Is Bitcoin the New Swiss Bank Account (And Is That a Problem?)

Victoria Ross

March 24, 2016

Bitcoin was embraced by many for its libertarian ideals of economic liberty and individual sovereignty. But it has now effectively been dragged into the current, and very public, privacy debate between Apple and the FBI.

Last week, President Barack Obama said he believes a balance must be sought between privacy and security. As one example of the risks of strong encryption, and seemingly referring to cryptocurrencies, Obama pointed out that if government can't access phones, "everybody is walking around with a Swiss bank account in their pocket."

To find out where Bitcoin's industry representatives stand on this issue, *Bitcoin Magazine* reached out to Bitcoin Foundation director Bruce Fenton Coin Centerdirector of research Peter Van Valkenburgh, and senior fellow at the libertarian think tank Cato institute and former Bitcoin Foundation board member Jim Harper.

Encryption and Law Enforcement

The current debate on encryption started when recent acts of terrorism in San Bernardino, California brought about a highly publicized showdown between Apple and the FBI.

After a San Bernardino couple, Syed Farook and his wife, Tashfeen Malik, killed 14 people, the FBI found Farook's iPhone 5C was locked with a password and data encrypted. The action of the FBI to seek the decryption from the terrorist Farook's iPhone brought Apple into the California district court of Judge Sheri Pym, who ruled Apple should offer "reasonable technical assistance" to law enforcement, and must provide a tool that would allow federal agents to beat a security feature that prevents the phone from erasing after some failed unlocking attempts.

Apple CEO Tim Cook, however, worries that creating a patch to enable entry through a back door threatens the ability to maintain privacy for its hundreds of millions of customers worldwide.

This sentiment was echoed by Bitcoin industry representatives.

Bitcoin Foundation director Bruce Fenton – who also organizes the industry's Satoshi Roundtable – took over as director of the foundation last year.

Speaking to *Bitcoin Magazine*, he stated:

"There are those who believe privacy is a right and there are those who believe that it is not. I don't support efforts to erode privacy under claims of defense from imaginary threats."

Jim Harper, who at Cato works to adapt law and policy to the information age, wholeheartedly agreed.

"Weakening encryption for terrorism investigations, money laundering prevention and tax collection would cost more in lost security for everyone than it would benefit us through greater security, crime control and fattened government coffers," Harper said. "I've personally been working for several years to strengthen Fourth Amendment doctrine in the Supreme Court. My work may help courts recognize that conscripting Apple into writing code that breaks its security is a Fourth Amendment seizure of Apple's resources, and an unreasonable one."

Implications for Bitcoin

Several Bitcoin wallet apps currently offer "zero knowledge security" which ensures user data by generating private keys completely client side.

But what happens if Pandora's Box is opened? What if encryption is weakened or even broken by state agencies?

Zeid Ra'ad al-Hussein, the United Nations high commissioner for human rights, sees trying to break the encryption protecting one phone as having "extremely damaging implications" for the rights of many millions of people worldwide, with possible effects on their physical and financial security.

Obama, meanwhile, seemed to suggest that this kind of financial security should in fact not be absolute. He believes a balance must be struck, suggesting encryption should be weakened to allow government agencies access to encrypted phones in certain cases.

Peter Van Valkenburgh, director of research at Coin Center, doubts any technical trade-offs are possible at all.

"You can't weaken encryption," he explained. "You can only weaken the ability of American companies to compete in the development of secure technologies, and the ability of law-abiding American citizens to have secure tools. If Americans don't build and maintain these tools, then people in other countries or in the underground economy will. Outlawing the use or development of these tools will only hasten the demise of our legitimate institutions as they would continually fail to compete with international or extralegal institutions that are not hobbled by impractical restrictions."

But what if it is indeed technically possible to completely shut state agencies out of phones? Should that be considered a problem? Should we as a society be concerned about citizens walking around with Swiss bank accounts in their pockets, as Obama suggested?

Fenton doesn't believe so.

“My first reaction to the president's statement was: 'So what?' Why should the federal government care if people have a bank account in their pocket? That is a technological achievement, and, in itself, is nothing close to a crime that government should be concerned with," Fenton said.

He added:

“It is concerning when politicians reach far from concerns about crimes that have actual victims to areas which are more about restricting freedom than protecting citizens. I think we do need to worry about the trend of government officials who push the idea that citizens having privacy and control of their own money is somehow a bad thing. It's only in recent years, with the proliferation of credit cards and online banking, that government has become so presumptive about their rights to our privacy. I think this is much more dangerous than whatever drawbacks that privacy may have.”

Tax Implications

The main reason Obama used the Swiss bank analogy is probably tax evasion. Using Bitcoin, it becomes increasingly easy for users to hide vast amounts of wealth, which enables citizens to avoid certain forms of tax evasion.

Industry representatives actually shared this concern – or at least believe the concern is valid.

Though, according to Fenton:

“The tail should not wag the dog regarding taxes and Bitcoin. Commerce, innovation and jobs come first. The IRS for decades had to deal with cash-based economies where it was very difficult to track real income and revenue. They should adjust and do whatever they need to do to adapt to new technology; we should not delay or impede innovation for concern that the IRS may have a harder job.“

Harper believes potential tax evasion issues will eventually call for alternative solutions.

“In decades or perhaps even a century, Bitcoin or successor currencies and transaction mechanisms may narrow the field of taxable transactions,” he said. “Fully digital transactions will be too fluid to catch or may lack a recognizable physical jurisdiction. This will push tax collection toward physical things like housing, durable goods, and disposable goods. It's all a long way off, though, I'll emphasize.”

Money Laundering

Another problem often brought up regarding Bitcoin is money laundering. Increased anonymity and the inability of law enforcement to block or regulate the flow of funds enables criminals to use Bitcoin for nefarious purposes.

Fenton:

“People like New York State's former Superintendent of Financial Services Ben Lawsky, who's responsible for the BitLicense, seem to take it as a given and indisputable fact that money laundering is a horrible crime. I challenge that notion. In most cases of money laundering there is no clear victim, no person or people who were actually harmed. Opportunists make the leap of saying that things like terrorism will be more prevalent because of money laundering, but this is hogwash. Terrorism is more of a risk because of things like bad foreign policy than money laundering. Could technologies like Bitcoin make life easier for criminals? Of course. Just as shoes, the Internet and mobile phones do. New technologies make things easier for everyone. Regulators and thief supporters would be better off spending time focusing on violators of the law than on technologies.”

Harper agreed:

“I don't worry about degrading governments' power to curtail money laundering because it is a regulatory crime, not a genuine wrong. Money laundering controls probably cost more in compliance expense and curtailed trade (especially internationally) than they provide in security, crime control and quality-of-life benefits. We're worse off as a society because of money laundering laws and the financial surveillance that supports them.”

As such, the question is what the Bitcoin community can do to protect itself against potential weakening of encryption or breaches of security. Should Bitcoin companies and users accept certain trade-offs, or should they move to protect themselves?

Harper prefers the latter.

“Our best defense is going to be shifting to open source, non-proprietary communications and transaction tools. Such tools don't have a head office that can be bought off, bullied, or required by law to render themselves insecure. It's going to be hard to make that shift, but there's no time like the present to get started,” he said.