Director Kenneth A. Blanco,
Financial Crimes Enforcement Network
P.O. Box 39
Vienna, VA 22183

Re: Comments to the Financial Crimes Enforcement Network on Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets

FinCEN Docket No. FINCEN-2020-0020, RIN 1506-AB47

January 4, 2021

Dear Director Blanco:

This letter serves as our comments on the proposed Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets, published on Dec 23, 2020. We specifically address the enhanced reporting and record keeping requirements proposed for MSBs involved in blockchain-based CVC and LTDA transactions. While we appreciate the opportunity to respond, the abbreviated comment period has precluded a fulsome discussion of the questions we raise below. Further time to research and evaluate the complexities and market impact of these rules is required to ensure a sound and effective framework for detecting and deterring illicit finance while maintaining a competitive marketplace for CVC and LTDA services.

Dr. Neha Narula is the Director of the Digital Currency Initiative at the Massachusetts Institute of Technology's Media Lab. She is an academic researcher in computer systems, cryptocurrency, and distributed ledger technology, has published in top conferences on computer systems and information security, and has served on numerous program committees. Her team at MIT is engaged in research to design, build, and test hypothetical central bank-issued digital currency. She contributes to the development of Bitcoin Core, the most widely-used implementation of Bitcoin node software. She is not an investor, advisor, or board member of any cryptocurrency company or foundation.

Patrick Murck is an Affiliate at the Berkman Klein Center for Internet & Society at Harvard University and Chief Legal Officer at Transparent Financial Systems. He also serves as a member of the High Level Advisory Group on Fintech for the International Monetary Fund, the Fintech Advisory group for the Federal Reserve Bank of New York, and the Fintech Working Group for the Massachusetts Securities Division. Patrick co-founded and was Executive Director of the Bitcoin Foundation and has founded, invested in and advised numerous Fintech startups. Through this work he has advised regulators and policymakers around the world on the risks and benefits of cryptocurrency and blockchain technology, including presentations to the Bank Secrecy Act Advisory Group.

We are submitting these comments in our personal capacity and not on behalf of any of the organizations listed above.[1]

We believe there are many benefits to treating blockchain-based CVC and LTDA as monetary instruments, among them enhanced regulatory clarity and integration into existing principles-based regulatory frameworks (including CTR requirements) on equal footing with any other monetary instrument or cash. However, the discordant record-keeping requirements and requirements to identify both the sender and recipient of a transaction are problematic from a technical perspective. Further, like many technology-specific rules, this proposal could distort the market for CVC and future LTDA services and put the US at a disadvantage economically, thereby degrading our financial surveillance capabilities. Additionally, the rule could further hem in the design and innovation of blockchain-based or cryptographic "digital dollars" (whether issued by the Federal Reserve or private actors) at a time when development in these approaches is nascent, potentially putting the future dollar at a competitive disadvantage as compared to other sovereign money.

We urge FinCEN to extend the comment period to the normal sixty (60) days usually afforded such rulemaking notices to allow for further research and discussion of these and the many other substantive points that have been articulated in the comments filed in response to proceeding. Given the unusually brief window (amounting to a mere six (6) business days due to the holidays) to assess and respond to these proposed rules, we are concerned that many stakeholders will not have time to fully express their views. Our comments also reflect the lack of time needed to fully research and assess the impact of these proposed rules; we would welcome the opportunity to follow up with more complete comments given the opportunity.

1. The Proposed Rule Misunderstands Blockchain Addresses

We must be careful not to prematurely map new technology onto existing frames of reference. The proposed rule, unfortunately, makes this mistake by assuming that cryptocurrency transactions are merely payments from one person or entity to another.[2] Many others have written comments in response to the proposed rule pointing out that MSB customers can also send payments to "smart contracts." Here we seek to expand on this point and show why thinking of cryptocurrency transactions as only payments from one legal entity to another is

[1] Special thanks to Thomas Hopkins, Harvard Law School class of 2021, for help in drafting this comment.

