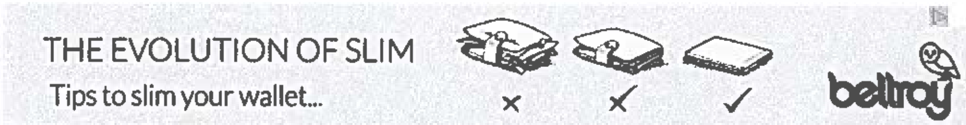
≡ WIRED.CO.UK

6 issues for £9 + FREE iPad & iPhone editionsSubscribe



Why is it so hard to regulate Bitcoin?

FINANCE (/FINANCE) / 25 JUNE 14 /
by CHRIS BARANIUK (/SEARCH/AUTHOR/CHRIS+BARANIUK)

88 Tweet 46 Recommend 5 g+1 6

Casascius

Although increasingly popular, Bitcoin has long been troubled by the ogres of criminal activity and poorly secured exchanges. But regulation continues to be a highly controversial topic, as a group of researchers in The Netherlands recently discovered.

About three months ago, five of Professor Johan Pouwelse's students at the University of Technology in Delft had a brainstorming session. They wanted to come up with a way of improving Bitcoin and they decided they ought to work on a type of regulation for the cryptocurrency which could stop mining activity being attached to Bitcoins that had been used in criminal activity.

But as the weeks passed by, the mood among the students eventually changed from enthusiasm to anxiety. The idea the students were discussing, which involves an effective boycott of Bitcoin wallets used in criminal transactions,

turned out to be anathema to much of the Bitcoin community.

"They had some interactions with community members and they got completely flamed and trolled," explained Pouwelse to Wired.co.uk. "I had five scared students in my room."

Because Bitcoin is designed from the ground up as a decentralised currency, the idea of centrally managed lists of criminal Bitcoin wallets is seen by many as counter-intuitive and, potentially, dangerous.

Mike Hearn, founder of Bitcoin infrastructure development outfit Vinumeris (http://blog.vinumeris.com/), said he doesn't agree with the paper's use of the term "redlisting", a term which he coined (https://bitcointalk.org/index.php?topic=333824.0). He says the researchers are actually proposing a form of blacklisting.

"Government blacklists of all kinds have a terrible track record," he commented. "They're opaque, vague enough to often be just a list of names, have no working appeals process and just generally exist to sidestep the much better judicial systems that already exist."

Semantics aside, one interesting claim the paper makes is that if the researchers' approach were adopted, the Bitcoin network would be split into miners who could choose to abide by the boycott recommendations -- or not. Initially, those who did follow the rules would make fewer profits, but if their group grew to 35% of the network then they would start negatively impacting the profits of the other miners who ignored regulatory advice.

The paper presents a model in which, at this point, those could start losing 15% of their earnings, a loss which only increases as the boycotting miner group takes on more members.

However, for Bitcoin commentator and fellow of the Adam Smith Institute Preston Byrne, the idea would be a hard sell for to the Bitcoin community.

"I simply cannot foresee a network consensus emerging in favour of this functionality," he said, adding, "In effect, this proposal enables the state to render a bitcoin balance valueless. This would both compromise the independence of the protocol and discourage its use -- as a store of value, even cash would be better."

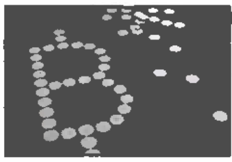
While the cryptocurrency community considers its options, regulation may ultimately come from above. While some countries like Japan (http://www.reuters.com/article/2014/06/19/uk-japan-bitcoin-idUSKBN0EU0JA20140619) are still waiting to decide whether Bitcoin regulation is necessary, others such as Germany (http://bitcoinmagazine.com/9922/regulation-bitcoins-germany-first-comprehensive-statement-bitcoins-german-federal-financial-supervisory-authority-bafin/) and Canada (http://www.duhaimelaw.com/2014/06/22/canada-implements-worlds-first-national-bitcoin-law/) are already imposing restrictions on who can and cannot legally trade virtual currencies. Canadian dealers, for example, will soon have to register with the Financial Transactions and Reports Analysis Centre (FINTRAC) and take active steps to thwart money-laundering.

Mike Hearn's original idea is a softer approach to self-regulation which gives Bitcoin users the option of reporting a set of Bitcoins as stolen to a private sector organisation of some kind which attempts to verify the report. If the coins do indeed appear to be stolen, they can be marked as such. Wallet owners can then decide to help out with an investigation that traces where the Bitcoins might have gone.

The key point is that the whole process, from reporting to investigation, is elective and also allows an avenue for co-operation with authorities of the state -- but only when such intervention is desired.

"To decide that someone actually is a thief or extortionist will almost certainly require a police investigation and then a trial in an open court of law," he said. "The Bitcoin community is in no place to judge someone guilty of breaking rules that can't be summed up in a few lines of

READ NEXT



(/news/archive/2014
OPINION walle
Bitcoin anc
could be us
terrorists. S
(/news/arcl
09/24/bitc-
wallet-terrc

code, so co-operation with the existing legal infrastructure would be essential as the alternative is Reddit-style vigilante justice."

Correction [25 June 16:35]: *A previous version of this article stated that the University of Technology was situated in Amsterdam rather than Delft. It has now been corrected.*

1 COMMENT

LATEST ON WIRED.CO.UK

UK SITES

WIRED INTERNATIONAL

INFORMATION

© Condé Nast UK 2014