Forbes

Bitcoin: 'Blood Diamonds' Of The Digital Era

Jason Bloomberg

March 28, 2017

Bitcoin has long been the transaction currency of choice for drug dealers and extortionists, but this month, the IRS has upped the game. Just as tax evasion finally took down Al Capone, now the IRS is looking for tax evaders and other tax cheats who have been using Bitcoin in an attempt to hide their tracks.

The IRS recently subpoenaed customer records from Coinbase, a leading Bitcoin exchange. However, the subpoena is but the latest skirmish in a years-long war against criminals who have been leveraging Bitcoin for a wide variety of nefarious purposes.

The specifics of the IRS subpoena, however, make one thing clear: the majority of Americans who trade in Bitcoin are likely breaking the law.

Coupled with Bitcoin's popularity among ransomware extortionists and all manner of other cybercriminals, we must now face a chilling realization: the underlying value of Bitcoin really has little if nothing to do with its artificial scarcity or popularity as a medium of speculation.

On the contrary – the only reason Bitcoin has value to anyone is because of the underlying value as a medium of exchange for lawbreakers. If we could flip a switch and eliminate all illegal uses of Bitcoin, there would be nothing left of the cybercurrency.

The 'John Doe' Summons

The most recent order from the IRS to Coinbase is a 'John Doe' summons, which means that the IRS isn't naming any particular Coinbase customers, but is rather issuing a blanket request for information about a large number of individuals – even though the IRS may not have any suspicions about all of them.

In response, Coinbase says that while it has a policy of complying with all legal orders (of which this is one), it believes this one overreaches, and is thus fighting it in court. "Suffice to say, we feel the IRS's subpoena is overly broad and incorrectly implies that all users of virtual currency are evading taxes," writes Coinbase Cofounder and CEO Brian Armstrong in a blog post. "Asking for detailed transaction information on so many people, simply for using digital currency, is a violation of their privacy, and is not the best way for us to accomplish our mutual objective."

The IRS, however, is on firm ground with the John Doe summons. "The IRS uses John Doe summonses to obtain information about possible violations of internal revenue laws by individuals whose identities are unknown," the agency says. "The IRS not only has a suspicion that the John Doe class includes U.S. taxpayers who are not complying with the law – it knows that the class in the past included such violators, and very likely includes others," it continues.

Such noncompliance, in fact, may not always be intentional. It's likely many Bitcoin enthusiasts are inadvertently running afoul of IRS's guidance that Bitcoin is property, not currency. As a result, every Bitcoin interaction is potentially taxable individually, leading to a paperwork headache for active Bitcoin traders.

Be that as it may, the IRS has reason to suspect virtually all Bitcoin traders have fallen into this trap. According to the IRS, it "searched the MTRDB [Modernized Tax Return Database] for Form 8949 data for tax years 2013 through 2015." Form 8949 is the one that Bitcoin traders must use to report their activity. "Those results reflect that in 2013, 807 individuals reported a transaction." Furthermore, the number for 2014 is 893 and for 2015, it dropped to 802 individuals.

Given the number of US citizens to conducted at least one Bitcoin transaction in 2015 probably numbers in the tens or hundreds of thousands, 802 is a mere drop in the bucket. The IRS is quite justified in presuming, therefore, that the vast majority of American Bitcoin traders are breaking the law.

Rationalization to the Rescue?

Armstrong's exhortation that the IRS summons implies that all users of virtual currency are evading taxes is thus an overstatement. More worrisome, however, is his opinion that taking a legal action to enforce tax law is a violation of privacy.

The blogosphere, in fact, is rife with related rationalizations. The most extreme Libertarian proponents of Bitcoin are against taxes and the IRS in general, and even for those individuals who allow for the necessity of taxation, many believe that they are justified in using Bitcoin to evade more onerous legal constraints like the 'Bitcoin is property' guidance.

Another fallacious line of reasoning: the IRS is overstepping because they're looking for a needle in a haystack. "It amounts to nothing more than asking for large amounts of hay in the hope they might find a needle," opines Michael Beckerman, President and CEO of the Internet Association, a trade group whose members include Coinbase as well as companies like Alphabet, Google, Facebook, and Amazon.com.

Such arguments, however, do not sway the IRS. "The IRS not only has a suspicion that the John Doe class includes U.S. taxpayers who are not complying with the law," the agency says. "It knows that the class in the past included such violators, and very likely includes others."