[2] Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets, 84 Fed. Reg. 83,840 (Dec. 23, 2020) (to be codified at 31 C.F.R. pts. 1010, 1020, and 1022), https://www.federalregister.gov/public-inspection/2020-28437/requirements-for-certain-transactions-involving-convertible-virtual-currency-or-digital-assets. The first paragraph states: "To transfer an asset on a blockchain, a person enters an alphanumeric code known only to the transferor (a private key) into a cryptographic hash function enabled by the network software, which allows the transferor to request that the network software validate a new entry on the ledger showing that control of an asset has been assigned to the recipient. Once the network has validated this transfer, the ledger is altered and the recipient may transfer the asset to another recipient using their own private key. Ledger entries are cryptographically secured, and accounts are identified on a blockchain by alphanumeric 'public keys'—not by the owner's name." This is incorrect, as it only describes one type of transaction possible in a cryptographic CVC.

limiting.[3] Cryptocurrencies truly operate in a different paradigm than traditional financial transactions.

A cryptocurrency transaction does not necessarily transfer coins to an address that maps onto an existing person or entity, known at the time of transaction creation. In cryptocurrencies like Bitcoin, coins are transferred into a conditional statement specified in the form of a short *script* or set of computer instructions*.* This script serves as an escrow for the coins, noted on the blockchain ledger maintained by the distributed computer network. Whoever can satisfy the specified script by providing the appropriate data can not only prove to others that they have the capability to then transfer those coins (temporarily, without necessarily actually transferring them, and not to the exclusion of others), they can supply data to the network in a second transaction to try to take the coins and transfer them further. Note that just because someone produces this second transaction it does not mean that they will actually succeed in taking the coins; their second transaction must first be confirmed in the blockchain. Someone else who can also produce the data (or other valid data) might get their transaction confirmed first, taking the coins. Importantly, the creator of the original transaction *might not even know exactly how the coins will be redeemed, or by whom*. For these types of transactions, it can be difficult or impossible to determine the recipient at the time the original transaction is created, or even at the time it is confirmed in the blockchain. These transactions are common in almost all cryptocurrencies, including Bitcoin and Ethereum. This type of functionality, transferring funds conditionally without a trusted third party (commonly known as “smart contracts”), is what makes programmable money such an exciting new technology.[4]

The most common script in use to date in Bitcoin is indeed the one that mimics traditional payments and transfers coins to a public key.[5] The coin is transferred into a script which specifies a public key, the owner of which can redeem the coins and transfer them further.[6] This is the use case to which the proposed rulemaking speaks. However, other interesting and important use cases require transferring coins into more complex scripts. One widely-used example of these more complex scripts has quickly become best practice for custody of blockchain-based CVC. In this approach, the owner of the coins creates a transaction which transfers her bitcoin on the blockchain into a script specifying that in order to move the funds *later*, two authorizations must jointly sign a new transaction to transfer the coins (presumably done by two separate people or entities). This is known as *multisig*[7] and is equivalent to figuratively putting the coins into a lockbox escrow which can only be opened by a two-person

[3] One might think that it is possible to, for example, name the author of the smart contract as the recipient. These comments demonstrate why this is not the case.

[4] Deutsche Bundesbank, *Money in programmable applications: Cross-sector perspectives from the German economy*, (December 21, 2020), https://www.bundesbank.de/resource/blob/855148/ebaab681009124d4331e8e327cfaf97c/mL/2020-12-21-programmierbare-zahlung-anlage-data.pdf.

[5] In Bitcoin, this type of spend is known as a Pay to Pubkey Hash (P2PKH). Over 50% of outstanding Bitcoin is currently in this state. *See* TXStats, *Pay to Pubkey Hash Statistics*, https://txstats.com/dashboard/db/pay-to-pubkey-hash-statistics?orgId=1 (last visited Jan 4, 2021).

[6] Other commenters have noted that it can be difficult to reliably associate a person or entity with a public key, with which we agree. This comment goes further to show that even if that were straightforward, the potential recipient in a transaction might not be able to be determined at the time the transaction is confirmed, and possibly indefinitely.

