New York Law Journal
SERVING THE BENCH AND BAR SINCE 1888
WWW.NYLJ.COM
An ALM Publication
VOLUME 251—NO. 20
THURSDAY, JANUARY 30, 2014

INTERNATIONAL CRIMINAL LAW AND ENFORCEMENT

Expert Analysis

Bitcoins: 'Illegal Tender' Or Currency of the Future?


By **Nicholas M. De Feis** And **Philip C. Patterson**

Each day brings a new article about the digital currency called bitcoins. As some commentators deride them as unsafe or a fad, bitcoins trade on bitcoin exchanges at values close to $1,000 and with a market capitalization of around $10 billion.[1] Former Federal Reserve Chair Ben Bernanke told the U.S. Senate in November that currencies such as bitcoins "may hold long-term promise," while two weeks later China's central bank banned Chinese banks from accepting bitcoins.[2] Meanwhile, Vancouver has the world's first bitcoin ATM, and attempts are being made to bring one to New York City. And announcements by corporations such as Richard Branson's Virgin Galactic that it will accept bitcoins as payment for space flights indicate that bitcoins, for the moment at least, undoubtedly have a certain cool cachet.

Bitcoins do, however, have a dark side, including serving as the exclusive form of payment for the infamous online narcotics bazaar known as Silk Road. Ironically, the greatest testament to the viability of bitcoins may be the fact that the U.S. Department of Justice's Silk Road prosecution has included the seizure of bitcoins.

A further testament to their potential is the number of competitors challenging them. Digital currencies such as Ripple, Litecoin, Peercoin and others are similar to bitcoin but with their own variations. The increasing number of these digital currencies—sometimes referred to as virtual currencies or altcoins—indicates that the concepts, if not the brands, are here to stay. As set forth below, however, bitcoins raise a host of international regulatory and enforcement issues that ultimately may have to be addressed by every government in the world.

What Are Bitcoins?

In 2008, a paper was posted on the Internet under the pseudonym Satoshi Nakamoto proposing the creation of bitcoins.[3] To date, no one knows who Satoshi Nakamoto is, or whether he is even one person or many, but the bitcoin currency described in the paper went online in 2009. The website bitcoin.org provides a detailed explanation of what bitcoins are and how they work. Bitcoins are essentially a digital unit of currency, but, unlike online pay services such as Paypal, they are not linked to actual currencies such as U.S. dollars. Instead, bitcoins are the product of open source technology supported by a peer-to-peer network. Each bitcoin is created through "bitcoin mining," although the process is poorly named. Bitcoins are not, as the "mining" name suggests, collected by trolling the depths of the Internet. Instead, people who devote computing power to supporting the bitcoin network are rewarded with the creation of bitcoins. This has spawned a cottage industry of "miners" purchasing ever more powerful computers and pooling their computing power to try to create more bitcoins for themselves.

The primary innovation of bitcoin is the apparent solution of the "double spending" problem that has undermined previous attempts to create digital currencies. Double spending occurs when a unit of digital currency is duplicated and spent twice or more, thus undermining the currency. Bitcoin's solution to this problem is the "block chain," which is essentially an online public ledger that time stamps and records all bitcoin transactions using a diffuse, decentralized network of computers. If someone tries to duplicate a bitcoin, the publicly available block chain reveals that the duplicate is illegitimate. In a sense, the block chain is similar to confirming clear title in a real estate transaction. The block chain is controlled by a consensus of the computers involved, meaning that the only way for a criminal to alter the chain and steal or duplicate a bitcoin would be by controlling the majority of computing power maintaining the block chain.

Apart from this greater reliability, the benefits of bitcoin, as touted by its creator(s), are many. Bitcoins can be used to instantly pay for goods or services anywhere in the world and at any time. There are no bitcoin bank holidays, although verification of a transaction by the block chain can take 10 minutes. Bitcoin fees are also low by comparison to other forms of payment, although they exist. Paying a fee results in faster transaction processing.[4]

NICHOLAS M. DE FEIS *is a partner at De Feis O'Connell & Rose and a former federal prosecutor.* PHILIP C. PATTERSON *is counsel to the firm.*

Most significantly, both to supporters and skeptics, bitcoins may be safe and reliable in part because they are not the product of a government. Currencies issued by central banks or treasuries can be counterfeited. Moreover, banks and treasuries can print money by fiat, meaning that currency holders always run the risk that a government, rather than market forces, will arbitrarily alter the value of its currency. The best recent example of this risk is Zimbabwe, which from 2007 to 2009 tried to pay its mounting debts simply by printing more currency. The demise of the Zimbabwean dollar was preceded only slightly by the issuance of the $100 trillion bill. In contrast, the bitcoin system is designed to gradually reduce the creation of new bitcoins until creation ceases with 21 million bitcoins in circulation.[5] At that point, presumably, there is a finite number of bitcoins and their value will depend solely on market forces.