Charles Stross, popular author and blogger, summed up the situation nicely. "Bitcoin is pretty much designed for tax evasion," he quips.

Tax Evasion Merely the Nail in Bitcoin's Coffin

Running afoul of the IRS, however, is merely the focus of the latest news. The fact remains that Bitcoin is enormously popular for all manner of criminal enterprises, from illegal drug dealing to extortion cons.

The most popular con, in fact, is ransomware. The US Justice department reports that ransomware attacks quadrupled in 2016 to an average of 4,000 per day, with extortion amounts ballooning to $209 million for the first quarter of 2016 as compared to $24 million for all of 2015.

While there is broad agreement that most of today's ransomware extortionists demand payment in Bitcoin, there remains disagreement as to whether Bitcoin is the primary cause of the rapid growth in ransomware attacks.

Is Bitcoin in fact tied to the growth of ransomware? "It's helping. I think that's definitely true," says David Emm, Senior Security Researcher at Kaspersky Lab. "The existence of effectively anonymised payment mechanisms definitely plays into the hands of cybercriminals."

Maya Horowitz, Threat Intelligence Group Manager at Check Point Software. Technologies agrees. "It makes it much easier to avoid law enforcement," she says.

And while it's true that Bitcoin is not fully anonymous, many criminals are simply using a Bitcoin-based money laundering operation known as a 'mixing service.' "If you want your money in one wallet but you don't want anyone to be able to trace it back and know how you got it, then you take it though a mixing service – like money laundering – and then it all eventually gets back to you after being mixed with other money," Horowitz says. "It's pretty standard for Bitcoin."

Cue the Rationalization Again

Once again, however, there are a number of voices seeking to diminish the connection between Bitcoin and ransomware – or criminal enterprise in general.

One argument: if it weren't for Bitcoin, bad guys would simply use something else. "The reality is cybercriminals will always use what is available to them," explains Greg Day, VP and CSO, EMEA at Palo Alto Networks. "In many ways they're inherently lazy, so if Bitcoin wasn't there they'd find a different process to channel funds through."

Another argument: paper currency is just as bad, so why all the fuss about Bitcoin? "The U.S. government should find it awkward to regulate bitcoin on the grounds that it facilitates illegal transactions," opines William J. Luther, Assistant Professor of Economics at Kenyon College and an adjunct scholar at the Center for Monetary and Financial Alternatives at the Cato Institute, a conservative think tank. "Its own currency — and the $100 bill in particular — has done so for years."

And then there's the argument that Bitcoin isn't really anonymous in the first place. "If you catch a dealer with drugs and cash on the street, you've caught them committing one crime," says Sarah Meiklejohn, a computer scientist at University College London. "But if you

catch people using something like Silk Road, you've uncovered their whole criminal history. It's like discovering their books."

Silk Road, of course, was the Bitcoin-driven clearinghouse for illegal drugs and stolen credit cards (and other contraband) that law enforcement shuttered in 2014. Bitcoin – and Bitcoin-related crime – have only flourished since.

Bitcoin-centered ransomware is so popular among the criminal element, in fact, because it is dead simple. Any modestly skilled bad actor can simply download the software off the Dark Web, create a Bitcoin wallet, and send out phishing emails to find gullible targets. The number of such extortionists and the typically modest ransoms are usually sufficient to avoid law enforcement investigations – a gamble such criminals are obviously willing to make.

Is that Bitcoin in Your Wallet? Didn't Think So

For the readers of this article who are law-abiding citizens, the cold reality is that there is little reason to get involved in Bitcoin in the first place. "Bitcoin transactions are not very useful in casual purchases, thus there has been little mainstream consumer adoption," admits Mikko Ohtamaa, CTO of Gibraltar-based cybercurrency trader TokenMarket. "Bitcoin shines in anonymous online payments and most day-to-day and/or point-of-sale payments don't require this level of anonymity or the complexity it brings along with it."

The final question for law-abiding, tax-paying citizens who may be interested in speculating in Bitcoin: does the fact that the cybercurrency is primarily used for criminal purposes taint it for other uses, a la blood diamonds?

Such a question of morality is beyond the scope of this article, but important food for thought for anyone interested in using Bitcoin for legal purposes.