Bloomberg BNA

White Collar Crime Report™

BANKING

A White Collar Lawyer's Guide to Virtual Currency

BY MARCUS A. ASNER AND ALEXANDRA L. MITTER

You can't hold it in your hand or carry it in your billfold, but you soon may be able to use virtual currency to buy your morning coffee or pay your bills, just the way you now pay with cash, checks or a credit card. While some might raise their eyebrows about money they can't see or touch, virtual currencies are fast gaining credibility, making the jump from being a novelty for computer geeks or a high-tech way to launder drug money to a legitimate medium of exchange increasingly accepted by stores, rental companies and even law firms. Bitcoin ATM machines are planned for cities from Toronto to Brooklyn, and prominent venture capitalists are placing heavy bets on a wide range of companies developed around virtual currencies. Even once-skeptical regulators are starting to accept that virtual currencies are here to stay and are publicly mulling over ways to regulate—but not kill—Bitcoin and its various virtual cousins.

Marcus Asner is a litigation partner in Arnold & Porter LLP's New York office. Among other focuses, he has significant experience in the areas of virtual currencies, Internet gaming, cybercrime, data breaches and anti-money laundering. Before joining the firm, Asner served as an assistant U.S. attorney for the Southern District of New York from 2000 to 2009, where he was the chief of the Major Crimes and Computer Hacking/Intellectual Property unit from 2007 to 2009.

Alexandra Mitter is a litigation associate in Arnold & Porter LLP's New York office. She has experience in a wide range of matters, including representing clients in internal investigations and providing guidance on SEC reporting and compliance. Mitter currently represents several clients operating in the virtual currency space.

Granted, virtual currencies may seem alien and hard to get your head around, at least at first. But our guess is that white collar lawyers—both defense attorneys and prosecutors—are going to start seeing more and more folks using Bitcoin or other virtual currencies. We're going to need to adapt and understand the area, just like we previously came to accept and understand e-mail and how the Internet works and our predecessors had to learn about LUDS and MUDS and the inner workings of the telephone system.[1]

This article seeks to provide a practical introduction to the world of virtual currency for the white collar practitioner. Many of the issues are the same as in any case: You are doing an investigation or trying to defend a client, and you need to be able to find and secure evidence. The questions to ask are familiar: Where does someone leave evidence when she uses virtual currency, and how do I go about getting that evidence?

It turns out that the answers are not nearly as mysterious as one might think. To understand where to find the evidence, it pays to get some understanding about how virtual currencies work, how and why people use virtual currencies and how regulators and law enforcement have begun to treat the area. That will help point to some of the places where you should be able to find evidence and how you can use the tools already available to gather the material you need to build your case.

[1] LUD stands for ''Local Usage Detail,'' the records of incoming and outgoing phone calls to or from a particular phone number. MUD stands for ''Metro Usage Detail.''

 ISSN 1559-3185

A Virtual Currency Primer

We're still at an early stage in the history of virtual currencies, and many readers reflexively will associate virtual currency with money laundering or the illicit goods and services once famously available on the Silk Road website. But history is filled with stories of societies developing alternative ways to exchange money, often for completely legitimate reasons. While it's true, for example, that some may use hawalas to launder drug proceeds, the hawala alternative remittance system has existed in Asia as a legitimate means to transfer money since before the introduction of Western banking,[2] and many immigrants today use hawalas to transfer hard-earned, legitimate earnings back to their relatives who stayed behind.

Basic economics teaches that, where access to traditional forms of currency is scarce or traditional mechanisms of exchange are expensive, cumbersome or impractical, then cheaper, more practical alternatives will emerge. At bottom, virtual currency is another development in a long line of alternatives to traditional government-issued currency and methods of value transfer.

A key innovation of Bitcoin is that it avoids a so-called "double spending" problem without having to rely on a trusted intermediary to verify transactions.

The umbrella term ''virtual currency'' is used to talk about any number of currencies that exist only online, including Bitcoin, Ripple and Litecoin. Bitcoin, the most prominent virtual currency today, was conceptualized in a 2008 paper published by the pseudonymous ''Satoshi Nakamoto.''[3] The paper detailed a plan for an open source software through which computers around the globe have been able to facilitate the peer-to-peer transfer of currency without using a third-party intermediary such as a bank, PayPal or a hawalader. By design, only a limited number of bitcoins are potentially available (21 million) and so far, just over 12 million bitcoins are in circulation.[4] New bitcoins are released through ''miners,'' who serve a central role in the Bitcoin world. Miners use their computers to solve complex mathematical problems and get paid bitcoin in return. At the same time, the miners effectively lend their computers to the system, verifying each bitcoin transaction and running the Bitcoin infrastructure. As more computing power is added, the mathematical problems become more complex, which serves to stabilize the rate that new bitcoins can be introduced into the virtual economy.

