TIME TO VALIDATE VALIDATORS: DETERMINING THE LEGAL DUTY OF CRYPTOCURRENCY VALIDATORS UNDER THE BANK SECRECY ACT

Alexis M. Tellerd*

* Alexis Tellerd received her undergraduate finance degree from High Point University in 2019 and is a member of George Mason University Law School's Class of 2022. She sincerely thanks her family, mentors, and friends for their unwavering support. The views expressed are the author's and do not reflect the official policy or position of the Financial Crimes Enforcement Network, the U.S. Dept. of the Treasury, or the U.S. gov't.

INTRODUCTION

In August 2020, the Department of Justice seized approximately two million dollars' worth of cryptocurrency[1] dedicated to financing terrorist groups, such as al-Qaeda and the Islamic State.[2] The ability of terrorist organizations to invisibly transport billions of dollars poses a grave national security concern. Although the extent of criminality within cryptocurrency transactions is debated, it is clear that terrorist groups have adopted the use of cryptocurrency. Rather than dismiss the acknowledgment of this usage as an overreaction, it is imperative to address the future of criminal cryptocurrency behavior prior to widescale adoption.

The current general perception of cryptocurrencies is that of a volatile investment; however, its purpose is to serve as a decentralized, peer-to-peer payment system. Many use cryptocurrency for the privacy decentralization creates, or the ability to conduct transactions outside the purview of financial regulators or other institutions. While some regulation exists surrounding cryptocurrency, there are significant gaps in these regulations. One significant gap surrounds "unhosted" wallets.[3] Unhosted wallets are a

[1] There are several terms to refer to these types of assets. As technically defined, cryptocurrency does not specifically capture all sorts of digital assets; however, for purposes of consistency, the term "cryptocurrency" will be used throughout this Comment.

[2] Devlin Barrett, *U.S. Seizes Millions in Cryptocurrency Meant for Terror Group, Justice Dept. Says*, WASH. POST (Aug. 13, 2020), https://www.washingtonpost.com/national-security/justice-dept-cryptocurrency-terror-groups/2020/08/13/be89d1fa-dd76-11ea-809e-b8be57ba616e_story.html.

[3] Wallets are mechanisms used to store cryptocurrency tokens. Unhosted wallets are a type of wallet that is not associated with a third-party to manage or oversee the wallet. There are also hosted wallets that are managed by third-party entities such as a cryptocurrency exchange. Unhosted wallets are not currently covered by existing

concern as they evade any supervision by third parties or financial institutions, such as a cryptocurrency exchange. This evasion creates a convenient environment for financial crime to occur. Many debate the extent of criminality,[4] but the cryptocurrency structure, and the lack of detailed public information about cryptocurrency and crime, make the volume of cryptocurrency-influenced financial crime difficult to assess accurately. In 2019, Chainalysis[5] investigated twenty-seven different cryptocurrencies over a ten-month period. The results showed 0.4% of transactions involved an identified illicit entity.[6]

This percentage sounds minuscule, but it is equivalent to $3.8 billion moved without being screened for potential criminal activity.[7] From 2013 to 2017, *theft* of Bitcoin alone escalated from $3 million to $89 million;[8] nearly a 3,000% increase. If the cryptocurrency sector remains unregulated, the number of illicit cryptocurrency transactions will likely grow. If the growth in overall criminal activity mirrors the growth in theft, the value of criminal activity could increase from $3.8 billion to $113 billion in four years. This growth rate is concerning when the focus shifts from theft to terrorist financing.

To properly address the national security threat posed by cryptocurrency, it is imperative to establish a way to monitor the transactions falling outside of current regulations, such as transactions

---

cryptocurrency regulation, and the lack of third-party oversight exacerbates the risk of potential criminal activity occurring between unhosted wallets. *See* REQUIREMENTS FOR CERTAIN TRANSACTIONS INVOLVING CERTAIN CONVERTIBLE VIRTUAL CURRENCY OR DIGITAL ASSETS: FREQUENTLY ASKED QUESTIONS, U.S. DEP'T OF THE TREAS. (Dec. 18, 2020), https://home.treasury.gov/system/files/136/2020-12-18-FAQs.pdf.

[4] *See* Hailey Lennon, *The False Narrative of Bitcoin's Role in Illicit Activity*, FORBES (Jan. 19, 2021), https://www.forbes.com/sites/haileylennon/2021/01/19/the-false-narrative-of-bitcoins-role-in-illicit-activity/?sh=3079ca083432.

[5] Chainalysis is an organization providing Blockchain "data, software, services, and research to government agencies, exchanges, financial institutions, and insurance and cybersecurity companies in over 60 countries." CHAINALYSIS, https://www.chainalysis.com/ (last visited Oct. 12, 2021).

[6] Will Heasman, *Criminal Activity in Crypto: The Fact, the Fiction and the Context*, COINTELEGRAPH (Nov. 30, 2019), https://cointelegraph.com/news/criminal-activity-in-crypto-the-fact-the-fiction-and-the-context.