No bitcoin entity—not even its creator(s)—can issue more bitcoins arbitrarily. Bitcoins thus appear to offer a stable and fast means of payment. The reliability and efficiency of bitcoins, however, are attractive to those engaged in both legitimate and illegitimate transactions.

Global Potential for Abuse

On Oct. 1, 2013, the U.S. Department of Justice announced the arrest in San Francisco of alleged Silk Road mastermind Ross Ulbricht. Ulbricht, a 29-year-old U.S. citizen, has been charged in both the District of Maryland and Southern District of New York.[6] Silk Road was allegedly an online bazaar where anyone anywhere in the world could purchase contraband ranging from narcotics, forged identification and computer malware to murder-for-hire contracts. The unsealed complaint in New York charges him with narcotics, computer hacking and money laundering conspiracies and describes Silk Road as "the most sophisticated and extensive criminal marketplace on the Internet today" with 9.5 million in bitcoin revenue and 600,000 in bitcoin commissions paid over a period of about two years. According to the complaint, agents made over 100 narcotics purchases from Silk Road counterparties located in 10 countries throughout Europe and the Americas.[7]

The indictment in Maryland makes similar allegations, but also alleges that Ulbricht paid an undercover agent $80,000 to murder a Silk Road employee suspected of cooperating with authorities. Ulbricht is even alleged to have sent the final payment after agents sent him staged photos of the ostensibly murdered employee.[8]

> Bitcoins, for the moment at least, undoubtedly have a certain cool cachet. They do, however, have a dark side.

On Dec. 20, 2013, the Southern District U.S. Attorney's Office also announced the unsealing of an indictment charging three individuals in Virginia, Australia and Ireland with acting as administrators for Silk Road.[9] Most recently, on Jan. 26, 2014, two individuals—Robert Faiella, also known as "BTCKing," and Charles Shrem, founder and CEO of Bitinstant—were arrested and charged in the Southern District for allegedly facilitating payments for Silk Road users by selling bitcoins to them for cash. The unsealed complaint charges Shrem and Faiella with operating unlicensed money transmitting businesses, money laundering conspiracies, and failures to file suspicious activity reports (SARs).[10]

Reputation for Anonymity

Ulbricht went by the online alias Dread Pirate Roberts, a reference familiar to anyone who has seen the film The Princess Bride. In the film, the Dread Pirate Roberts was the name of a feared pirate, but the actual identity of the pirate changed as one Dread Pirate Roberts retired and another suitable candidate took his place. Presumably, Ulbricht expected the Silk Road website to continue in perpetuity with others eventually taking his place. In fact, in November 2013 a Silk Road 2 website went online with a moderator going by the name of the Dread Pirate Roberts.[11]

Perhaps Silk Road 2 and similar websites will persist despite law enforcement efforts, but if so it will not be because of bitcoins. Bitcoins have a reputation for anonymity which is misunderstood and not entirely deserved. For example, a press release from the Southern District U.S. Attorney's Office announcing the seizure of additional Silk Road bitcoins describes bitcoins as "an electronic currency that is as anonymous as cash," an assertion repeated in the civil forfeiture action.[12] This perception, although common, is incorrect.

Anonymity was never the primary goal of bitcoin. Bitcoins by design rely on the publicly available block chain to prove their legitimacy. While the identities of holders of bitcoins remain anonymous, academic studies have shown that the movements of bitcoins can be passively tracked and compared by computers over time to the point where it may be possible to associate a bitcoin with a particular identity.[13] Moreover, whenever a bitcoin comes into contact with a third party, the transaction may allow for identification of the bitcoin holder. For example, using a bank account to buy a bitcoin from a bitcoin exchange, or using a bitcoin to buy a product from a merchant, provides an opportunity to connect a bitcoin to an identity. These risks of "linking" were actually acknowledged in the original Nakamoto paper first describing bitcoins.[14]

True, bitcoins were apparently the only currency Silk Road accepted. But as an added layer of security, Silk Road was only available through the Tor network. Tor offers complete communication anonymity, or the closest thing to it on the Internet. It is a free online network that bounces every communication through multiple relays and levels of encryption, making it virtually impossible to identify the original IP address (which can reveal a computer's location) associated with the communication.[15] Interestingly, the bitcoin website actually suggests the use of Tor to increase anonymity.[16] Thus, the key to online anonymity is not so much bitcoins as it is other methods such as Tor. As set forth below, however, bitcoins do pose problems for regulators worldwide.