Major Innovation. A key innovation of Bitcoin is that it avoids a so-called ''double spending'' problem without having to rely on a trusted intermediary to verify transactions. If currency is virtual—no more than a series of zeros and ones—what stops me from using $5 worth of a virtual currency to buy coffee from one shop and then using the same $5 to pay for lunch? The usual solution is to employ a trusted middleman, such as PayPal or a bank, but one problem with that approach is that the middleman naturally will take a cut of each transaction, which increases costs, eliminating an advantage of working peer-to-peer.

Bitcoin solves the double-spending problem by using a public ledger or ''blockchain.'' Each user has two ''keys,'' a public key and a private key. The public key serves as a sort of routing number, and the private key serves as a PIN. For Sally to transfer bitcoins to Paul, she must sign her transmission of funds to Paul's public key using her private key. Next, computers running Bitcoin protocol (that is, the miners' computers) will verify the transaction and publish it on the Bitcoin blockchain with a group of other transactions verified at the same time called a ''block.'' The blockchain serves as a public ledger of all bitcoin transactions from the inception of Bitcoin. Looking at Sally's public key will show the bitcoin she previously transferred to Paul. The double spending problem is solved: Sally will be unable to transfer those same bitcoins to Joe, because the computers running the Bitcoin protocol will recognize that those bitcoins already have been transferred to someone else.

Much has been made of the purported anonymity of virtual currencies, particularly the alleged anonymity provided by Liberty Reserve dollars, which played a central role in a recent prosecution (discussed further below). In reality, Bitcoin (and every virtual currency is different) falls somewhere on the spectrum between a wire transfer and an all-cash transaction. While Bitcoin transactions are publicly available online on the blockchain, the transactions are tied to an individual's public key rather than her legal name. So while it is possible to follow a bitcoin or fraction of a bitcoin from transaction to transaction, you will not know who is involved in the transaction unless you know the identity of the individual holding a particular public key.

Because virtual currency transactions take place online, the movement of virtual currency often is traceable through IP addresses, much like any other internet activity.

Nevertheless, there are ways to figure out who holds certain bitcoins and trace their transactions, much like it often is possible to trace an e-mail address to an IP address and ultimately to a particular person. The key, of course, is the Bitcoin blockchain, which is available at various websites, including http://blockchain.info. These websites offer search engines, which allow you to

[2] U.S. Financial Crime Enforcement Network, *The Hawala Alternative Remittance System and its Role in Money Laundering*, available at http://www.treasury.gov/resource-center/terrorist-illicit-finance/Documents/FinCEN-Hawala-rpt.pdf.

[3] Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System* (Oct. 31, 2008), available at http://bitcoin.org/bitcoin.pdf.

[4] See https://blockchain.info/charts/total-bitcoins.

  WCR ISSN 1559-3185

search by a variety of potentially useful categories—by public key, by block of recorded transactions, by miner, etc. If you know your client's public key (the account number), you can trace every transaction of bitcoin to or from your client.

Let's say, for example, that you learn by searching for your client's public key that he transferred 10 bitcoins to another public key on Jan. 1. You can click on that public key to see that the person to whom your client transferred bitcoin then transferred five of those bitcoin to another person the following day. You also could go backward to see the address of the person from whom your client received the bitcoin, and so on. In one recent incident, regular bitcoin users following the public ledger were able to watch a computer hacker attempt to move the proceeds of a recent bitcoin theft.[5] Researchers have found that they can classify and identify users simply by analyzing patterns in the Bitcoin blockchain.[6]

Because virtual currency transactions take place online, the movement of virtual currency often is traceable through IP addresses, much like any other internet activity. Moreover, as discussed below, as virtual currency exchangers (companies exchanging virtual currency for traditional currency) continue to implement well-established ''know your customer'' rules and other anti-money laundering provisions, law enforcement should be able to use the public keys to trace transactions to real people just by sending out a grand jury subpoena.