[7] *Id.*

[8] Corinne Ramey, *The Crypto Crime Wave is Here*, WALL ST. J. (Apr. 26, 2018), https://www.wsj.com/articles/the-crypto-crime-wave-is-here-1524753366.

involving unhosted wallets, while balancing the privacy that cryptocurrency users value. The Bank Secrecy Act ("BSA") protects financial institutions against money laundering and other criminal activity by imposing recordkeeping and reporting requirements.[9] Despite the vast array of institutions subject to the BSA, the BSA does not directly capture cryptocurrencies. A proposed solution to fix this issue is to bring Blockchain validators within the regulatory jurisdiction of the BSA by classifying validators as a type of financial institution under 31 U.S.C. § 5132(a)(2).[10]

The Financial Crimes Enforcement Network ("FinCEN") conducts its regulatory duties on the assumption that cryptocurrency transactions fall within the money service businesses subsection of the financial institution definition under the BSA.[11] Specifically, it asserts that individuals engaged in cryptocurrency transactions are considered money transmitters, a type of money service business.[12] However, this definition has not been legally established, and there has been significant pushback from other organizations. The principal purpose of this Comment is to demonstrate the need for comprehensive cryptocurrency regulation and oversight, with a particular focus on the risks posed by unhosted wallets. Utilizing validators as a monitoring tool will bridge these current gaps. However, prior to establishing validators as a financial institution, it is important to analyze exactly how this would occur and the legal implications.

This Comment will discuss the purpose of the BSA and provide a proposed solution of how to cover transactions involving unhosted wallets within the Act's jurisdiction. This Comment will also

[9] Bank Secrecy Act, 31 U.S.C. § 5311 (2021); *FinCEN's Mandate From Congress*, U.S. DEP'T OF THE TREAS., FIN. CRIMES ENF'T NETWORK, https://www.fincen.gov/resources/statutes-regulations/fincens-mandate-congress.
[10] *See* MONEY TRANSMITTERS AND VALIDATORS, *infra* Section III.
[11] FIN. CRIMES ENF'T NETWORK, U.S. DEP'T OF THE TREAS., FIN-2019-G001, APPLICATION OF FINCEN'S REGULATIONS TO CERTAIN BUSINESS MODELS INVOLVING CONVERTIBLE VIRTUAL CURRENCY (2019), https://www.fincen.gov/sites/default/files/2019-05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf [hereinafter *FinCEN 2019 Guidance*].
[12] *Id.*

analyze how these transactions relate to current BSA regulations. The importance of this regulation is influenced by the grave national security risk a largely unregulated market capitalization of cryptocurrency transactions will create. Therefore, there must be a thorough way to regulate cryptocurrency, whether through validators or another avenue.

I. BACKGROUND

One available solution to the issue of balancing national security with privacy concerns is creating a legal duty for validators. If a duty to screen against potential criminal activity is added to the current task of validating all transactions along a Blockchain, [13] it will create a barrier against potential criminal activity without inviting financial regulators directly into the cryptocurrency ecosystem. The issue presented requires in-depth discussions of cryptocurrency technology and the current regulatory framework created by the BSA. This discussion will begin with an analysis of virtual currencies, Blockchain systems, and the validation processes on a Blockchain. Next, the BSA will be analyzed along with the entities subject to its regulations.

A. Technology

1. Virtual Currencies

Cryptocurrencies are virtual currencies secured by cryptography.[14] Cryptography is the tool permitting cryptocurrencies to operate on a decentralized basis.[15] They are not regulated by a central authority, making them a preferred payment method for those

[13] *What is a Cryptocurrency? A Beginner's Guide to Digital Money*, COINTELEGRAPH, https://cointelegraph.com/Blockchain-for-beginners/what-is-a-cryptocurrency-a-beginners-guide-to-digital-money (last visited Oct. 12, 2021).
[14] Jake Frankenfield, *Cryptocurrency*, INVESTOPEDIA (May 5, 2020), https://www.investopedia.com/terms/c/cryptocurrency.asp.
[15] Ben R. Craig & Joseph Kachovec, *Bitcoin's Decentralized Decision Structure*, FED. RSRV. BANK OF CLEVELAND (July 16, 2019), https://www.clevelandfed.org/en/newsroom-and-events/publications/economic-commentary/2019-economic-commentaries/ec-201912-bitcoin-decentralized-network.aspx.

who prefer privacy.[16] In addition to decentralization, the transactions occur pseudonymously. No personal information other than the public wallet address pseudonym of each party is relayed with each transaction or made public once the transaction is added to a Blockchain.[17] Some privacy coins operate anonymously; however, the vast majority of common cryptocurrencies, including Bitcoin, operate pseudonymously.

There are three general methods to acquire cryptocurrency. First, an individual may fund an account by purchasing cryptocurrency via a cryptocurrency exchange.[18] Through this method, a digital wallet holds the cryptocurrency purchased through the exchange. The wallet possesses a specific set of numbers to identify itself on a Blockchain, referred to as a public wallet address.[19] The exchange maintains custody of the wallet address, but the individual owns the contents of the wallet.[20] This is referred to as a "hosted" wallet.[21] On the other hand, unhosted wallets are privately held by the owner of the cryptocurrency.[22] It can be tremendously difficult to determine who is controlling the unhosted wallet or cryptocurrency held in the wallet.[23] For this reason, the threat of financial crime is more pervasive in these types of wallets.[24]

A second method of acquiring cryptocurrency is through using cash at a cryptocurrency ATM.[25] The ATM can generate a wallet, similar to an exchange, or send the cryptocurrency tokens to an

