October 2020

NAGTRI
THE NAAG TRAINING & RESEARCH ARM
CENTER FOR CONSUMER PROTECTION

Follow the Money: An Introduction to Cryptocurrency Transactions

Miles Vaughn, Assistant Attorney General,
Cyber Fraud Unit, Consumer Protection Division,
Florida Attorney General's Office

The world is experiencing a surge in the use of convertible virtual currencies or "cryptocurrency." America's largest financial institutions, along with the Federal Reserve, are currently exploring its uses and applications.[1] The American consumer is also adapting to this technology as it has never been easier to purchase and use cryptocurrency. However, as with many innovations, this potential for tremendous benefit comes at a cost. As the use of such currencies increases, so do the risks that this technology will be exploited by criminals at the expense of consumers. Bitcoin, the most widely used cryptocurrency, was created in 2009 and there has not been much time for regulators, law enforcement, or consumers to become knowledgeable on how exactly this technology works.[2] Understanding this technology is ever more necessary as the use of virtual currencies becomes more commonplace.

On October 8, 2020, the U.S. Department of Justice's (DOJ) Cyber-Digital Task Force published "Cryptocurrency: An Enforcement Framework" (the "Enforcement Framework").[3] This 83-page report is a comprehensive review of the current threats posed by cryptocurrencies, the laws and regulations governing the use of cryptocurrencies, and the future strategies and responses that the Department of Justice may implement to protect the public. In a press release accompanying the publication of the Enforcement Framework, Attorney General William P. Barr states that

[1] Governor Lael Brainard, Fed. Reserve Bd. of Governors, An Update on Digital Currencies, Address at the Federal Reserve Board and Federal Reserve Bank of San Francisco's Innovation Office Hours (Aug. 13, 2020) https://www.federalreserve.gov/newsevents/speech/brainard20200813a.htm. PayPal recently announced a new service enabling its customers to buy, hold and sell cryptocurrency from PayPal accounts. Press Release, "PayPal Launches New Service Enabling Users to Buy, Hold and Sell Cryptocurrency," PAYPAL (October 21, 2020), available at: https://newsroom.paypal-corp.com/2020-10-21-PayPal-Launches-New-Service-Enabling-Users-to-Buy-Hold-and-Sell-Cryptocurrency.

[2] Zoë Bernard, *Everything You Need to Know about Bitcoin, its Mysterious Origins, and the Many Alleged Identities of its Creator*, BUSINESS INSIDER (Nov. 10, 2018, 8:00 AM), https://www.businessinsider.com/bitcoin-history-cryptocurrency-satoshi-nakamoto-2017-12.

[3] U.S. DEP'T OF JUSTICE, REPORT OF THE ATTORNEY GENERAL'S CYBER-DIGITAL TASK FORCE ON CRYPTOCURRENCY: AN ENFORCEMENT FRAMEWORK (2020) [hereinafter Enforcement Framework], available at: https://www.justice.gov/ag/page/file/1326061/download (last accessed Oct. 19, 2020).

"[c]ryptocurrency is a technology that could fundamentally transform how human beings interact, and how we organize society. Ensuring that use of this technology is safe and does not imperil our public safety or our national security, is vitally important to America and its allies."[4]

It is readily apparent from the words and actions of the heads of the United States' financial and legal entities that Bitcoin and other cryptocurrencies are here to stay. However, as this technology continues to develop, it poses a critical challenge to law enforcement. The DOJ report describes in detail a variety of criminals, ranging from international drug dealers, to terrorists, to sex trafficking rings, that used this technology to fund their illegal activities. Although not every agency will have at its disposal the same breadth of resources available to the Department of Justice, DOJ's Enforcement Framework shows that criminals using Bitcoin are not untouchable and despite the complexity of this technology, it is still possible to bring these criminals to justice. This article is not intended to serve as a guide on how to conduct investigations into crypto-related crimes but instead offers a glimpse into the information necessary to make meaningful decisions in an investigation.

