

Follow Don on Twitter [@don_pittis](https://twitter.com/don_pittis)

[More analysis](#) by Don Pittis