---

[16] *Id.*
[17] Andrey Sergeenkov, *What is Bitcoin?*, COINDESK (Aug. 18, 2020), https://www.coindesk.com/learn/what-is-bitcoin.
[18] Luke Conway & Julius Mansa, *How to Buy Bitcoin*, INVESTOPEDIA (May 31, 2021), https://www.investopedia.com/articles/investing/082914/basics-buying-and-investing-bitcoin.asp.
[19] *Id.*
[20] *Id.*
[21] *Id.*
[22] *Id.*
[23] *Id.*
[24] *See* Conway & Mansa, *supra* note 18.
[25] David Thorne, *Cryptocurrency ATM And How Does It Work*, ENTREPRENEUR (Oct. 1, 2020), https://www.entrepreneur.com/article/357028#:~:text=Cryptocurrency%20ATM%20is%20a%20terminal,into%20a%20stand%20or%20wall.

already-owned address.[26] Similarly, individuals may purchase cryptocurrency directly from others online and send these tokens to a public wallet address.[27]

The third method of acquiring cryptocurrency is to "mine" for them. The primary role of a miner is to verify the transactions occurring along a Blockchain.[28] If a miner correctly identifies a transaction as valid, they are rewarded with a unit of that cryptocurrency in exchange for maintaining the peer-enforced supervision.[29] This process only occurs for cryptocurrencies utilizing a proof of work consensus algorithm.

2. Blockchain

Individuals who wish to pay or conduct transactions in a cryptocurrency do so on a Blockchain. A Blockchain is a virtual ledger system that maintains a complete history of the transactions that have occurred in a specific cryptocurrency.[30] The ability for parties to send cryptocurrencies to one another without an overseeing entity relies on individuals known as validators. These individuals have a duty to verify the legitimacy of each transaction before it is added to a Blockchain ledger.[31] One example of ensuring validity would be checking the sender truly owns the proper amount of cryptocurrency and has the amount available in their virtual wallet.[32] The historical transactional data on the Blockchain, combined with a third-party validator, allows a pseudonymous transactional ecosystem to function without the need for an overseeing financial institution.[33]

---

[26] Jake Frankenfield, Erika Rasure & Michael Logan, *Bitcoin ATM*, INVESTOPEDIA (Aug. 27, 2021), https://www.investopedia.com/terms/b/bitcoin-atm.asp.
[27] *Id.*
[28] Bruno Skvorc, *What is a Bitcoin Node? Mining Versus Validation*, SITEPOINT (May 17, 2018), https://www.sitepoint.com/bitcoin-nodes-mining-validation/.
[29] *Id.*
[30] Andrew Tar, *Proof-of-Work, Explained*, COINTELEGRAPH (Jan. 17, 2018), https://cointelegraph.com/explained/proof-of-work-explained.
[31] *What is a Cryptocurrency? A Beginner's Guide to Digital Money*, *supra* note 13.
[32] Conway & Mansa, *supra* note 18.
[33] Shobhit Seth, *What is a Cryptocurrency Public Ledger?*, INVESTOPEDIA (July 14, 2020), https://www.investopedia.com/tech/what-cryptocurrency-public-ledger/.

The Blockchain provides a historical public record of all transactions that have occurred with a specific cryptocurrency.[34] Before a transaction is confirmed on the Blockchain, all nodes must verify the validity of the transaction.[35] Because numerous transactions are occurring simultaneously for many cryptocurrencies, once a transaction is considered valid, the validators on a specific Blockchain must agree on the proper order to add these transactions to the Blockchain.[36] This process is referred to as establishing "consensus," and requires validators to agree to the order of the Blockchain's transactions.[37]

The pseudonymity of cryptocurrency transactions results from the use of public and private "keys."[38] A public key provides the address of a party's cryptocurrency wallet, or where their tokens are stored.[39] A private key holds a user's personal identifying information, and it serves as a password to access their virtual wallet.[40] The private key is used to confirm transactions being sent to a public key.[41] If an individual has cryptocurrency sent to their public wallet address, they can access it by inputting their private key, which is analogous to a digital signature, verifying the identity of the individual who owns the receiving public key.[42] Only the public keys, or the wallet addresses, are stored on a Blockchain along with the amount of tokens being transferred.[43] However, without access to a specific public key's corresponding private key, no identifying information is revealed by

[34] *Id.*
[35] *See* Hupayx, *How Are Blockchain Transactions Validated? Consensus v. Validation*, MEDIUM (June 29, 2020), https://medium.com/hupayx/how-are-Blockchain-transactions-validated-consensus-vs-validation-ada9c001fd0a (describing how a single computer in a Blockchain is referred to as a "node," and a full node retains a comprehensive copy of the Blockchain).
[36] *Id.*
[37] *Id.*
[38] *What Are Public Keys and Private Keys*?, LEDGER (Oct. 23, 2019), https://www.ledger.com/academy/Blockchain/what-are-public-keys-and-private-keys.
[39] *Id.*
[40] *Id.*
[41] *Id.*
[42] *Id.*
[43] *What is a Cryptocurrency? A Beginner's Guide to Digital Money, supra* note 13.

the mere possession of a public key.[44] This near-anonymity makes cryptocurrency an ideal method for criminal financial activity to be executed.

