© Parilov | stock.adobe.com

Understanding Bitcoin in Criminal Defense Cases

There is nothing mysterious about Bitcoin, and a criminal defense lawyer may run across it in various types of cases: a tax evasion prosecution involving Bitcoin, a case in which an individual allegedly used Bitcoin to buy or sell illegal goods or services, a money laundering investigation involving Bitcoin, or a case in which the client allegedly committed a street robbery involving cash and Bitcoin. Although a few prosecutors still think that Bitcoin is inherently criminal, the real-world use of Bitcoin readily proves otherwise. Bitcoin can be confusing as a concept and in real-world use, but it does not have to be.

What Is Bitcoin?

What is cryptocurrency, and specifically, what is Bitcoin? Why is it worth anything at all, never mind that it was worth upwards of $50,000 per bitcoin in early 2021 and is still over $40,000 per bitcoin? This article discusses Bitcoin the network, as well as bitcoin the cryptocurrency, what bitcoins are, and why they have value. Also, there will be a discussion of the ways that Bitcoin intersects the real world, how that translates into criminal cases, and how criminal defense attorneys will likely encounter bitcoins. Finally, the article will discuss how recent legislation and an uptick of enforcement by the IRS over "massive underreporting of income" from Bitcoin transactions, among other concerns, will mean that lawyers see Bitcoin involved in many more criminal defense cases in the future. This article will not be a technical treatise on the blockchain and public ledger, but rather a nuts-and-bolts discussion of cryptocurrency.[1]

Bitcoin is cryptocurrency, meaning that it is a digital store of value in which encryption techniques are used to regulate the generation of "coins" as well as to verify the transfer of funds, operating independently of a central bank, and without the involvement of any government in the issuance of the currency. Bitcoin is actually two separate and distinct things. Bitcoin the network is a decentralized peer-to-peer (P2P) payment network that does not require a third party, such as a bank, to hold or transfer virtual currency. While Bitcoin is a network, bitcoins are individual units of virtual currency that may be "mined," purchased, traded for goods and services, purchased with or exchanged for fiat currency (U.S. dollars, for example), and held as an investment. (Bitcoin, referring to the network, is capitalized; bitcoins, referring to coins held as currency, is not capitalized.)

Bitcoins are stored in a "virtual wallet," and one user can send bitcoins to another user by using their "public key," much like anyone who has a bank account number can deposit money into that account. Users can also transfer bitcoins using a program on a smartphone with QR codes, and transfer value with a single click. Users may print their virtual wallets as a backup or have them stored on their computer, which makes them vulnerable to theft as well as seizure by law enforcement.

BY BETH A. MOHR

The U.S. government has had a little trouble defining Bitcoin for the purposes of regulation. Bitcoin was unregulated from its inception in 2009 until 2013, as regulators began to grapple with it. The Anti-Money Laundering and Corporate Transparency Act of 2020 defines all cryptocurrencies and digital currencies as "value that substitutes for currency or funds" and thus is considered legal tender by FinCEN. Meanwhile, the SEC says Bitcoin is a security, and the CFTC (Commodities Futures Trading Commission) says Bitcoin is a commodity. The IRS currently defines Bitcoin as property, but it is hinting that its definition might soon more closely track that of FinCEN so that Bitcoin wallet accounts would fall under the IRS' FBAR (Foreign Bank and Financial Accounts) rules for the purposes of reporting and taxation. This is relevant because the IRS has identified many Bitcoin owners who are U.S. taxpayers.

There are hundreds of other cryptocurrencies in addition to Bitcoin, including Ethereum, Dogecoin (pronounced doggie coin), and Litecoin. Each hopes to be the next Bitcoin, creating its own equivalent of the "Bitcoin Billionaire." There are also digital currencies that are not cryptocurrencies, such as the SandDollar, a digital currency issued by the government of the Bahamas, which is directly tied to the Bahamian dollar. Many other governments, including Australia, are looking into issuing digital currencies because it solves several problems created by the production and circulation of cash, especially in rural areas.

So why is Bitcoin worth anything at all, and why would each bitcoin be worth $50,000 or more? The answer is the same as the answer to this question: "Why is the U.S. dollar worth anything?" The answer is: The Network Effect. The United States first abandoned the gold standard in 1933 as part of efforts to pull the country out of the Great Depression. The price of gold was artificially held at $35 an ounce until 1971, when President Nixon announced that the United States would no longer convert gold to dollars at a fixed value. Thus, the U.S. dollar is only worth more than the paper it is printed on because people deem it to have value – that's the Network Effect. Bitcoins have value because people deem them to have value. The value of Bitcoin shot up from a few dollars to over $50,000 in a few short years, buoyed recently by huge corporate investments.