An Introduction to Cryptocurrency

Cryptocurrencies are a form of virtual currency that rely on cryptography[5] and distributed ledgers. Cryptography provides security while distributed ledgers, which are shared databases between a network of users, create a reliable record of global transactions. On a "blockchain," which is a type of distributed ledger, a series of time-stamped "blocks" containing the current state of transactions must be cryptographically validated by users on the network.[6] Cryptocurrency blockchains are typically accessible to the public and are also referred to as "permissionless" blockchains, to distinguish them from "permissioned" blockchains, access to which is restricted. A record of every single Bitcoin transaction is publicly available information and there are a variety of open source intelligence (OSINT) resources to access and search these records. Permissioned blockchains, like JP Morgan's Quorum, are only accessible to approved participants.[7] There are also hybrid blockchains, like Ripple's XRP token, that simultaneously use both permissioned and permissionless blockchains.[8]

[4] Press Release, "Attorney General William P. Barr Announces Publication of Cryptocurrency Enforcement Framework," U.S. DEP'T OF JUSTICE (Oct. 8, 2020), available at: https://www.justice.gov/opa/pr/attorney-general-william-p-barr-announces-publication-cryptocurrency-enforcement-framework (last accessed Oct. 19, 2020).

[5] Shobit Seth, *Explaining the Crypto in Cryptocurrency*, INVESTOPEDIA, https://www.investopedia.com/tech/explaining-crypto-cryptocurrency/#:~:text=Cryptography%20is%20the%20mathematical%20and,the%20purpose%20of%20%22mining.%22 (last updated Jan. 25, 2020). ("Cryptography is the mathematical and computational practice of encoding and decoding data.")

[6] Shermin Voshmgir, *What Is Blockchain?*, BLOCKCHAINHUB BERLIN, https://blockchainhub.net/blockchain-intro/ (last visited Oct. 26, 2020).

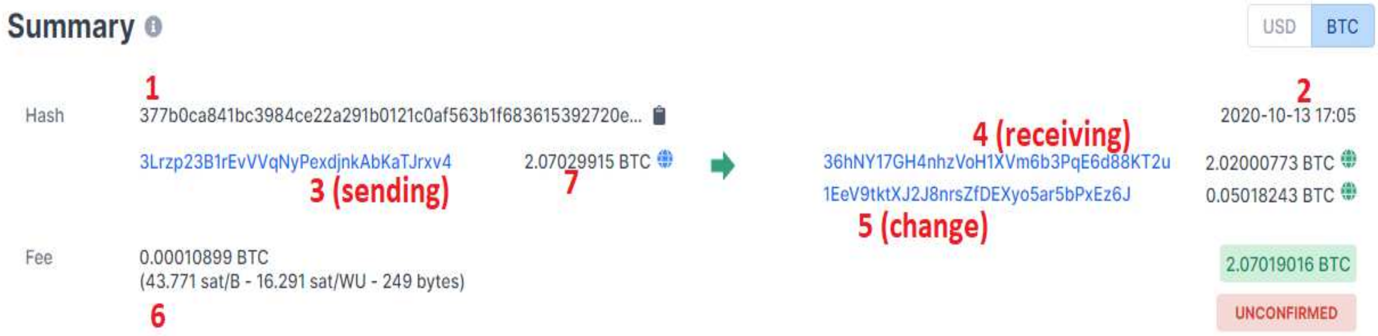
[7] Calvin Price, *Introduction to Quorum: Blockchain for the Fin. Sector*, MEDIUM (Jan. 4, 2018), https://medium.com/blockchain-at-berkeley/introduction-to-quorum-blockchain-for-the-financial-sector-58813f84e88c.

[8] Toshendra Sharma, *What Is Hybrid Blockchain? How Can It Help to Solve Everyday Problems?*, BLOCKCHAIN COUNCIL, https://www.blockchain-council.org/blockchain/what-is-hybrid-blockchain-how-can-it-help-to-solve-everyday-problems/#:~:text=Another%20real%2Dworld%20application%20of,the%20case%20of%20a%20dispute.

Bitcoin transactions are considered pseudo-anonymous since the history of transactions is publicly available. However, the information provided in these reports can be difficult to interpret without understanding how Bitcoin is transacted. An OSINT report on Bitcoin transactions typically contains the following data:

1. The hash[9] of the transaction;
2. The date and time of the transaction;
3. The sender's wallet address;
4. The receiving wallet's addresses;
5. The change wallet's address;
6. The processing fees; and
7. The amount transacted.

The figure below is a depiction of an OSINT report of a Bitcoin transaction showing the transactional data elements which are recorded on the Bitcoin blockchain.



Summary

Hash 377b0ca841bc3984ce22a291b0121c0af563b1f683615392720e...