3. Validation Processes

The validator's role changes depending on the type of consensus algorithm a specific cryptocurrency utilizes. A consensus algorithm constructs the process of allocating validating duties to the plethora of validators present on each Blockchain.[45] Only one validator may successfully confirm a particular transaction, even if multiple validators attempt to solve it simultaneously.[46] The validator who succeeds is rewarded with a token of the respective cryptocurrency.[47] The two main algorithms are "proof of work" and "proof of stake."[48]

A "proof of work" consensus algorithm rewards the first miner who solves the cryptographic puzzle; therefore, this system rewards speed and efficiency.[49] Proof of work systems often refer to validators as miners, who compete against one another to acquire the cryptocurrency reward.[50] The well-known cryptocurrency Bitcoin utilizes this type of consensus algorithm.[51] It was the first type of algorithm utilized within cryptocurrency transactions along a Blockchain; however, it has created some issues over time.[52] The more miners that enter the environment, the greater the competition is to solve these puzzles. Numerous miners attempting to validate the same transactions not only encourages competition in solving the cryptographic puzzle, but it also encourages competition to acquire as

[44] Conway & Mansa, *supra* note 18.
[45] *What Is a Blockchain Consensus Algorithm?*, BINANCE ACAD. (Aug. 17, 2021), https://academy.binance.com/en/articles/what-is-a-Blockchain-consensus-algorithm.
[46] *Id.*
[47] *Id.*
[48] *Id.*
[49] Jake Frankenfield, *Proof of Work (POW)*, INVESTOPEDIA (July 22, 2021), https://www.investopedia.com/terms/p/proof-work.asp.
[50] *Id.*
[51] Tar, *supra* note 30.
[52] *Id.*

much processing power to do so. The more processing power a miner possesses, the more likely it is for the miner to acquire the reward.

One tremendous issue with the proof of work algorithm is the waste of resources that occurs, specifically, electricity. The electricity cost of dozens, if not hundreds, of miners attempting to be the sole validator of a transaction is significant.[53] In 2015, it was estimated that one Bitcoin transaction required the amount of electricity necessary to power one and a half American households per day.[54]This has led to the growing popularity of another algorithm, known as "proof of stake."

Proof of stake algorithms significantly differ from proof of work systems as they do not rely on competition. Instead, the validator responsible for validating the next block of the Blockchain is randomly selected by the proof of stake algorithm.[55] To be included in the pool of potential validators, an individual must own the cryptocurrency of the corresponding Blockchain.[56] The odds of being selected directly correlates to the amount of cryptocurrency owned.[57] The more cryptocurrency owned, the greater the chance of being selected. Since there is no competition to compete in the validation process, selection leads to the receipt of the validation reward.[58] This eradicates the tendency of multiple miners to simultaneously validate the same transactions as well as the waste of excessive amounts of processing power due to the lack of competition.[59]

B. Regulation

The current state of cryptocurrency regulation is littered with grey areas and unclear borders. Different parties have begun

[53] Jake Frankenfield, *Proof of Stake (PoS)*, INVESTOPEDIA (Aug. 11, 2019), https://www.investopedia.com/terms/p/proof-stake-pos.asp.
[54] *Id.*
[55] Alicia Naumoff, *Why Blockchain Needs 'Proof of Authority' Instead of 'Proof of Stake'*, COINTELEGRAPH (Apr. 26, 2017), https://cointelegraph.com/news/why-Blockchain-needs-proof-of-authority-instead-of-proof-of-stake.
[56] Frankenfield, *supra* note 53.
[57] *Id.*
[58] *Id.*
[59] *Id.*

constructing regulations and legislation to combat the issues arising in the cryptocurrency space, but it remains the wild west of the financial sector. The main regulation used to combat financial crime is the BSA, the nation's comprehensive anti-money laundering statute.[60] However, the BSA does not directly cover cryptocurrency transactions. FinCEN possesses the regulatory jurisdiction of enforcing the BSA, and the agency performs this duty by monitoring reports of suspicious activity and other problematic actions.[61]

The BSA requires financial institutions to abide by heightened reporting and recordkeeping guidelines of transactions occurring within and between these institutions.[62] The term "financial institutions" under the BSA is a broad, encompassing term. According to the U.S. Code, there are twenty-six definitions of "financial institutions" under this regulation.[63] These definitions range from insured banks[64] to travel agencies[65] to dealers in precious metals, stones, or jewels.[66] Although the scope of these definitions is vast, no section explicitly applies to virtual currencies or assets. The currently agreed-upon classification for cryptocurrencies belongs in subsection R, referring to money service businesses ("MSB"). The twenty-five other subsections of the "financial institutions" definition do not apply to cryptocurrencies, so applying the money service businesses definition to cryptocurrency entities at least provides regulators an avenue to reach cryptocurrency transactions.[67]

---

[60] *FinCEN 2019 Guidance*, *supra* note 11, at 1.
[61] *Id.*
[62] FED. DEPOSIT INS. CORP., RISK MANAGEMENT MANUAL OF EXAMINATION POLICIES, § 8.1, https://www.fdic.gov/regulations/safety/manual/ [hereinafter FDIC MANUAL].
[63] 31 U.S.C. § 5312(a)(2).
[64] 31 U.S.C. § 5312(a)(2)(A).
[65] 31 U.S.C. § 5312(a)(2)(Q).
[66] 31 U.S.C. § 5312(a)(2)(N).
[67] *Is Gemini Licensed or Regulated*, GEMINI, https://support.gemini.com/hc/en-us/articles/204734485-Is-Gemini-licensed-and-or-regulated- (last visited Oct. 26, 2021). One exception to the focus on money services businesses is Gemini, a cryptocurrency exchange, wallet and custodian. Gemini is registered as a trust company, which removes it from regulatory oversight by FinCEN. It is monitored by the New York State Department of Financial Services.

II. MONEY SERVICE BUSINESSES, MONEY TRANSMISSION SERVICES, AND MONEY TRANSMITTERS

Three fundamental definitions within the money transmission subsection include money service businesses, money transmitters, and money transmission services.[68] Defining actors as money transmitters or money service businesses imposes the recordkeeping and reporting standards required by the BSA.

