BloombergView

Are Bitcoins the Criminal's Best Friend?

NOV 18, 2013 1:29 PM EST

By Stephen Mihm

a A

Until very recently, the virtual currency known as bitcoins could be mistaken for just another Internet fad (the Winkelvoss twins of Facebook fame even had a role). But when federal law enforcement closed the "Silk Road," the wildly popular online illegal-drug emporium that used Bitcoin as a medium of exchange, politicians and policy makers took notice. Criminals, it turns out, really like bitcoins, which can be exchanged for nefarious purposes on the "Dark Web," with complete anonymity and, it seems, impunity.

The shift to a virtual currency signals a huge -- and worrisome -- shift in behavior for criminals, who for decades have favored cold, hard cash, with the dollar the preferred medium of exchange. Just how alarmed we should be is one of the topics of a hearing today in the Senate Committee on Homeland Security and Governmental Affairs.

A refresher on the history of the relationship between crime and cash might be a good place to start.

Try, for a moment, to think like a criminal. Any financial transaction that leaves a trace also leaves evidence of your misdeeds. For that reason, cash has been king. For years, wrongdoers of every stripe, from hit men to drug dealers, had to tote around suitcases full of dollar bills to trade illegal goods and services.

In the 1960s, though, narcotics traffickers selling drugs in U.S. cities faced daunting logistical challenges when it came to cash. Their merchandise was paid for in small bills. But how to get that money back to, say, a drug kingpin in Columbia? One option was to smuggle the cash in bulk, an approach that has become increasingly risky. Instead, gangs began to hire small-time couriers to gather up the revenue from local dealers and deposit it in local banks. Once deposited, this cash could readily be laundered via transfers to foreign accounts.

This flood of cash was welcomed by banks because it gave them reserves for profitable, low-risk

loans. As the journalist David Andelman later observed: "The banks turned a blind eye to the source of this wealth. They never questioned the propriety of fish stands or vegetables markets that were generating half a million dollars a day in cash, all in small-denomination bills."

In 1970, Congress passed the Bank Secrecy Act, which attempted to make it impossible to launder money through the U.S. banking system. Under its terms, banks had to report cash transactions in excess of $10,000 via a Currency Transaction Report. Some banks complied with the regulations; others didn't. In the late 1970s and early 1980s, federal law enforcement officials, the Internal Revenue Service and the Customs Service all created task forces to target money laundering of this sort. The first of these, "Operation Greenback," led to the prosecution of both money launderers and banks for violations of the BSA. Other high-profile campaigns followed.

Yet these efforts barely put a dent in the billions of dollars being laundered through U.S. banks. Worse, street-level dealers quickly circumvented the BSA requirements by setting up small bank accounts to launder their proceeds. Each day, low-level couriers -- dubbed "smurfs" -- would deposit sums of $9,900 or so into these accounts in order to avoid triggering a "Currency Transaction Report" to the federal government.

Congress moved to fix the problem in stages in the succeeding years. The most significant update was in 1986, with the Money Laundering Control Act, which imposed far more serious penalties for evading the requirements of the BSA. It also enabled banks to provide information on customers to the federal government without violating privacy laws. Increasingly, banks opted to cooperate rather than risk a prosecution, and by the late 1980s it had become rather difficult to launder money from within the U.S.

The same, however, couldn't be said of banks in other countries, particularly those with a history of taking deposits with no questions asked. Increasingly, criminals, especially drug traffickers, focused their efforts on shipping their cash proceeds out of the U.S. to be laundered in more hospitable locales that put a premium on bank secrecy: Venezuela, the Cayman Islands, and other places off the beaten path.

But, as before, moving cash out of the U.S. presented a serious logistical challenge, one that in some cases exceeded the obstacles in the way of getting drugs here in the first place. Simply put, the ill-gotten cash weighed too much. In 1997, the Justice Department estimated that every pound of cocaine sold on the street generated six pounds of cash; every pound of heroin yielded 10 pounds of small-denomination bills. This posed a bit of a problem, particularly because the BSA required that anyone leaving the country with more than $5,000 had to report their actions to the

government. Faced with this obstacle, the drug cartels resorted to a host of expedients, filling hollowed-out objects from toasters to washing machines with cash and shipping them out of the country.

In what may or may not be a coincidence, the amount of dollars in circulation outside the U.S. exploded in the 1990s and early 2000s, from $86 billion in 1980, to $401 billion in 1999, to more than $500 billion today. Most of the increase can be attributed to the ever-growing demand for $100 bills. Economists have puzzled over why this is the case, but illicit economic activity likely played a role. The fact that the dollar is accepted the world over, and is readily converted into any number of other currencies, also makes it well-suited for international criminal activity.

Even so, the old problems remained. They got worse after the Sept. 11 attacks, when growing scrutiny of international banking transactions made money laundering more perilous, and not only in the U.S. In the process, cash became the weak link in the international criminal economy. It was bulky, hard to hide, and suspicious: anyone with millions of dollars in cash on hand is automatically a suspect.

That's where digital currencies come into play. In recent years, criminals started experimenting with online payment systems. The most successful of these was a Costa Rican payments processor called Liberty Reserve. It accepted deposits of "dirty" money, converted them into a digital currency (Liberty Reserve dollars) and then converted them back again into clean currencies. This online money laundering took place behind a veil of anonymity. It was eventually shut down, but not before it allegedly laundered $6 billion. One of its founders, Vladimir Kats, pleaded guilty to money laundering and operating an unlicensed money transmitting business on Oct. 31.

Unlike Liberty Reserve, Bitcoin's transactions aren't truly invisible. Thanks to the elaborate software architecture that stands behind this "cryptocurrency," it's possible to see the web of exchanges involving Bitcoin. But it's not possible to see who is using them, much less what they're buying. Little wonder that bitcoins have a growing criminal constituency, particularly in the unregulated, murky online world of the "Deep Web."

The U.S. government recently imposed money laundering controls on legitimate businesses that use bitcoins, and a recent study suggests that it's pretty hard to use them to launder money on a mass scale, though the FBI has argued otherwise.

Bitcoin may have a bright future in the above-ground world, too. In letters to the Senate committee holding the hearing today, the Department of Justice and the Securities and Exchange Commission

said the virtual currency is a legitimate financial instrument, which like any other online-payment system, offers benefits and presents risks.

Speculators, meanwhile, are voting with their wallets. The currency has soared in value since the closing of the "Silk Road" marketplace drew wide attention to it.

And given the speed with which bitcoins entered illicit commerce, it looks likely that drug traffickers and other international criminals will ditch old-fashioned cash for digital currencies. This shouldn't come as a surprise. When it comes to moving ill-gotten gains, hitting a few keys on a laptop beats shipping bogus toaster stuffed with cash.

(Stephen Mihm, an associate professor of history at the University of Georgia, is a contributor to the Ticker. Follow him on Twitter.)