2020-10-13 17:05

3Lrzp23B1rEvVVqNyPexdjnkAbKaTJrxv4 2.07029915 BTC

36hNY17GH4nhzVoH1XVm6b3PqE6d88KT2u 2.02000773 BTC

1EeV9tktXJ2J8nrsZfDEXyo5ar5bPxEz6J 0.05018243 BTC

Fee 0.00010899 BTC
(43.771 sat/B - 16.291 sat/WU - 249 bytes)

2.07019016 BTC

Figure 1. Example OSINT report with corresponding numbers added; courtesy of Blockchain.com[10]

On the Bitcoin blockchain, the transaction hash is a unique, 64-character series of numbers and letters that is assigned to every verified transaction added to the blockchain.

A wallet, in broad terms, can be thought of as a virtual account that stores the user's cryptocurrency. There is no physical representation of cryptocurrencies such as Bitcoin; instead, these wallets hold pairs of public and private keys that can be used to make and receive payments.[11] The public key is the wallet's address as written in the OSINT depiction above. This can be compared to a bank account and routing numbers. A private key is akin to a password or bank PIN. In order to control the Bitcoin associated with the wallet, the user must provide the

[9] Ameer Rosic, *What Is Hashing? [Step-by-Step Guide-Under Hood of Blockchain]*, https://blockgeeks.com/guides/what-is-hashing/ (last visited Oct. 26, 2020). "Hashing is generating a value or values from a string of text using a mathematical function … [and] is one way to enable security during the process of message transmission when the message is intended for a particular recipient only. A formula generates the hash, which helps to protect the security of the transmission against tampering."

[10] Example of an OSINT Report, BLOCKCHAIN.COM, http://blockchain.com (follow "Explorer" hyperlink; then search transaction 377b0ca841bc3984ce22a291b0121c0af563b1f683615392720e5bb20611f0eb).

[11] Lucas Mearian, *What's a Crypto Wallet (and How Does It Manage Digital Currency)?*, COMPUTERWORLD (Apr.17, 2019, 3:00 AM), https://www.computerworld.com/article/3389678/whats-a-crypto-wallet-and-does-it-manage-digital-currency.html.

private key. Wallets can interact with different blockchains and can store different types of cryptocurrencies.

When a transaction is made using Bitcoin, the sender's wallet is emptied into the recipient's wallet and then the change is transmitted to the change wallet.[12] For example, if a soda costs one dollar and I hand the cashier a five-dollar bill, the cashier will keep the five and hand me four one-dollar bills. The dollar bills go back into my pocket and, although I lost five dollars in this transaction, I have in return gained four dollars from the cashier. The wallet generates a new pair of public and private keys which gives you access to the remaining "change."

A processing or transaction fee, although not required, is often paid in a Bitcoin transaction. These fees are passed on to Bitcoin "miners" as an incentive. On the Bitcoin blockchain, the transaction blocks are validated using computational effort by people or organizations called miners. Bitcoin mining involves significant computational power and, as part of the reward for validating a block, miners receive all the processing or transaction fees associated with transactions in that block. Inevitably, miners will prioritize validating transactions with the highest fees. Bitcoin transactions are not instantaneous and can take many hours to complete. Therefore, users may decide to pay a higher fee in order to have their transactions processed faster. Fees are variable depending on network transaction volume and desired processing time for the transaction.[13] One study concluded that average Bitcoin transaction costs in March 2019 were $0.30 per transaction, however costs averaged $40 per transaction in 2017 when Bitcoin's price was near its peak and transaction volume was very high. An average Bitcoin transaction confirmation in September 2020 took 9.2 minutes[14] at an average cost of $2-7.00. [15]

Exchanges and Cashing Out

At some point, the criminal will stop moving cryptocurrency around and either convert it to "fiat" currency (government-issued currency) or exchange it for goods or services. This is the point at which personal information like names, addresses, and phone numbers can be associated with these accounts. This type of personal information is not intrinsically linked to wallets or transactions. Instead, an investigator must analyze data such as Know Your Customer and Anti-Money Laundering (KYC/AML) records kept by companies and correlate that information to account activity.

Record keeping requirements for cryptocurrency companies vary not only from country to country but, within the United States, from state to state. Aside from state licensing

[12] Danny Bradbury & Khadija Khartit, *How Does Bitcoin Work? Bitcoin Transactions Explained*, THE BALANCE (May 26, 2020), https://www.thebalance.com/how-does-a-bitcoin-transaction-work-391213.

[13] Matt Godshall, *Bitcoin Transaction Fees Explained [Complete Guide]*, UNHASHED (Mar. 13, 2019), https://unhashed.com/cryptocurrency-terms-faq/bitcoin-transaction-fees-explained-complete-guide/#:~:text=Bitcoin%20transaction%20fees%20are%20(generally,when%20making%20a%20Bitcoin%20transaction.&text=When%20a%20miner%20successfully%20adds,fees%20contained%20within%20the%20block.