A. Money Service Businesses

MSBs are defined as "'a person wherever located doing business, whether or not on a regular basis or as an organized or licensed business concern, wholly or in substantial part within the United States,' operating directly, or through an agent, agency, branch or office, who functions as, among other things, 'a money transmitter.'"[69] A "person" under this definition can be a natural person, corporation, partnership, trust, etc.[70] There are seven distinct categories of money service businesses: dealers in foreign exchanges; check cashers; issuers or sellers of traveler's checks or money orders; providers of prepaid access; money transmitters; the U.S. Postal Service; and seller of prepaid access.[71] The type of MSB relevant to the discussion of cryptocurrency regulation is a money transmitter.

B. Money Transmission Services

"Money transmission services" is defined as the "acceptance of currency, funds, or other value that substitutes for currency from one person and the transmission of currency, funds, or other value that substitutes for currency to another location or any person by any means."[72] FinCEN does not include cryptocurrency within the definition of "funds," nor are cryptocurrencies included within the definition of currency.[73] They are neither coin nor paper money of the

[68] *FinCEN 2019 Guidance*, *supra* note 11.
[69] *Id.* (citing 31 C.F.R. § 1010.100(ff)).
[70] *Id.*
[71] 31 C.F.R. § 1010(ff).
[72] 31 C.F.R. § 1010(ff)(5)(i)(A).
[73] *FinCEN 2019 Guidance*, *supra* note 11.

United States.[74] FinCEN has intentionally kept "other value that substitutes for currency" broad, which allows cryptocurrency to reside under this definition.[75]

C. Money Transmitter

FinCEN defines a money transmitter as a "person," who "provides money transmission services" or "any other person engaged in the transfer of funds."[76] As stated, FinCEN does not include cryptocurrencies within the definition of "funds," so the second definition is not at issue here. With the first definition of money transmission in mind, a money transmitter is an entity tasked with moving value from one party to another. They accept currency or other value from one party and move it to another party. In its 2019 guidance, FinCEN stated a person may be a money transmitter when they engage in transactions that fall within the purview of money transmission services, regardless of the technology utilized in the transaction or the value or type of asset being substituted for currency, either physical or virtual.[77]

An example of an organization designated as a money transmitter is a cryptocurrency exchange that sells initial coin offering ("ICO") coins or tokens.[78] These exchanges sell or exchange the ICO coins for other cryptocurrency, fiat currency, or other value that substitutes for currency.[79] This acceptance of a type of currency and

---

[74] 31 C.F.R. § 1010(m).

[75] FIN. CRIMES ENF'T NETWORK, FIN-2013-G001, APPLICATION OF FINCEN'S REGULATIONS TO PERSONS ADMINISTERING, EXCHANGING, OR USING VIRTUAL CURRENCIES, at 3 (Mar. 18, 2013), https://www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdf. Virtual currencies have been included under the phrase, "other value that substitutes as currency." *Id.* at 5. Since "funds" is commonly used in a series with this phrase, it infers that "other value that substitutes as currency" and "funds" are separate entities. *FINCEN 2019 GUIDANCE*, *supra* note 11.

[76] 31 CFR § 1010.100(ff)(5)(i)(A).

[77] *FINCEN 2019 GUIDANCE*, *supra* note 11.

[78] Letter from Drew Maloney, Ass't Sec'y for Legis. Aff., to Sen. Ron Wyden, Ranking Member on the Senate Comm. on Fin. (Feb. 13, 2018), https://www.coincenter.org/app/uploads/2020/05/fincen-ico-letter-march-2018-coin-center.pdf.

[79] *Id.*

subsequent conveyance of another type of currency would fall within the realm of a money transmitter's duties.

III. MONEY TRANSMITTERS AND VALIDATORS

Validators do not fall within the money transmitter definition provided by FinCEN's 2019 guidance on convertible cryptocurrency.[80] FinCEN defines "money transmitter" as a "person that provides money transmission services" which consist of "the acceptance of . . . other value that substitutes for currency from one person and the transmission of . . . other value that substitutes for currency to another location or person for any means."[81] Validators are not involved with the actual movement of assets from one person to another; validators act as a screening mechanism to ensure the transmission is legitimate. Thus, they serve more as a foundational structure in the cryptocurrency system than a participatory element in the transmission of the cryptocurrency.

An example to demonstrate the relatively limited role that validators play in most cryptocurrency transactions are Lightning nodes, which operate on top of the Bitcoin network. Lightning nodes are created to allow two counterparties already transacting along a Blockchain to transact within a private channel.[82] When a Lightning node is opened, a specific amount of cryptocurrency may be added to the channel, and the counterparties may move these tokens between their respective wallets.[83] The only effect Lightning nodes have on the underlying Blockchain is the addition of the final value of cryptocurrency remaining in the channel when the channel is closed.[84] The previous transactions are not reflected within the Blockchain's immutable ledger. Lightning nodes operate to rapidly settle potentially large amounts of transactions between different parties, allowing the node operator to settle the aggregate amounts of transactions later,

[80] *FINCEN 2019 GUIDANCE*, *supra* note 11.
[81] *Id.*
[82] *What is Lightning Network and How Does it Work*, COINTELEGRAPH, https://cointelegraph.com/lightning-network-101/what-is-lightning-network-and-how-it-works.
[83] *Id.*
[84] *Id.*

much like other informal value transfer systems.[85] On the contrary, validators do not function in this way. Validators are at no time in possession of the funds in transit, unlike the Lightning nodes in the above example.

