Bitcoin Losing Anonymity As IRS Tracks Bitcoiners With New Blockchain Analysis Tools

The Bitcoin community has desperately sought financial anonymity but now is at risk for total betrayal as the IRS and other nations have learned how to track and analyze encrypted blockchains. In the digital age, Technocrats rule anytime they choose to do so. TN Editor

Last month **Alt-Market.com** founder Brandon Smith warned that Bitcoin may not be all that it's cracked up to be in terms of **its purported anonymity**:

> *For years, one of the major original selling points of bitcoin was that it was "anonymous." It always surprised me that so many people in the liberty movement bought into this scam. Surely after the revelations exposed by Edward Snowden and organizations like Wikileaks, it is utterly foolish to believe that anything in the digital world is truly "anonymous." The feds have been proving there is no anonymity, even in bitcoin, for some time, as multiple arrests using bitcoin tracking have indeed occurred when the FBI decided it was in their interest. Meaning, when the feds want to track bitcoin transactions, they can, and it does not matter how well the people involved covered their actions.*

Because every transaction exists on a public blockchain ledger, an enterprising organization – say like the NSA or IRS – could conceivably implement blockchain analysis tools to track down Bitcoin fund transfers around the globe. These days most bitcoin transactions are originated on "trusted" exchanges that exist in Western nations, where governments have always found new and innovative ways to ensure citizens have no privacy whatsoever, especially when it comes to personal finances. This means that there is more than likely a record of your original Bitcoin transaction, perhaps involving a credit card or bank transfer, and if regulators ask an exchange to turn over the information you can bet they'll do so in order to avoid unwanted government scrutiny. Moreover, most exchanges now require a driver's license, passport and even a phone number in order to approve your account for trading.

The point is, for government investigators with a bone to pick, your crypto currency activities online may not be as anonymous and private as you may think.

In fact, so exposed is the blockchain to Big Brother monitoring and interference, that the Internal Revenue Service has now implemented blockchain analysis tools to help them track down individuals who are profiting off the crypto currency and not declaring these profits on their tax returns.

Via **Bitcoin.com**:

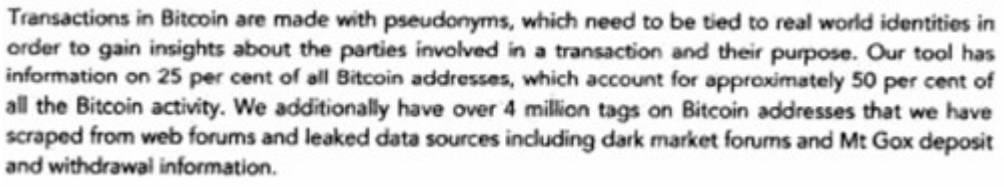
> *According to a contract recently obtained by the Daily Beast, the IRS can now track bitcoin and other cryptocurrency addresses. They can do this to route out potential tax evaders. They purchased software from the blockchain analysis group Chainalysis.*
>
> *The document details that "criminals" have used digital currencies to launder money, deal drugs, and commit other unlawful behavior. However, criminals have also been using digital currencies to ignore tax liabilities and evade responsibility. The Daily Beast article elaborated:*
>
> > *The document highlights how law enforcement isn't only concerned with criminals accumulating bitcoin from selling drugs*

or hacking targets, but also those who use the currency to hide wealth or avoid paying taxes.

Reason for IRS Crackdown; Tracking Bitcoiners

The reason the IRS is cracking down on digital currencies appears to be because only 802 people declared bitcoin profits or losses in 2015. The Daily Beast article suggests that many people may have not expected the IRS to collect on digital currencies. Others may have just thought they could easily sidestep this alleged obligation.

As a result of this failure to pay taxes, the IRS consulted with Chainalysis. ***They are now providing the IRS with tools to track bitcoin addresses through the blockchain and centralized exchanges.*** *A Fortune article captured a screen shot of the letter:*



Transactions in Bitcoin are made with pseudonyms, which need to be tied to real world identities in order to gain insights about the parties involved in a transaction and their purpose. Our tool has information on 25 per cent of all Bitcoin addresses, which account for approximately 50 per cent of all the Bitcoin activity. We additionally have over 4 million tags on Bitcoin addresses that we have scraped from web forums and leaked data sources including dark market forums and Mt Gox deposit and withdrawal information.

The tool that Chainaylsis gave the IRS is called a refactor tool. ***It visualizes, tracks, and analysis transactions on the blockchain. Agencies from law enforcement, IRS, and banks will be able to use the tool****, according to sources. To date, records show the IRS has paid Chainaylsis $88,700 since 2015 for its services.*

Full article at bitcoin.com

Prepare for a full-out onslaught against the government's newest enemy: crypto terrorists.

That means YOU, if you happen to own any Bitcoin.

Because as we highlighted in 2014, under new directives passed by the Obama Administration, **concrete facts are not necessary for you to be put on any number of government watch lists**:

> *The recently declassified Watchlisting Guidance rule book issued in 2013 and developed by members of 19 law enforcement agencies that include the FBI, NSA, CIA, and NSA, outlines the rules for placing individuals, including American citizens, on the various watch lists currently in use. As noted by The Intercept, the rules, much like America's secretive anti-terrorism laws, are vague and often contradict each other.*
>
> > *It reveals a confounding and convoluted system filled with exceptions to its own rules, and it relies on the elastic concept of "reasonable suspicion" as a standard for determining whether someone is a possible threat.*
> >
> > ***Because the government tracks "suspected terrorists" as well as "known terrorists," individuals can be watchlisted if they are suspected of being a suspected terrorist, or if they are suspected of associating with people who are suspected of terrorism activity.***
> >
> > *"Instead of a watchlist limited to actual, known terrorists, the government has built a vast system based on the unproven and flawed premise that it can predict if a person will commit a terrorist act in the future," says Hina Shamsi, the head of the ACLU's National Security Project. "On that dangerous theory, the government is secretly blacklisting people as suspected terrorists and giving them the impossible task of proving themselves innocent of a threat they haven't carried out."*
> >
> > The guidelines for who is or is not a terrorist are now so vague that any American could potentially be added to a list for something as menial as knowing someone who has committed an activity deemed to be of terrorist nature. And as has been highlighted previously, those activities could range from making a hand gesture that looks like a gun or manufacturing your own gold and silver coins.

And now, of course, trading or owning Bitcoin.

Read full story here…