Challenges for Regulators

The U.S. Department of Justice has stated in various court filings that bitcoins are not inherently illegal.[17] But a report on bitcoin by the FBI Directorate of Intelligence reveals that they pose potential problems.

The report, marked “Unclassified” but “For Official Use Only,” was leaked to the media. Media outlets confirmed with the FBI that it is genuine but that the FBI was not the source of the leak.[18] The report contains a distribution list indicating that it was sent to law enforcement authorities in The United Kingdom, Australia, New Zealand and Canada.

The FBI report is not alarmist and simply points out the potential for abuse, including theft of bitcoins. But the report notes that because the bitcoin network has no central authority, it cannot perform due diligence, monitor or report suspicious transactions, follow anti-money laundering or other policies, or even receive or respond to subpoenas. The report also raises the anonymity issue, but points out that transaction comparisons and interactions with third-party payment systems provide possible solutions.

The report, however, does not anticipate certain developments relating to bitcoin anonymity that may require legislative action. Not surprisingly, enterprising programmers have devised methods to attempt to keep bitcoin ownership anonymous. The most common method is through the use of “tumblers.” The typical analogy used to explain a tumbler is 500 people each place a penny in a jar and the jar is shaken vigorously. Each person then removes a penny from the jar. Everyone has a penny but no one knows whose penny they received. Similarly, a bitcoin tumbler accepts bitcoins from people, verifies them and pools them. Each person then gets the correct amount of bitcoins back less a small fee. New bitcoin deposits are held as long as possible and the oldest bitcoins are paid out first, further minimizing the possibility of associating any deposit with any withdrawal.

A sort of arms race thus is occurring with respect to anonymity of bitcoin ownership. This arms race reveals a potential gap in international enforcement regimes. While even the Southern District U.S. Attorney concedes that bitcoins are not inherently illegal, and the U.S. central bank and merchants worldwide have begun to conclude that they are an acceptable form of payment, the United States and other countries may well need to enact new laws against bitcoin laundering. Indeed, the U.S. money laundering statutes contain terms such as “monetary instrument” and “monetary transaction” that are defined as coin or currency of the U.S. or any other country.[19] Thus, these terms arguably do not apply to bitcoins.

While even the Southern District U.S. Attorney concedes that bitcoins are not inherently illegal, and the U.S. central bank and merchants worldwide have begun to conclude that they are an acceptable form of payment, the United States and other countries may well need to enact new laws against bitcoin laundering.

The U.S. Treasury’s Financial Crimes Enforcement Network (FinCEN) has taken steps to address these sorts of regulatory gaps by releasing guidance extending FinCEN’s regulations to entities trading in virtual currencies.[20] FinCEN’s announcement, however, acknowledges that it is issued pursuant to FinCEN’s authority to administer the Bank Secrecy Act and does not affect the applicability of other laws or rules to bitcoins. A month later, the Department of Homeland security seized an account controlled by Mt. Gox, the largest bitcoin trading exchange, on the grounds that Mt. Gox did not register with FinCEN as a money transmitting business.[21] Mt. Gox responded by registering with FinCEN, which lends bitcoins a further air of legitimacy.

The Future of Bitcoin

Bitcoins thus pose fundamental challenges for regulators worldwide, but steps such as those taken by FinCEN indicate that regulators can adapt existing regulations to conform to the bitcoin phenomena. Many commentators, however, have questioned whether the whole bitcoin concept—creating something out of nothing—is inevitably doomed to fail. Bitcoins have no intrinsic value and thus questions have been raised over whether bitcoins and anything like them are simply the purest form of speculative bubble. Despite this, and notwithstanding China’s central bank, governments and businesses throughout the world appear receptive to bitcoins. Perhaps then bitcoins will survive. After all, as writer Publilius Syrus observed in the 1st century, BC, “Everything is worth what its purchaser will pay for it.”