Legitimate Advantages of Virtual Currency

Critics complain that virtual currencies are anonymous havens for money laundering and other criminal enterprises, and it's certainly true that virtual currencies have been used by criminals. That said, criminals also rely on cash, the mainstream banking system, auction houses and countless other vehicles and mechanisms to launder money. Moreover, as noted, currencies such as Bitcoin are not nearly as anonymous as one might think. As it has in countless other areas relied upon for money laundering, law enforcement is getting increasingly sophisticated at rooting out and halting criminal uses of virtual currencies, as the Liberty Reserve and Silk Road cases suggest.

More fundamentally, virtual currencies may well provide a number of profound advantages, and these features recently have led to a boom in virtual currency-focused startups. Clients or potential clients—both companies and individuals—increasingly are using virtual currency, accepting it as payment at their places of business and developing businesses to invest in or service the virtual currency market. White collar practitioners need to understand the legitimate uses of virtual currency and take care not to dismiss the presence of virtual currency as necessarily a marker of illegality.

Virtual currencies such as Bitcoin can provide a relatively frictionless way to transfer money from one person or entity to another. Without third-party intermediaries such as banks, credit card companies and global money transfer services, the costs of transactions can be much lower and faster. This potentially may lead to several pro-competitive, pro-consumer results.

First, lower cost and faster transactions are attractive to individuals and businesses. Transaction fees associated with Bitcoin, for example, often are less than 1 percent. Virtual currencies like Bitcoin provide businesses with a way to avoid the higher transaction fees charged by mainstream credit card companies. This can mean greater profit margins for the business, or the company can choose to pass those savings along to consumers, giving it a competitive edge in the marketplace. Similarly, using virtual currency, individuals can make low-cost remittances to friends or relatives in other countries, avoiding the much higher transactions fees (sometimes nearly 10 percent) associated with companies such as Western Union or MoneyGram. The lower costs and increased speed provided by virtual currency, in turn, should place competitive pressure on traditional financial institutions.

Second, virtual currencies may provide users with ways to hedge against inflation and currency fluctuations. This can be done on an individual or institutional scale, and several bitcoin-tied funds already have sprung up, including Exante Ltd.'s Bitcoin Fund, SecondMarket's Bitcoin Investment Trust and an exchange traded fund founded by the Winklevoss twins. That Bitcoin and other virtual currencies are untethered to a government-issued currency also could help people living in countries with devalued currency or frozen capital markets.

The Regulatory Landscape Of Virtual Currency Evolves

The virtual currency landscape is rapidly changing, and white collar practitioners should understand how the developments in state and federal regulation of virtual currency and the prosecution of virtual currency-related crimes will affect their practice. Regulators around the globe are getting involved. Regulatory action has varied widely—from China, which warned financial institutions not to accept bitcoin or provide services for individuals or business who do,[7] to Germany, which has a thriving bitcoin economy.[8] Thus far, actions taken by U.S. lawmakers and regulators suggest that virtual currencies will not be regulated out of existence.[9] In many instances, U.S. regulation also may

[5] Jim Edwards, *Two Guys On Reddit Are Chasing A Thief Who Has $220 Million In Bitcoins*, BUSINESS INSIDER (Dec. 4, 2013), available at http://www.businessinsider.com/220-million-sheep-marketplace-bitcoin-theft-chase-2013-12.

[6] See, e.g., Sarah Meiklejohn et al., *A Fistful of Bitcoins: Characterizing Payments Among Men with No Names*, presented at the 2013 Internet Measurement Conference (Oct. 23-25, 2013) in Barcelona, Spain, available at http://cseweb.ucsd.edu/~smeiklejohn/files/imc13.pdf; Elli Androulaki et al., *Evaluating User Privacy in Bitcoin*, IACR Cryptology ePrint Archive 596 (2012), http://fc13.ifca.ai/proc/1-3.pdf.

[7] *China Bans Financial Companies From Bitcoin Transactions*, Bloomberg News (Dec. 5, 2013), available at http://www.bloomberg.com/news/2013-12-05/china-s-pboc-bans-financial-companies-from-bitcoin-transactions.html.

[8] Matt Clinch, *Bitcoin recognized by Germany as 'private money,'* CNBC (Aug. 19, 2013), available at http://www.cnbc.com/id/100971898.

[9] In November, the Senate Homeland Security and Governmental Affairs Committee and two subcommittees of the Senate Committee on Banking, Housing and Urban Affairs held two days of hearings on virtual currency, with testimony from FinCEN Director Jennifer Shasky Calvery and Edward W. Lowery III, the Special Agent in Charge of the Criminal Investigative Division of the U.S. Secret Service, among others.

overlap criminal enforcement, and practitioners must take care to understand where in the regulatory landscape their client fits.