Similar but Different

Everyone already uses virtual currency every day. The bank does not have a box of cash stored in its vault with each customer's name on it; the bank stores the value of each account in little zeroes and ones in a computer. When customers use their credit or debit cards, wire transfer funds, or even write a check, that value is exchanged digitally between the customer's bank and the merchant's bank. The majority of people in the United States do not carry cash anymore, and with the advent of the COVID-19 pandemic and concerns over passing around objects that might carry the virus, using cash has become even less popular.

In some ways, though, Bitcoin is like cash: Once stolen, it is gone forever; transactions cannot be reversed or retrieved; and there are no fraud protections. Cash is fairly anonymous in that it is difficult to trace to a particular individual. Cash has been favored by criminal enterprise for all of these reasons, so it makes sense that individuals with criminal intent would seize on Bitcoin for some of these same reasons.

In other ways, Bitcoin is like a credit or debit card. Transactions take place in the virtual world, the exchange may be managed by a third party for a fee, value can easily be transferred around, payments can be made using a phone app or virtual wallet, and cash can be deposited or withdrawn using a Bitcoin ATM.

The volatility of Bitcoin makes it act like a stock and is one thing that dramatically differentiates it from government-backed fiat currency, like the U.S. dollar. Like a stock, people purchase Bitcoin for speculation on its future value. In fact, certain companies like MicroStrategy ($MSTR) have invested so heavily in Bitcoin that people are buying that stock as a proxy for directly investing in Bitcoin, thus essentially turning MicroStrategy into a Bitcoin mutual fund. Tesla ($TSLA) has invested heavily as well, recently reporting $100 million dollars, or nearly a quarter of its profits directly attributable to the purchase and sale of Bitcoin. The market capitalization of Bitcoin is over $1 trillion, so it is not going away anytime soon, regardless of definition or regulation.

Even though Bitcoin shares some attributes with cash, credit cards, and stocks, it is also completely unique, like nothing before it. Bitcoin can be "mined" by individuals or corporations, who essentially do the work of the peer-to-peer network by solving cryptography problems in exchange for bitcoins (or fractions of bitcoins). Also unique to Bitcoin is the online ledger, which makes the details of each and every Bitcoin transaction available to anyone, anytime, anywhere. In fact, anyone can watch transactions happening live.[2] Bitcoin can be stored in networked wallets, with Coinbase being the largest wallet provider, or offline in a printed paper wallet (that if lost, is irretrievably gone).

Bitcoin and Defense Lawyers

Where is criminal defense counsel likely to see Bitcoin in criminal defense cases? Bitcoin is involved in crimes from the extremely low-tech to the extremely high-tech, and everywhere in between. Bitcoin robberies are occurring in all major cities and are spreading to rural areas as well. Those who wish to buy or sell Bitcoins can do so from third parties, but those are treated like money service businesses (MSBs) for the purposes of regulation, and those third parties now perform due diligence on their customers, similar to opening a bank account. Thus, if people want to buy Bitcoin with cash, they can reach out to those individuals who wish to sell Bitcoin via websites that match buyers and sellers, who set their own exchange rate. LocalBitcoins, a person-to-person bitcoin trading site, is the most popular of these services.[3] The problem with carrying large amounts of cash to meet a stranger is obvious, and it is no surprise that sometime those buyers instead become robbery victims who lose their cash, and sometimes their bitcoin, as well.

Bitcoin has also been used to buy and sell illegal drugs, child pornography, murder-for-hire, and has been a preferred medium of exchange for alleged criminals via dark web websites like the Silk Road. Some of these crimes are identified via software and research of the public ledger, but most are solved due to the intersection between Bitcoin in the virtual world and the physical world. Drugs can be bought via the dark web with Bitcoin, but the drugs have to be physically shipped and delivered to customers in the real world. Once law enforcement discovers the FedEx account used for the drug deliveries, all the customer's and seller's information become readily accessible to investigators.

Bitcoin is pseudonymous, which is to say it is almost, but not quite, anonymous. Bitcoin physically touches the real-world individual and the individual's identity via email, credit card transactions, shipment of goods, and delivery of services. Very few alleged criminals have the discipline to keep their Bitcoin transactions completely anonymous, and it inevitably can be traced back to them. Even one single usage in the real world irrevocably links the individual to the public blockchain, where all that person's other transactions become traceable to each other and to that individual. Federal agencies have technology and consultants who are quite adept at tracing Bitcoin ownership and usage to individuals, and they have the ability to determine which users are U.S. citizens. This ability becomes important in tax cases involving Bitcoin.

The IRS has served a series of John Doe summonses on the largest wallet holding companies, and it has done so for several years in a row. Thus, the IRS now knows the identity and value held by many, if not most, U.S. citizens who have Bitcoin valued at over $20,000. The IRS recently sent a "soft" letter to individual taxpayers who were identified in the summonses. The letter suggests that the taxpayers might want to restate their taxes for prior years since they forgot to mention the Bitcoin. Anyone receiving that letter who failed to restate his or her taxes to include taxable Bitcoin transactions should anticipate hearing from the IRS in the near future and should plan on seeing that letter as an exhibit at trial.