[14] Jennifer Rudden, *Average Confirmation Time of Bitcoin Transactions from January 2017 to September 2020*, STATISTICA (Oct. 1, 2020), https://www.statista.com/statistics/793539/bitcoin-transaction-confirmation-time/#statisticContainer.

[15] *Bitcoin Average Transaction Fee*, YCHARTS https://ycharts.com/indicators/bitcoin_average_transaction_fee (last visited Oct. 26, 2020).

requirements, federal agencies, such as the Securities and Exchange Commission (SEC) and the U.S. Department of Treasury's Financial Crimes Enforcement Network (FinCEN) and Office of Foreign Assets Control (OFAC), have statutory oversight responsibility over many cryptocurrency companies.[16] Companies that create new cryptocurrencies need to consider SEC guidance while companies that conduct cryptocurrency transactions should follow guidance published by FinCEN and OFAC.[17] Many cryptocurrency companies should also be registered as Money Service Businesses (MSB) and comply with requirements set forth under the Bank Secrecy Act.[18]

Examples of companies that are regulated by these agencies include cryptocurrency exchanges and cryptocurrency kiosks.[19] Cryptocurrency exchanges are online marketplaces that allow users to buy, sell, and store cryptocurrency. Exchanges are also the websites typically used to convert cryptocurrency into fiat currency. Exchanges can be centralized, where buy and sell orders are made to the exchange itself, or peer-to-peer (P2P), where the exchange connects users to make their own independent transactions.[20] P2P exchanges typically do not handle fiat currency and instead act as an escrow service between users. Cryptocurrency kiosks are physical machines, like an ATM, that convert fiat currency to cryptocurrency and vice versa.
Per regulations such as the Bank Secrecy Act, these exchanges and kiosks must maintain KYC/AML records of their users and, in certain cases, file Consumer Transaction Reports and Suspicious Activity Reports.[21] Foreign exchanges that operate in the United States must also register with FinCEN and have an agent for service of process located within the United States that complies with reporting requirements.[22] Legitimate cryptocurrency exchanges face tight regulatory scrutiny. Since cryptocurrencies are considered a risky class of assets, an exchange's bank is also very invested in their client's KYC/AML and other record keeping requirements.[23] A bank is typically not willing to risk an investigation or even its FDIC status over a cryptocurrency exchange that fails to maintain proper records.

[16] *Framework for "Investment Contract" Analysis of Digital Assets*, U.S. SEC. & EXCHANGE COMMISSION (Apr. 3, 2019), https://www.sec.gov/corpfin/framework-investment-contract-analysis-digital-assets.

[17] Eric Auslander et al, *OFAC Releases Guidance on Cryptocurrency*, JD SUPRA (Apr. 9, 2018), https://www.jdsupra.com/legalnews/ofac-releases-guidance-on-cryptocurrency-92621/.

[18] FIN. CRIMES ENF'T NETWORK, APPLICATION OF FINCEN'S REGULATIONS TO CERTAIN BUSINESS MODELS INVOLVING CONVERTIBLE VIRTUAL CURRENCIES, FIN-2019-G001 (May 9, 2019), https://www.fincen.gov/sites/default/files/2019-05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf.

[19] Joe Ciccolo, *What Is a Bitcoin ATM? What Consumers Should Know*, BITAML (June 8, 2020), https://bitaml.com/2020/06/08/what-is-a-bitcoin-atm/.

[20] Andrew Marshall, *P2P Cryptocurrency Exchanges, Explained*, COINTELEGRAPH (Apr. 7, 2017), https://cointelegraph.com/explained/p2p-cryptocurrency-exchanges-explained.

[21] Joe Ciccolo, *Cryptocompliance 101: Everything Cryptos Need to Know about Currency Transaction Reports*, BITAML (Mar. 11, 2019), https://bitaml.com/2019/03/11/ctr-filing-cryptocurrency/.

[22] 31 C.F.R. §§ 1010.100(ff), 1022.380 (2020). *See also* FIN-2012-A001, "Foreign-Located Money Services Businesses" (Feb. 15, 2012); "Bank Secrecy Act Regulations; Definitions and Other Regulations Relating to Money Services Businesses," 76 Fed. Reg. 43,585 (July 21, 2011).

