BlockTribune
All the News that's fit to Mine

Cato Institute: Can The Government Destroy Bitcoin?

William Luther

October 5, 2017

Cato Institute's William Luther details the history of world government monetary regulation and speculates how it may be applied to cryptocurrency…..

China-based cryptocurrency exchange BTCC suspended all domestic trading in yuanlast weekend. The decision came on the heels of a September 5 statement from regulatory authorities in China, which required all domestic cryptocurrency exchanges publish closing announcements, stop registering new users, and establish a schedule to cease yuan-denominated trading by September 15. Huobi and OKCoin — two other exchanges based in China — have announced similar plans to stop trading. To be clear: China has not banned the use of cryptocurrencies. It has banned cryptocurrency exchanges and initial coin offerings (ICOs). Even still, it has prompted some to consider whether a government might ban cryptocurrencies like bitcoin — and, perhaps more importantly, whether such a ban would be effective.

There seems to be no denying that governments can ban cryptocurrencies. Bolivia, Ecuador, Kyrgyzstan, and Bangladesh have already done so. Russia issued a draft billto ban cryptocurrencies in October 2014 and recent rumors suggest it might follow through. More broadly, governments have taken steps to prevent other alternatives to their preferred monies. Cambodia recently suggested it might ban the dollar. Syriaprohibited the use of any foreign currency in 2013. And the U.S. government shut down Liberty Dollar and E-Gold in the mid-2000s. Can governments ban cryptocurrencies? Absolutely. The question is whether — or, to what extent — a ban will actually discourage use.

Some bitcoin proponents have argued that governments cannot really prevent bitcoin use. Jon Matonis once stated that "a government ban on bitcoin would be about as effective as alcohol prohibition was in the 1920s." How could a government prevent people from using bitcoin? It's online. It's pseudonymous. And, as Matonis notes, "demand for an item […] does not simply evaporate in the face of a jurisdictional ban."

Or, does it? For starters, one must recognize that monetary demand — that is, the demand to use an item as a medium of exchange — is not quite like the demand for most other goods. Monies are subject to network effects. I can enjoy a fine bathtub gin even if no one else does. But the usefulness of a would-be money like bitcoin depends crucially on whether other people are using it. We must coordinate beliefs. If one does not believe others will use bitcoin, she will be less inclined to accept it herself. For cryptocurrencies that lack some non-monetary use, that means demand might fall to zero even if everyone would prefer it to the relevant alternative.

In general, governments might determine the medium of exchange by coordinating beliefs, employing transactions policy, and punishing users of alternatives. By declaring an item legal tender, for example, the government might create an especially salient focal point around which individuals can coordinate on a particular money. Legal tender status might be nothing more than a designation; it need not convey any special privileges under the law (though sometimes it does). Since I want to use the money you are using and you want to use the money I am using, simply stating that the dollar is legal tender and bitcoin is not legal tender might be enough to generate coordination on the dollar. As a large and powerful player in the economy, governments are often in a position to provide such a focal point.

Of course, if the net gains from switching to bitcoin are greater than the costs of coordination, we might establish some competing focal point to coordinate on the superior alternative. In this case, governments might resort to transactions policy — that is, committing to accept and spend its preferred money — in order to prevent bitcoin from gaining widespread acceptance. By collecting taxes and spending dollars (and not bitcoin), the government guarantees some demand for dollars and, correspondingly, limits the potential network size of bitcoin. Some governments will not be able to determine the medium of exchange with transactions policy. But a sufficiently large government can.

Even if a government is not large enough to determine the medium of exchange via transactions policy, it still has one last trick up its sleeve: punishments. By punishing those employing an alternative money, it lowers the expected benefits of the alternative and, hence, the relative demand for its preferred money. Whereas a sufficiently big government is required to determine the medium of exchange with transactions policy, a government of any size can determine the medium of exchange with punishments, so long as it is willing and able to mete out sufficiently severe punishments.

There are some obvious limits to the government's ability to punish cryptocurrency users. For one, it has to find them. And, as Matonis and others have noted, cryptocurrencies like bitcoin are pseudonymous, making it difficult to tie an individual to his or her balance of bitcoin. Difficult, but not impossible.

Even if one has access to a perfectly anonymous payment mechanism, many transactions inevitably reveal one's identity. When you purchase a good or service, there is usually some point in the transaction where you actually receive the good or service. And, at that moment, your identity is vulnerable to detection. That you can send or receive an anonymous payment is of little consequence if the other party in the transaction is a government agent. Sting operations are real.

More importantly, exploring the limits also reveals the vast range of transactions that would be relatively trivial to stamp out. A ban with significant punishments for those caught sending and receiving cryptocurrencies would surely see those "bitcoin accepted here" signs disappear. It would make finding a trading partner willing to use bitcoin a lot more cumbersome. Most people prefer to be on the right side of the law most of the time. Most routine transactions do not warrant the added costs of obscuring one's identity or vetting one's trading partner. Why risk being caught using a banned currency to buy milk and bread? Privacy is just not that important to most people in most situations. No doubt a government would find it difficult — perhaps even impossible — to eliminate *all* bitcoin transactions. But a committed government would have little trouble making bitcoin sufficiently unattractive for most users, significantly limiting bitcoin's potential network size. In such a world, bitcoin would function as a niche currency — or, not at all.

There are exceptional cases, to be sure. If the government's preferred currency is poorly managed (think: hyperinflation, not two-percent) or black market transactions are the norm, one might not hesitate to use a banned alternative. That seems to be the case in Venezuela at present. If one must operate outside the law just to buy lunch, she might not be too concerned about the risk of additional sanctions for using bitcoin. And, since everyone else is operating outside the law, she might be reasonably confident that others will accept bitcoin as well. But such cases are the exception. When bitcoin proponents maintain that governments cannot prevent bitcoin use, they do not usually limit the claim to such extreme scenarios.

Fortunately, very few countries have taken steps to ban cryptocurrencies to date. But the threat is legitimate. Governments might not be able to prevent all cryptocurrency transactions, but they can significantly discourage their use. With this in mind, we should continue to push for choice in currency. We should continue to explain the benefits of financial privacy and stateless monies. However, we should also support sensible regulation that would preserve most of the benefits from cryptocurrencies while eliminating the major justifications for outright bans. It is a second-best solution. In a world with powerful governments, it might be the best one can hope for.

William J. Luther is an adjunct scholar at the Cato Institute, an Assistant Professor of Economics at Kenyon College, and Director of the American Institute for Economic Research's Sound Money Project.