Although validators do not seem to fall within the accepted definition of a money transmitter, they still require additional regulatory scrutiny to close the gaps in the financial system abused by illicit actors. This is not to assert the necessity of pervasive rules and regulations, which would render the emphasis on privacy that many cryptocurrencies tout obsolete. However, maintaining a balance between privacy and oversight is vital. Otherwise, current users may abandon the current cryptocurrency framework to avoid exposure, or technical engineers may rapidly evolve the system into an entity beyond the reach of proposed regulations.

Without the presence of validators in a Blockchain, the peer-to-peer transactions could not be properly executed without an overseeing financial institution. This demonstrates validators' key roles in confirming transactions along a Blockchain; they are an outside party to this transaction, working to certify and maintain an ecosystem founded upon mutual trust. There may be cryptocurrencies that use technologies where validators take custody of assets or otherwise are involved in the sending of a transmittal order for a transfer of funds. In such a scenario, validators may become an MSB, but barring that, validators generally do not qualify as MSBs.

IV. IS REGULATION NECESSARY?

Many advocates for cryptocurrency prefer utilizing these assets for the privacy they afford. However, imposing monitoring responsibilities upon validators would not destroy this privacy. When an individual transacts with a registered and regulated financial institution, personal information is attached to those transactions.[86] If suspicious activity is detected, the financial institutions have direct access to the information attached to the transactions.[87] When

[85] *Id.*
[86] *Id.*
[87] *Id.*

individuals transact on Blockchains, the only available information associated with the transaction is the individual's public key.[88] While it is possible to follow conveyances made by a single public key, it is technically impossible to directly identify individuals without direct access to their cryptocurrency wallets or private key.[89] If this information is obtained, law enforcement would have access to such identifying information.

The proposal to place a screening duty upon validators preserves the privacy already in place within cryptocurrency transactions. Validators have access to each transaction occurring on a Blockchain to verify the validity of the conveyance. In addition, the proposal introduces a secondary responsibility for the validators to alert regulators if a red flag indicating potential money laundering activity accompanies a specific transaction.

For national security purposes, it is imperative that cryptocurrency transactions are screened for potential financial criminal activity. The sources of these illicit funds come from a plethora of criminal acts such as narcotic or human trafficking, cybercrime, organized crime, bribery, among many others.[90] These laundered funds are used to support terrorist organizations or acts of terrorism.[91] The presence of these illicit funds throughout the financial system is detrimental to the overall marketplace. It eradicates the ethical standards currently in place to protect consumers and draws the financial institutions themselves into a web of criminal activity.

Beyond the implications for financial markets, the use of hidden assets to finance terrorist activity creates a tremendous national security concern. The introduction of pseudonymous

---

[88] *What Are Public Keys and Private Keys*?, *supra* note 38.
[89] *Id.*
[90] Malcolm Wright, *Money Laundering: Part of a Wider Web of Criminal Activity*, THOMSON REUTERS, https://store.legal.thomsonreuters.com/law-products/solutions/fraud-investigations/corporate-investigative/CLEAR-picture/money-laundering-part-of-wider-web-criminal-activity.
[91] Bureau of Int'l Narcotics and Law Enf't Affairs, *Anti-Money Laundering and Countering the Financing of Terrorism*, U.S. DEP'T OF STATE, https://www.state.gov/anti-money-laundering-and-countering-the-financing-of-terrorism/ (last visited Oct. 26, 2021).

payment systems, such as cryptocurrencies and Blockchain technology, eradicates access to personal information in these transactions. If criminal or terrorist organizations have methods to transact and move assets outside the scope of any regulatory jurisdiction, there is no risk of possible detection or seizure of the funds. As the BSA stands now, the simple use of cryptocurrencies will not allow financial regulators to detect suspicious activity that could potentially prevent destructive or catastrophic events from occurring.

V. PROPOSED SOLUTION TO INCLUDE CRYPTOCURRENCY TRANSACTIONS UNDER BANK SECRECY ACT REGULATIONS

Inserting cryptocurrency validators as a subsection of the financial institution's definition under 31 U.S.C. § 5312(a)(2) is the best solution to balance the privacy priorities with the necessary oversight of cryptocurrency transactions. Leaving cryptocurrency exchanges as the sole entity capable of assisting in virtual currency regulation would be insufficient. It would incentivize criminals to simply avoid the regulated exchanges and conduct their business outside the scope of current regulations.

A. How to Utilize Validators to Screen Cryptocurrency Transactions

Leaving cryptocurrencies partially unregulated poses a severe national security risk. There must be a degree of oversight to these transactions. However, if regulators or law enforcement impose overbearing regulations, individuals currently utilizing traditional Blockchain or cryptocurrency technology will be incentivized to transition to increasingly anonymous or unconventional transaction methods. This will ultimately make regulatory oversight more challenging and less effective. Balancing current levels of privacy with the necessity of oversight is the only option to cultivate effective national security protections. The use of validators to maintain this screening duty preserves this balance without disrupting the current function of the cryptocurrency ecosystem.

Validators exist to verify the validity of each cryptocurrency transaction, so the addition of a screening responsibility upon these

entities is the most logical and efficient method to screen for potential financial crime. The simplest recommendation is for current regulators to compile a database of known wallet addresses associated with financial crime. Validators would be tasked to utilize this database and include it within their validation processes. Prior to validating a transaction, the validator would be required to screen the transactions through the provided database to ensure the validators are not confirming transactions associated with an identified illicit entity. If the database identifies one counterparty to a transaction the validator would flag the transaction and provide the two wallet addresses to an overseeing regulator to investigate further. No validation of the transaction would occur prior to a regulator's approval.