In March 2013, the U.S. Treasury Department's Financial Crimes Enforcement Network, or FinCEN, issued guidance on application of the Bank Secrecy Act to virtual currency.[10] FinCEN divides the virtual currency world into three groups: administrators, exchangers and users:

> (1) An ''administrator'' issues virtual currency and ''has the authority to redeem (withdraw from circulation) such virtual currency.''
>
> (2) An ''exchanger'' is involved in the exchange of virtual currency for traditional, hard currency or another virtual currency.
>
> (3) A ''user'' ''obtains convertible virtual currency and uses it to purchase real or virtual goods or services,'' whether by purchasing, earning or digital mining. Companies receiving virtual currency as payments for goods or services qualify as users.[11]

Understanding the distinction between the three groups will be critical in many cases. While virtual currency users are not regulated under the FinCEN guidance, virtual currency administrators and exchangers are considered ''money transmitters'' subject to FinCEN oversight. Once categorized as a money transmitter, a virtual currency administrator or exchanger must register as a money services business and must comply with FinCEN's regulations in the same way a money transmitter dealing in traditional currency does. This includes compliance with the Bank Secrecy Act and its anti-money laundering and know-your-customer provisions. While the failure to register as a money services business is punishable by civil penalty, operating as such without registering is a criminal offense.[12]

Perhaps because the virtual currency is new and still evolving, FinCEN appears to have been giving certain virtual currency businesses a short-term reprieve. In January 2014, FinCEN reportedly sent letters to ''roughly a dozen'' companies dealing in bitcoin, notifying them that they may be considered money transmitters under FinCEN's March 2013 guidance.[13] The letters seem to give the companies an opportunity to come into compliance before FinCEN initiates any regulatory or criminal action against them.

This may reflect a change in the government's attitude toward virtual currencies. In May 2013, shortly after FinCEN issued its guidance, the U.S. Department of Homeland Security took action against Mt. Gox, a Japanese company and Bitcoin's largest exchanger at the time, for its alleged failure to register with FinCEN as a money transmitting service.[14] Homeland Security secured warrants and seized the contents of three accounts, totaling more than $5 million—including Mt. Gox's account with an Iowa payment processor where Bitcoin customers deposited traditional currency to buy bitcoins. While the Mt. Gox account seizures were purely a regulatory action, they underscore the need for white collar practitioners to stay on top of the regulatory changes in this rapidly evolving environment.

We soon may see more virtual currency-targeted action from other regulators, such as the Internal Revenue Service and the Commodity Futures Trading Commission or state regulatory agencies. The New York Department of Financial Services, for example, has jumped into the fray, holding two days of highly publicized hearings at the end of January.

Criminal Actions Against Virtual Currency Companies

Criminal law enforcement also is actively policing the world of virtual currency. This recently resulted in several high-profile criminal actions in the virtual currency sphere. As we might have expected, the techniques used to develop and prosecute cases involving virtual currency mirror the techniques used to investigate and prosecute other crimes. Law enforcement built the cases using subpoenas, undercover agents, phone and e-mail pen registers and wiretaps.

In May 2013, the U.S. Attorney's Office for the Southern District of New York announced criminal charges against Liberty Reserve, a virtual currency service selling ''LR dollars,'' and seven of its principals and employees.[15] The indictment alleges that Liberty Reserve's founders specifically designed the company and the currency to provide anonymity ''to help criminals conduct illegal transactions and launder the proceeds of their crimes.'' To distance itself from any of its customers' identifying information, Liberty Reserve allegedly refused to exchange currency for LR dollars itself and offered a ''privacy fee'' to further obscure its users' identities. To confirm that Liberty Reserve made no effort to verify its users' identities, an undercover agent

---

Available at http://www.hsgac.senate.gov/hearings/beyond-silk-road-potential-risks-threats-and-promises-of-virtual-currencies and at http://www.banking.senate.gov/public/index.cfm?FuseAction=Hearings.Hearing&Hearing_ID=955322cc-d648-4a00-a41f-c23be8ff4cad. On Jan. 28-29, the New York State Department of Financial Services held hearings on virtual currency as well. Available at http://www.totalwebcasting.com/view/?id=nysdfs.

[10] Department of the Treasury, Financial Crimes Enforcement Network, *Application of FinCEN's Regulations to Persons Administering, Exchanging or Using Virtual Currencies*, Fin-2013-G001 (March 18, 2013).