1. See, e.g., http://bitcoinwatch.com, http://coinmarketcap.com.
2. Steven Perlberg, “Bernanke: Bitcoin ‘May Hold Long-Term Promise,’” Business Insider, Nov. 18, 2013, available at http://www.businessinsider.com/ben-bernanke-on-bitcoin-2013-11; “China Bans Financial Companies From Bitcoin Transactions,” Bloomberg, Dec. 5, 2013, available at http://www.bloomberg.com/news/2013-12-05/china-s-pboc-bans-financial-companies-from-bitcoin-transactions.html.
3. Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, bitcoin.org, available at http://bitcoin.org/bitcoin.pdf (hereinafter “Nakamoto Paper”).
4. See Nakamoto Paper, supra note 3.
5. See http://bitcoin.org/en/faq.
6. See *USA v. Ulbricht,* 13 MG 2328 (SDNY); *USA v. Ulbricht,* 13 CV 6919 (SDNY); *USA v. Ulbricht,* 13 CR 222 (D. Md.).
7. See Complaint, *USA v. Ulbricht,* 13 MG 2328 (SDNY), Complaint, Ex. A, USA v. Ulbricht, 13 CV 6919 (SDNY).
8. See Superseding Indictment, *USA v. Ulbricht,* 13 CR 222 (D. Md.).
9. *USA v. Jones*, 13 CR 950 (SDNY); Press Release, Manhattan U.S. Attorney Announces Charges Against Three Individuals In Virginia, Ireland, And Australia For Their Roles In Running The “Silk Road” Website, Dec. 20, 2013, available at http://www.justice.gov/usao/nys/pressreleases/December13/JonesetalArrestsSilkRoad2PR.php.
10. *USA v. Faiella and Shrem*, 14 MG 0164 (SDNY); see also Nathaniel Popper, “Two Executives of Bitcoin Businesses Are Arrested,” NYTimes.com, Jan. 27, 2014, available at http://dealbook.nytimes.com/2014/01/27/two-executives-of-bitcoin-businesses-are-arrested/.
11. Andy Greenberg, “‘Silk Road 2.0’ Launches, Promising A Resurrected Black Market For The Dark Web,” Forbes.com, Nov. 6, 2013, available at http://www.forbes.com/sites/andygreenberg/2013/11/06/silk-road-2-0-launches-promising-a-resurrected-black-market-for-the-dark-web.
12. Press Release, Manhattan U.S. Attorney Announces Seizure of Additional $28 Million Worth of Bitcoins Belonging to Ross William Ulbricht, Alleged Owner and Operator of “Silk Road” Website, Oct. 25, 2013, available at http://www.fbi.gov/newyork/press-releases/2013/manhattan-u.s.-attorney-announces-seizure-of-additional-28-million-worth-of-bitcoins-belonging-to-ross-william-ulbricht-alleged-owner-and-operator-of-silk-road-website (Hereinafter “SDNY Press Release 10/25/13”).
13. See, e.g., Fergal Reid and Martin Harrigan, An Analysis of Anonymity in the Bitcoin System, July 22, 2011, available at http://arxiv.org/abs/1107.4524; Sarah Meiklejohn et al., A Fistful of Bitcoins: Characterizing Payments Among Men with No Names, U.C. San Diego & George Mason Univ., Oct. 23, 2013, available at http://cseweb.ucsd.edu/~smeiklejohn/files/imc13.pdf.
14. See Nakamoto Paper, supra note 3, at ¶ 10.
15. See https://www.torproject.org/.
16. See http://bitcoin.org/en/protect-your-privacy.
17. See SDNY Press Release 10/25/13, supra note 11; Complaint, *USA v. Ulbricht,* 13 MG 2328 (SDNY), Complaint, Ex. A, *USA v. Ulbricht,* 13 CV 6919 (SDNY).
18. Kim Zetter, “FBI Fears Bitcoin’s Popularity with Criminals,” Wired.com, May 9, 2012, available at http://www.wired.com/threatlevel/2012/05/fbi-fears-bitcoin/; Report, Bitcoin Virtual Currency: Unique Features Present Distinct Challenges for Deterring Illicit Activity, FBI, Apr. 24, 2012, available at http://cryptome.org/2012/05/fbi-bitcoin.pdf.
19. 18 U.S.C. §§1956, 1957.
20. Guidance, Application of FinCEN’s Regulations to Persons Administering, Exchanging, or Using Virtual Currencies, FInCEN, March 18, 2013, available at http://fincen.gov/statutes_regs/guidance/html/FIN-2013-G001.html. One federal court has also held that bitcoins constitute both money and investments for the purposes of securities laws. See *SEC v. Shavers,* No. 13 CV 416, 2013 U.S. Dist. Lexis 110018 (E.D. Tex. Aug. 6, 2013).
21. *USA v. The Contents of one Dwolla account*, 13 MJ 01162 (D. Md.).