For the Defense

New Mexico
CRIMINAL DEFENSE LAWYERS ASSOCIATION

Summer 2015 Volume XIX, Issue 2

Inside This Issue:

What Criminal Defense Attorneys Need to Know About Bitcoin.....1

President's Message.....5

Breathaliars & Other Fraud Machines.....7

Roundhouse Round-Up.....10

Tenth Circuit Update.....12

Tenth Circuit Spotlight.....13

News from NMCDLA Regional Directors.....15

State Case Law Update.....16

Bad Cop, No Donut.....20

Helping Your §1326 Clients Avoid Deportation.....22

Reel to Real.....25

Mission Statement:
The New Mexico Criminal Defense Lawyers Association provides support, education and training for attorneys who represent persons accused of crime. NMCDLA also advocates fair and effective criminal justice in the courts, the legislature and in the community.

What Criminal Defense Attorneys Need to Know About Bitcoin

Beth Mohr, Managing Partner, McHard Accounting Consulting LLC, Albuquerque

What is Bitcoin, and how might it impact your practice as a criminal defense attorney? In this article we'll look at Bitcoin, what it is and how it works; we'll discuss how bitcoins are used, both for illicit purposes, as well as for legal and legitimate business purposes. We will also examine how you might encounter bitcoins; discover ways to determine that bitcoins may be a factor in your case; discuss the difficulties (and the ironic ease) with which bitcoins can be traced as assets through transactions; and vectors to consider when your case drops into the virtual world. *Disclaimer: This article is not intended to be a highly technical treatise about Bitcoin, but rather to offer a general understanding of virtual currency for busy defense attorneys.* Please visit each of the websites listed to find more in-depth information about technical subjects. (Bitcoin referring to the currency or network is capitalized; bitcoins, referring to coins held as currency, is not capitalized.)

There are many different digital currencies, also known as Crypto-currencies, with names like Darkcoin, Litecoin, Primecoin and Dogecoin. This article discusses only Bitcoin, which is the most mainstream and widely recognized virtual currency. Bitcoins are accepted at big retailers like Amazon, Target, Sears, and by other companies such as the Chicago Sun Times and Virgin Airlines, as well as many lesser known companies. Because of the "*pseudonymous*" - almost anonymous - online nature of Bitcoin, and the fact that it has been exempt from most regulation since its inception in 2009, it is also used to make online purchases of drugs, stolen goods, child pornography, murder for hire, terrorist financing and other criminal enterprises.

Figure 1 - Minted Bitcoins

Bitcoin is a virtual currency, basically digital money, exchanged in a decentralized, peer-to-peer payment network that operates without the aid or cost of a third party, such as a bank or credit card company to hold and transfer virtual currency, and without the oversight of regulatory

bodies or basic fraud protections. It is extremely volatile, and also acts like a stock, in that the value changes in accordance with the market. People invest in Bitcoin, betting that the value will go up over time; however, nothing guarantees it will have any future value at all. The U.S. District Court of the Eastern District of Texas held in August 2013 that investments in Bitcoin or investments purchased with bitcoins are securities *(SEC v. Shavers*, No. 4:13-CV-416).

You can see the value of one Bitcoin anytime at http://bitcoin.info/. Bitcoins have been worth as little as $10 in November 2012, to over $1,000 a year later, but as of this writing, one Bitcoin is worth $238.83 in U.S. dollars, and has been holding steady in that price range for a few months. The volatility of Bitcoin is one of the things that make it unique as a currency.

Users acquire bitcoins by purchasing them at a Bitcoin exchange, exchanging them online or in person, or by accepting them as payment for goods or services. You can see who buys or sells Bitcoin in your area here: https://localbitcoins.com/, but obviously there are inherent risks in meeting personally with strangers to conduct financial transactions. In fact, "Bitcoin robbery" is becoming very common, particularly in New York (http://observer.com/2015/02/bitcoin-crime-wave-breaks-out-in-nyc). Typically, people meet on Craigslist or a Bitcoin networking site and agree to meet to exchange cash for Bitcoins. Sometimes, instead of making an exchange, one person forces the other to transfer their bitcoin, and typically makes off with any cash, as well. Once transferred, even when stolen, Bitcoins are gone forever, just like lost or stolen cash.