[23] Joshua Mapperson, *FinCEN Director Warns Banks about Cryptocurrency Risk Exposure*, COINTELEGRAPH (Sept. 30, 2020), https://cointelegraph.com/news/fincen-director-warns-banks-about-cryptocurrency-risk-exposure.

The Investigator's Report

During the course of an investigation, the independent recovery firm or government investigator may create a report that details the flow of stolen goods from wallet to wallet. Some criminals may make little effort to hide their tracks and route the cryptocurrency directly to an exchange wallet where it is then converted into fiat currency. More sophisticated criminals may bounce Bitcoins from wallet to wallet and from exchange to exchange in an effort to hide their tracks. When visually represented, these transaction flow charts can become very lengthy and convoluted at first glance. However, an investigator trained with forensics software may identify the exchange that the criminal uses to deposit the ill-gotten gains.

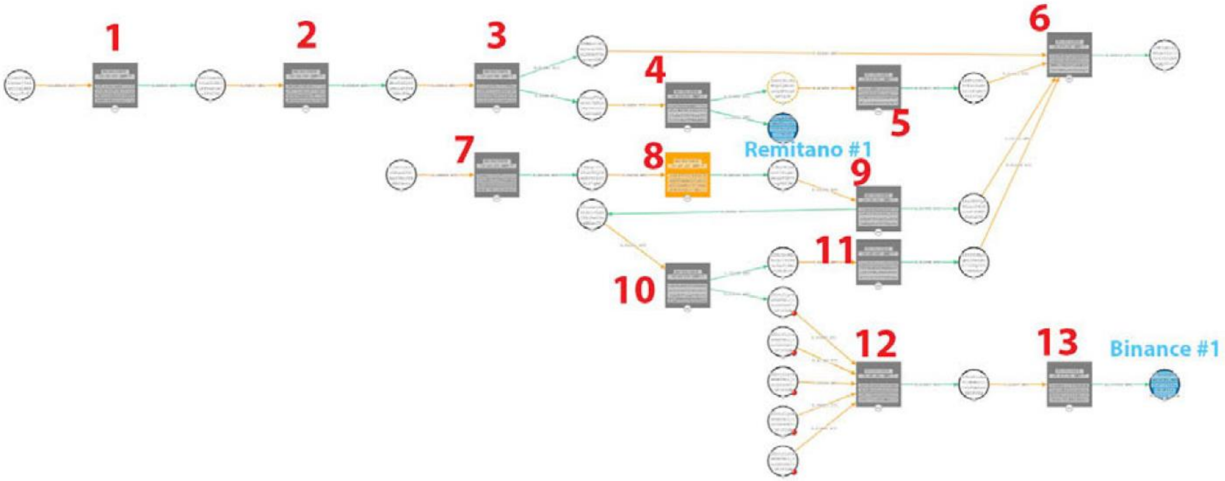


Figure 2 An example transaction flow chart; courtesy of Coinstructive[24]

In Figure 2, there are two exchanges identified by the investigator. Remitano is a P2P exchange headquartered in the Seychelles and Binance is a centralized exchange headquartered in Malta. Binance, as an example, is a registered MSB with a street address in San Francisco, California.[25] Since Binance, as a regulated entity, collects the personal information of every wallet owner, a request can be made to Binance for the suspected criminal's information. A court order can also be sought to freeze or hold the wallet. This is similar to freezing a bank account, locking down the funds until a decision can be made later.

Knowledge and Enforcement

This article only serves as a preview into certain aspects of the cryptocurrency industry. There are many more mechanisms to hide illegal activity involving virtual currencies including mixers, dark web marketplaces, and anonymity enhanced cryptocurrencies. Outside the use of OSINT and forensics tools to track the flow of illicit funds, the most powerful tool to hinder criminal behavior is the enforcement of licensing regulations that require cryptocurrency companies to maintain accurate customer records. As demonstrated above, the use of cryptocurrency does not make a criminal invisible. However, unless proper records are maintained by companies like

[24] CoinStructive is a leader in the fraud investigations and training solutions industry. *See* https://coinstructive.com/.
[25] MSB Registrant Search, FINANCIAL CRIMES ENFORCEMENT NETWORK, http://www.fincen.gov/msb-registrant-search (Search DBA Name field "Binance").

exchanges, it is significantly harder to determine the criminal's identity. Virtual currencies are borderless, and the inherent nature of the technology will require cooperation between states and nations. Armed with the knowledge of how this technology works, state agencies will be better equipped to face these challenges and protect consumers.