[11] The text of FinCEN Director Shasky Calvery's speech at the April 16, 2013, National Cyber-Forensics Training Alliance conference is available at http://fincen.gov/news_room/speech/pdf/20130416.pdf.

[12] 18 U.S.C. § 1960; 31 CFR § 1022.300 et seq.; 31 CFR § 1022.400.

[13] Brett Wolf, *U.S. Treasury cautions Bitcoin businesses on compliance duties, advocate cites 'chilling effect,'* Reuters (Jan. 6, 2014), available at http://blogs.reuters.com/financial-regulatory-forum/2014/01/06/u-s-treasury-cautions-bitcoin-businesses-on-compliance-duties-advocate-cites-chilling-effect.

[14] While Mt. Gox had been Bitcoin's largest exchanger, the company recently filed for bankruptcy, acknowledging that approximately 750,000 bitcoins were stolen by hackers. Despite our general enthusiasm for Bitcoin, it is important for potential users or investors to remember that it remains a developing technology with a rapidly changing landscape. See Grace Huang & Carter Dougherty, *Mt. Gox Exchange Files for Bankruptcy*, Bloomberg News (Feb. 28, 2014), available at http://www.bloomberg.com/news/2014-02-28/mt-gox-exchange-files-for-bankruptcy.html.

[15] *United States v. Liberty Reserve et al.*, No. 13-cr-00368 (S.D.N.Y.). Interestingly, the founders of Liberty Reserve also were involved in the E-Gold Ltd. scheme, operating an intermediary called Gold Age Inc., for which they were convicted in 2006. See *United States v. E-Gold Ltd.*, No. CR-07-109 (D.D.C. 2008).

  WCR ISSN 1559-3185

signed up for an account as ''Joe Bogus'' living in ''Completely Made Up City, New York.''[16]

While its blockchain or public ledger approach likely will make Bitcoin much less attractive to the criminal underworld, criminals can and allegedly have used bitcoins for criminal schemes. Silk Road—a website that was accessible only through the encrypted dark Internet—allegedly was ''the most sophisticated and extensive criminal marketplace on the Internet today.''[17] The merchants on Silk Road allegedly accepted exclusively bitcoin for the drugs, counterfeit identification documents and computer hacking services offered. In September, the alleged owner of the website, Ross Ulbricht, was arrested and charged with conspiracy to violate narcotics trafficking, computer hacking and antimoney laundering laws.[18] Several others purportedly associated with Silk Road were arrested in the ensuing months.[19] Law enforcement built their case over nearly two years using old-fashioned detective work. Among other methods, undercover agents purchased illegal drugs on Silk Road and posed as hit men solicited by the website's alleged owner.[20]

Conclusions

The virtual currency world—and regulators' and law enforcement's reaction to it—is rapidly changing. Virtual currencies may sound like the stuff of science fiction, but when you peel through the layers, many of the concepts in fact are familiar from other contexts. In investigating or defending matters involving virtual currencies, you still will be able to use many long-familiar techniques to find evidence—as long as you learn how virtual currencies work and where to look for the evidence you will need.

---

[16] U.S. Attorney's Office, Southern District of New York, press release, *Manhattan U.S. Attorney Announces Charges Against Liberty Reserve, One of World's Largest Digital Currency Companies, And Seven of Its Principals and Employees For Allegedly Running A $6 Billion Money Laundering Scheme* (May 28, 2013), available at http://www.justice.gov/usao/nys/pressreleases/May13/LibertyReservePR.php.

[17] *United States v. Ulbricht*, No. 13-civ-6919 (S.D.N.Y.)

[18] *United States v. Ulbricht*, No. 13-civ-6919 (S.D.N.Y.); *United States v. Ulbricht*, No. 13-mag-2328 (S.D.N.Y.).

[19] *United States v. Jones*, No. 13-cr-950 (S.D.N.Y); *United States v. Faiella*, No. 14-mag-0164 (S.D.N.Y.); National Crime Agency, press release, *NCA arrests silk road suspects* (Oct. 8, 2013), available at http://www.nationalcrimeagency.gov.uk/news/198-nca-arrests-silk-road-suspects.

[20] Christie Smythe and Greg Farrell, *Silk Road Cyber-Bazaar Suspect Denied Bail in New York*, Bloomberg News (Nov. 22, 2013), available at http://www.bloomberg.com/news/2013-11-21/silk-road-online-drug-market-suspect-ulbricht-denied-bail-1-.html.