Figure 2 – A Bitcoin Wallet with Public Key

Bitcoins can also be obtained by "mining" them. Bitcoin "miners" use computers to competitively solve special math problems, and the first computer to solve a particular problem is issued bitcoins in exchange for this work. The Bitcoin network is using this computer power to securely function as these problems are being solved, so the Bitcoin is paid as reward for miners doing this work. As Bitcoin's value changes and more bitcoins are issued, the computer problems get harder or easier to solve. It is believed that this function was ostensibly designed to take the place of government oversight to stabilize monetary value, as well as to ensure that the supply of bitcoins never runs out. However, it is predicted that Bitcoins will indeed all be mined by 2140, and it remains to be seen what will happen to Bitcoin at that point (See http://www.bitcoinmining.com/ for more information on how bitcoins are mined).

Bitcoins are stored in a "virtual wallet," like the one depicted in Figure 2, and one user can send coins to another user by using their "public key," much like anyone who has your bank account number can deposit money into your account using the night deposit drop at your bank. Unlike credit card charges, which can be reversed, or checks which can be stopped by the bank, an exchange of bitcoins is irreversible. Users can also transfer bitcoins using a program on their smart phone with QR codes, and transfer value with a single click (QR codes are the square barcodes like the one depicted in Figure 2). Users tend to print their virtual wallets as a backup, or have them stored on their computer, which then makes them vulnerable to theft as well as seizure by law enforcement.

While Bitcoin is completely open to public view, it is also somewhat anonymous; more accurately, it is *pseudonymous*. Bitcoin users have a pseudonym linked to their public wallet, rather than a real name, and so as long as their real name is never linked to their pseudonym, they are truly anonymous. However, keeping that pseudonym separated from one's real identity

is extremely difficult, and once the linkage is made between real identity and the public key, everything is open to public view.

Government and regulatory agencies have struggled to define and deal with Bitcoin, and fit it into regulations not designed to deal with virtual currency. For some time, Bitcoin was completely unregulated, but recently the Financial Crimes Enforcement Network (FinCEN) has ruled that while Bitcoin users are not subject to regulation generally, businesses who exchange and convert bitcoins to real currency and some "virtual wallet" providers are considered a Money Service Business (MSB) under the Bank Secrecy Act, and must follow a host of Anti-Money Laundering (AML) regulations including the filing of Currency Transaction Reports (CTRs). To see FinCEN's recent guidance regarding trading of virtual currency, visit: http://www.fincen.gov/news_room/rp/rulings/html/FIN-2014-R011.html

The decentralized nature of Bitcoin makes it more difficult for law enforcement to obtain information – in part because there is no central server or financial institution upon which to serve a search warrant or subpoena. However, difficult does not mean impossible, and law enforcement has been successful at connecting Bitcoin transactions to corresponding unlawful activity. The most significant example of this is *USA v. Ross William Ulbicht aka: Dread Pirate Roberts* (Southern District of NY 14-CR-68 (KBF) July 9, 2014).

Ironically, a DEA Agent and a Secret Service agent who worked on the *Dread Pirate Roberts* case allegedly transferred over $800,000 of the seized Bitcoin using various accounts they had previously opened, but were caught using the same tools and techniques that brought down the Silk Road drug dealers from which the coins were originally seized (http://www.huffingtonpost.com/2015/03/30/dea-agent-silk-road-secret-service_n_6970758.html).

Although Bitcoin is used to make legitimate purchases, it is controversial because of the way it can also be used for illegal enterprises. Sites on the internet known as the "Dark Web" or the "Deep Web" can be hubs of criminal activity, and these can only be accessed through the "Tor" browser. Tor stands for "The Onion Router," likening layers of an onion to the way in which Tor makes web surfing anonymous by bouncing internet connections through a network of unrelated computers all over the world. You can learn more about Tor and download it for free at https://www.torproject.org/. Just like Bitcoin itself, Tor can be used for a variety of purposes, from protecting your online privacy to defeating censorship in countries where free speech is disallowed, or for other purposes, such as making online drug purchases in a way that is difficult (but not impossible) for law enforcement agents to trace.

Bitcoin is completely open to public inspection, with every transaction visible on the "Blockchain," a permanent public ledger that anyone with internet access can freely download and review. Visit https://blockchain.info/ to watch transactions worth a few dollars to millions of dollars as users from all over the world buy, sell or exchange bitcoins. You can follow a person's public key code from their current transaction back to their very first transaction of either mining or purchasing their very first Bitcoin. You don't know what they're purchasing, but you can see those purchases happening in real time, and trace them back. This also means that once law enforcement makes the connection between a user and their public key, every Bitcoin transaction made by that key can be traced to the beginning of Bitcoin's existence.