As current regulations leave a gap over transactions involving unhosted wallets, this approach would capture all cryptocurrency transactions without tremendously burdening or altering the current validation system. Additionally, it preserves user's privacy by only allowing regulators access to flagged transactions directly provided by the validators. Finally, it would not provide regulators a "backdoor" into monitoring Blockchain ledgers or cryptocurrency transactions, which is a tremendous concern of many cryptocurrency users.

B. The Effect on Validators

Imposing this screening task on a validator would not change the overall role of the validator within the Blockchain ecosystem. It is a validator's duty to ensure legitimate transactions are occurring between two pseudonymous parties.[92] If suspicious activity is detected, it would then be their duty to ensure the regulating agency is aware of this detection. Until the validator receives notice from the regulatory agency, it should withhold from verifying the transaction.

Waiting for such approval would not detract from the efficiency of the validation process or slow down the creation of blocks on a specific Blockchain. This is because transactions are not verified

[92] *What is a Cryptocurrency? A Beginner's Guide to Digital Money*, *supra* note 13.

in the same order by every validator.[93] The validator's role is to take the transactions, validate them, and add them to a block.[94] However, validators often "hear" of transactions at different times or choose to pursue different transactions.[95] This results in each individual validator constructing a unique block of validated transactions. The community then decides which block shall be added to the Blockchain ledger through establishing consensus.

The nonlinear process of adding transactions to a block, and thus the Blockchain, provides more flexibility for regulators to approve transactions during this validation period. Until a regulator approves of a suspect transaction, no consensus can be agreed upon for its addition to a block or the Blockchain.

Opponents to this suggestion may refer to the difficulty of executing this in a proof of work setting. Validators receive their reward by being the first to finish their block. If specific transactions require additional screening prior to validation, this would deter validators from choosing to validate that specific transaction. The solution to this concern is merely that validators will not know whether a transaction requires additional screening prior to choosing to validate it. The additional screening requirements will be discovered through the validation process. In this way, the "blind" selection of potentially lengthy validation times will be equally distributed to the pool of validators.

VI. PENDING REGULATIONS AND LEGISLATION

Throughout the last calendar year, there have been several new iterations of cryptocurrency regulation proposals. FinCEN released a Notice of Proposed Rulemaking ("NPRM") in December of 2020 and Representative Don Beyer released proposed legislation in July of 2021, among a dozen others. However, each of these regulation attempts does not patch the existing holes in the regulatory framework. FinCEN's NPRM and Representative Beyer's legislation

[93] Hupayx, *supra* note 35.
[94] *Id.*
[95] *Id.*

are analyzed below to demonstrate the importance of focusing on the validator role to generate effective cryptocurrency regulation.

A. FinCEN 2020 NPRM

In December 2020, FinCEN issued a Notice of Proposed Rulemaking extending its regulatory oversight of cryptocurrency to include unhosted wallets.[96] FinCEN's proposed rule would require banks or other money service businesses to maintain records for transactions with unhosted wallets.[97] The new reporting standards would add requirements for cryptocurrency transactions amounting to $10,000 or more.[98] Additionally, if a customer transacted with an unhosted wallet in an amount greater than $3,000, the money service business or bank must record cryptocurrency transactions, which includes verifying the identities of their customers.[99] The inclusion of regulations surrounding unhosted wallets tremendously assists in the identification of bad actors in the transaction space.

Several issues exist with this proposed rule. The first issue is the lack of inclusion of transactions between two unhosted wallets. If an individual owns a wallet unaffiliated from a financial institution, there would be no oversight available to screen for potential money laundering or terrorist financing activity. This is a very accessible loophole for bad actors to avoid regulatory oversight. The second issue is the simple disagreements regarding the application of the money service business classification to different cryptocurrency actors. It is disputed whether cryptocurrency transactions may reside under the money service businesses definition, indicating contention over whether there may be Bank Secrecy Act jurisdiction at all.

However, if FinCEN focused on validators who encountered the respective $10,000 or $3,000 thresholds within transactions with a

---

[96] THE FINANCIAL CRIMES ENFORCEMENT NETWORK PROPOSES RULE AIMED AT CLOSING ANTI-MONEY LAUNDERING REGULATORY GAPS FOR CERTAIN CONVERTIBLE VIRTUAL CURRENCY AND DIGITAL ASSETS TRANSACTIONS, U.S. DEP'T OF THE TREAS. (Dec. 2020), https://home.treasury.gov/news/press-releases/sm1216 [hereinafter FinCEN Proposed Rulemaking].

[97] FinCEN Proposed Rulemaking, *supra* note 96.

[98] *Id.*

[99] *Id.*

hosted or unhosted wallet, FinCEN would be alerted to *all* transactions within this range. Validators must exist for cryptocurrency transactions to exist on a Blockchain, regardless of whether an entity utilizes a hosted or unhosted wallet, or is a user, exchanger, or administrator.