Software, consultants, and John Doe summonses aside, many Bitcoin cases involve more old-school investigation than anyone in law enforcement might wish to admit. The operator of the Silk Road drug website was only successfully prosecuted[4] because while he sat in a public library using the internet, one FBI agent distracted him and another agent literally grabbed his computer off the table and ran away with it, while it was open and turned on. Bitcoin frequently becomes involved in a criminal defense case as an artifact of an investigation into real-world crime rather than being the starting point for an investigation.

A few lawyers accept Bitcoin for payment of services in a flat-fee case or for services already rendered, but even fewer will consider accepting Bitcoin into a retainer account. Dealing with bitcoins and IOLTA accounting is 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 having a forensic accountant evaluate the funds as legitimate source income prior to accepting them.

Bitcoin is not difficult to understand or use. However, criminal defense counsel may find it helpful to hire a consulting or testifying expert in Bitcoin cases to help with the understanding of the case or to assist the defense team in educating the judge and jury about Bitcoin. Bitcoin has a stigma in the minds of some jurors and judges, and an expert may be able to help dispel that notion. Ultimately, Bitcoin is just another currency, and its involvement in a criminal defense case is not that much different than any other currency allegedly involved in a crime.

Notes

1. This article is neither tax advice nor investment advice, and nothing herein should be considered as such.

2. Watch real-time transactions at https://www.blockchain.com/explorer.

3. https://localbitcoins.com/buy-bitcoins-online/us/united-states/cash-deposit.

4. The Silk Road case is *United States v. Ross William Ulbicht a/k/a Dread Pirate Roberts*, 14-CR-68 (KBF), (SDNY July 9, 2014). ■

About the Author

Beth A. Mohr is Managing Partner of The McHard Firm, a firm dedicated to expert testimony, forensic accounting, investigations, and professional education.

Beth A. Mohr
The McHard Firm
Albuquerque, New Mexico
505-554-2968
EMAIL bmohr@TheMcHardFirm.com
WEBSITE https://themchardfirm.com

Attacking an Informer

(Continued from page 20)

F.3d 518, 522–23 (2d Cir. 2005) (upholding conviction where the trial court had given a general "interested witness" charge); *United States v. Ridinger*, 805 F.2d 818, 820–22 (8th Cir. 1986) (no "cautionary tale" of instruction to treat informer's testimony with special care); *United States v. Solomon*, 856 F.2d 1572, 1578–79 (11th Cir. 1988) (no mention in instruction of the witness's "credibility as an accomplice or a drug addict"); *see also United States v. Hopkins*, 518 F.2d 152, 155 (3d Cir. 1975) (holding that while an instruction on witness's drug addiction and status as a paid informant would have been proper, there was no error when defense counsel had not requested it).

18. *United States v. Bernal-Obeso*, 989 F.2d 331, 334 (9th Cir. 1993).

19. FED. R. EVID. 702(a); see *Daubert v. Merrell Dow Pharmaceuticals, Inc.*, 509 U.S. 579 (1993).

20. FED. R. EVID. 704(a) & comment. Further, Rule 608(a).

21. See Anne Bowen Poulin, *Credibility: A Fair Subject for Expert Testimony?* 59 FLA. L. REV. 991, 1008–09 (2007).

22. See *United States v. Shay*, 57 F.3d 126, 131 (1st Cir. 1995); *United States v. Gonzalez-Maldonado*, 115 F.3d 9, 14-15 (1st Cir. 1997); but see *United States v. Beasley*, 72 F.3d 1518, 1528 (11th Cir. 1996); *Bastow v. General Motors Corp.*, 844 F.2d 506, 510-11 (8th Cir. 1988).

23. 343 U.S. at 757.

24. See *United States v. Gaind*, 31 F.3d 73 (2d Cir. 1974); *United States v. Cosentino*, 844 F.2d 30 (2d. Cir 1988); *United States v. Jones*, 763 F.2d 518, 522 (2d Cir. 1985).

25. 580 F.2d at 1150.

26. 703 F. Supp. 5 [trial transcript pg. 360] (EDNY 1989).

27. *Berger v. United States*, 295 U.S. 79, 88 (1935).

28. 618 F.2d 530, 536 (1980).

29. *Id.*

30. See *United States v. Necoechea*, 986 F.2d 1273, 1278 (9th Cir. 1993).

31. 547 N.E.2d 314 (Mass. 1989).

32. *Id.* at 319.

33. *People v. Enos*, 425 N.W.2d 104 (1988).

34. *State v. Palmer*, 199 P.3d 706 (Ariz. Ct. App. Div. 1 2008).

35. *People v. Smith*, 12 Cal. App. 5th 776 (Cal. App. 4th Dist. 2017).

36. *Silvestri v. State*, 332 So. 2d 351 (1976).

37. *Jones v. State* 285 S.E.2d 45 (1981).

38. *Mehaffey v. State*, 723 S.W.2d 798 (1987). ■