While Tor is extremely effective at masking the real ISP address for computer browsing (and thus the user) to a computer and a physical place, there are always places where the virtual

world and physical world touch. For example, drugs are sold over the Dark Web for bitcoins, and users give buyers and sellers a rating, not unlike eBay, but eventually the drugs must be shipped to a physical address, and thus buyer and seller are physically connected through FedEx or a similar shipper. Once law enforcement has identified one side of the transaction, the shipper can be served with a search warrant and the seller and other customers located.

There are many other avenues for those linkages to be made. When a user signs up for a Bitcoin wallet, they must use an email address, and few email addresses are truly anonymous. Even free anonymous email providers like Hushmail.com and disposable email boxes from Hidemyass.com will accept a subpoena or search warrant, and if a user has signed in from a browser other than Tor, even once, their physical location will be forever linked with that email. Other anonymous emails request a credit card for payment, which can be traced back to the owner.

Laundering money with Bitcoin isn't as easy as it sounds. Since Bitcoin transactions can be traced back through the Blockchain ledger, in order for Bitcoins to be separated from the identity of their owners, users pay a fee to run their bitcoins through a "tumbler", where their coins are mixed with the coins of others and returned in a way that makes them difficult to trace. While this is effective for small numbers of bitcoins, trying to tumble larger amounts mean that some of the original bitcoins invariably return to their original owner, and are eminently traceable; coins returned to their original owner are considered tainted and the percentage of linked coins is referred to as "taint."

Eventually, users will wish to spend their bitcoins or convert them to government-backed currency, and when they do, they risk having their bitcoins linked to them, thus exposing every transaction they've ever made. For example, a user who purchases drugs online and also makes a Bitcoin purchase from Overstock.com with the same wallet has exposed his or her information. Even if they have transferred coins from one wallet to another, each of those transactions can be traced back to the original wallet or mining operation. Law enforcement is becoming more adept at tracing these bitcoins, and new programs are being developed to help them efficiently read the ledger and trace such transactions.

A few lawyers accept Bitcoin for payment of services in a flat-fee case or for services already rendered; even fewer will consider accepting Bitcoin into a retainer account. Dealing with bitcoins and IOLTA accounting seems problematic, at best. There are also concerns that Bitcoin paid to defense attorneys will be clawed-back by the government if the Bitcoin is determined to be the proceeds of ill-gotten gain. As with all payments where claw-back is a concern, attorneys should consider getting assurance that the prosecutor has no plans to go after fees, or have a forensic accountant evaluate the funds as legitimate source income prior to accepting them.

A few banks allow Bitcoin exchanges directly into or out of a bank account, but most do not, having been scared away by the bad reputation Bitcoin acquired concerning potential money laundering. When tracing Bitcoin into or out of a bank account, expect to see the bank using the symbol "Bt" or similar, indicating a transaction to purchase or redeem Bitcoin.

Generally, merchants accepting Bitcoin use a third-party vendor, not unlike a credit card merchant account, to process transactions. Third-party vendors such as the Coinbase service do this free of charge (https://developers.coinbase.com/docs/merchants). Many

merchants who accept Bitcoin choose to avoid the volatility of Bitcoin by accepting it and immediately exchanging the accepted Bitcoin into U.S. Dollars; service providers do this for a fee of about 3%, similar to credit card merchant fees. When looking for payments from Bitcoin exchange outlets, look for the name of the vendor on the bank statement.

Ultimately, Bitcoin is very similar to cash, and yet lives only in the virtual world. Bitcoin is no more or less of a mystery than what happens to your money when the bank stores monetary value as computer code.

Beth can be contacted at bmohr@theMcHardfirm.com.

President's Message

In June, I ended my term as your President. It has been an incredible honor and joy to be able to work with all of you, plan the goals for our organization, and see them as they come to fruition. In late 2013, at the Board Retreat, we came up with several goals. First, we wanted to grow our membership and expand our reach to the four corners of our state, welcoming all attorneys in our state who practice criminal defense. We presented CLEs and had social events in Las Vegas, Roswell, Santa Fe, and Durango, Colorado. In Durango we welcomed practitioners of Indian law, and partnered with the Colorado Criminal Defense Bar. This was a