B. Representative Beyer's "Digital Asset Market Structure and Investor Protection Act"

In July of 2021, Representative Don Beyer introduced a new bill to regulate digital assets. The relevant component of this bill is Title IV, pertaining to the BSA. The bill suggests adding "digital assets" to 31 U.S.C. § 5312(a)(3)(b).[100] This section describes the type of monetary instruments that are regulated under the BSA.[101] The inclusion of "digital assets" here reflects FinCEN's inclusion of cryptocurrency under the phrase "or other value that substitutes for currency" when discussing money transmission services.[102]

In addition, the bill suggests the addition of a "virtual asset service provider" under the types of financial institutions to be regulated by the BSA.[103] The definition of a "virtual asset service provider" is a person who

> (i) exchanges between digital asset and fiat currencies; (ii) exchanges between digital assets; (iii) transfer of digital assets; (iv) is responsible for the custody, safekeeping of a digital asset or an instrument that enables control over a digital asset; (v) issues or has the authority to redeem a digital asset; and (vi) provides financial services related to the offer or sale of a digital asset by a person who issues such digital asset.[104]

The description of a virtual asset service provider parallels a cryptocurrency exchange operating with hosted wallets. The provider exchanges between assets and is responsible for the custody of digital

---

[100] Digital Asset Market Structure and Investor Protection Act, H.R. 4741, 117th Cong. (2021).
[101] *Id.*
[102] *FINCEN 2019 GUIDANCE*, *supra* note 11.
[103] H.R. 4741 § 404.
[104] *Id.*

assets. This is precisely what exchanges utilizing hosted wallets offer. As established, cryptocurrency exchanges qualify as money transmitters under the BSA. It is unclear what this bill adds to the regulatory component of cryptocurrency aside from providing crystal clear clarification about the regulatory status of cryptocurrency exchanges.

Further, the bill directs "financial institutions to prohibit any person from engaging in any transactions that involve digital assets . . . and (A) anonymizing services; (B) money mules; or (C) anonymity-enhanced convertible virtual currencies."[105] This merits discussion as subsections (A) and (C) prohibit financial institutions from dealing with cryptocurrencies that enhance anonymity features.[106] Some of these cryptocurrencies are referred to as dApps, or decentralized applications.[107]

For example, a cryptocurrency known as Monero utilizes "stealth addresses" on its Blockchain.[108] Stealth addresses are one-time addresses, contrasting with the use of a consistent public wallet address when dealing with Bitcoin transactions.[109] The use of one-time addresses prevents the ability to track the transactions stemming from one entity as it is tremendously difficult, if not impossible, to link the transactions. The instruction for financial institutions to prohibit the use of such anonymous cryptocurrencies will not diminish the use of such cryptocurrencies. The entities set on utilizing the immense privacy and security benefits will continue to do so outside the scope of financial institutions or exchanges. This example highlights the necessity of the use of validators to conduct cryptocurrency screening.

[105] *Id.*
[106] *Id.*
[107] Jake Frankenfield, *Decentralized Applications – dApps*, INVESTOPEDIA (June 22, 2021), https://www.investopedia.com/terms/d/decentralized-applications-dapps.asp.
[108] *FAQ*, MONERO, https://www.getmonero.org/get-started/faq/#anchor-different (last visited Oct. 26, 2021).
[109] *Id.*

C. The Vital Necessity for Validator BSA Requirements

The approaches by FinCEN and Representative Beyer attempt to regulate cryptocurrency transactions by drawing lines between the types of transactions susceptible to oversight and those that are not. If the purpose of cryptocurrency regulation is to prevent financial crime, terrorism financing, or other national security concerns, leaving gaps in the cryptocurrency regulation is counterproductive. Bad actors will continue to utilize the payment methods least likely to be detected by law enforcement. Instead of deciding where the line must be drawn between different types of transactions, cryptocurrencies, or entities, the focus is best set on the universal component of cryptocurrency transactions: the validator.

Blockchain transactions cannot exist without a third-party validator. Imposing a screening requirement on validators who already verify ongoing transactions does not overly burden the process. Adding validators as a type of financial institution under the BSA would ensure every transaction on a Blockchain is screened for potentially suspicious activity without inviting law enforcement or regulators directly into the Blockchain; thus, protecting the privacy of many users of cryptocurrency value.

CONCLUSION

Cryptocurrencies are a tremendous technology; they afford individuals the privacy of transacting in cash with the speed of digital transactions. However, the pseudonymity associated with these transactions creates tempting environments for bad actors wishing to engage in financial crime. The severe risk of terrorist financing is exacerbated by the ability to transact anonymously without regulatory oversight. The example provided of the Department of Justices' seizure of millions in cryptocurrency dedicated to financing terrorist organizations proves the existence of cryptocurrency's use in this capacity. Without providing a secure method of classifying virtual currencies under existing BSA regulations, bad actors will be able to maneuver around the selective regulations. If the use of cryptocurrency for terrorist financing grows, it will become

increasingly difficult for law enforcement to monitor transactions to protect the nation.

The selection of validators to execute the oversight responsibilities ensures a thorough screening of all cryptocurrency transactions occurring. Additionally, it does not upset the current function of the cryptocurrency validation process. If regulators continue to focus on methods to classify cryptocurrency transactions under the money service business definition or through cryptocurrency exchanges, there will always be transactions out of reach of the screening process. Validators are necessary to the proper functioning of the cryptocurrency peer-to-peer payment systems regardless of how these systems evolve.

The purpose of creating this regulatory oversight is to provide law enforcement the ability to protect the nation and its infrastructure from potential financial crime, from money laundering to terrorist financing. Every industry has experienced an increase in its dependency on technology over the last decade, and the prevalence of cyberattacks on this infrastructure has significantly increased as well. If bad actors can silently perform transactions with individuals around the world without any risk of recourse, this dramatically increases the likelihood of unprepared responses to targeted incidents against the nation. The use of validators to constantly screen for potential bad actors before validating each transaction provides a protective barrier against financial crime or national security threats without eradicating the privacy protections for cryptocurrency users.