[7] *Multisignature*, Bitcoin Wiki, https://en.bitcoin.it/wiki/Multisignature (last visited Jan 4, 2021).

nuclear launch procedure: In order to authorize a launch (transfer the coins), two soldiers must each turn a key (provide a cryptographic signature) at the same time. This gets even more complicated when a script specifies that, for example, some two-out-of-three authorization is required. As an example, Figure 1 shows a transaction where Alice has instructed Coinbase, on her behalf, to transfer her bitcoin to a two-of-three multisig which can be redeemed by any two of Alice, Bob, and Charlie.[8] The transaction is confirmed on the Bitcoin blockchain. But who is the recipient of the bitcoin in Coinbase's transaction? All three of Alice, Bob, and Charlie? All joint combinations of two out of the three? Note it's possible none of Bob, Charlie, or Dave are customers of Coinbase, and that no user is capable of moving the coins alone.

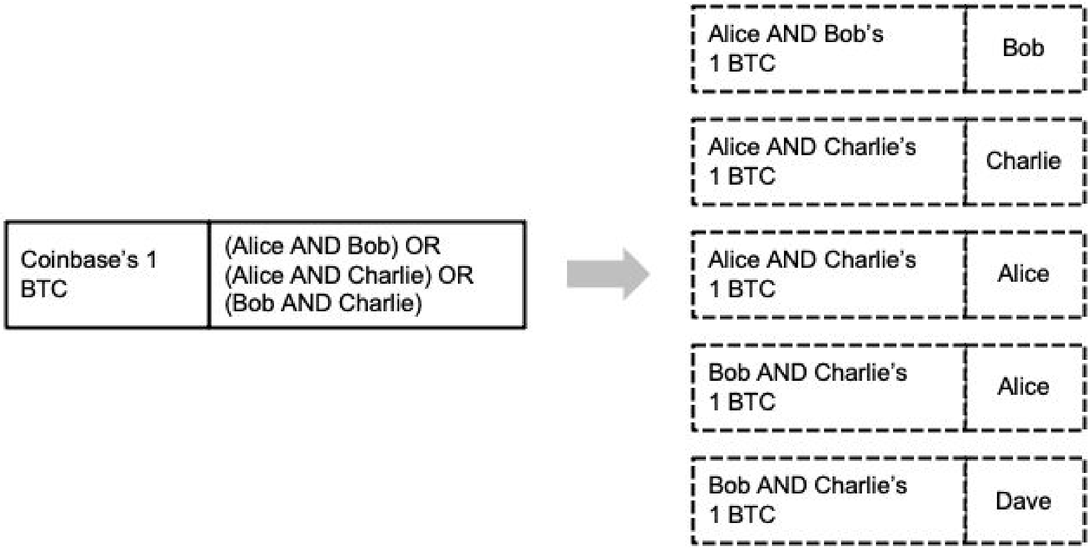
Coinbase's 1 BTC
(Alice AND Bob) OR (Alice AND Charlie) OR (Bob AND Charlie)
Alice AND Bob's 1 BTC
Bob
Alice AND Charlie's 1 BTC
Charlie
Alice AND Charlie's 1 BTC
Alice
Bob AND Charlie's 1 BTC
Alice
Bob AND Charlie's 1 BTC
Dave

Figure 1. Each transaction designates the source and recipient. Alice has previously deposited her bitcoin in an account at Coinbase. She instructs Coinbase to transfer her 1 BTC to a 2-of-3 multisig with Alice, Bob, and Charlie, resulting in Coinbase issuing the transaction on the left which gets confirmed on the Bitcoin blockchain. The transactions on the right are *possibilities* for how this bitcoin might be redeemed and further transferred; note that at the time Coinbase creates its transaction, it cannot know exactly which (if any) of the transactions on the right will eventually be created and confirmed.

In this example, there are only three participants. Multisigs in Bitcoin can currently contain combinations up to 15 participants, and there are proposed upgrades to Bitcoin which could increase this number significantly.[9] Users in Bitcoin can apply many more types of conditions on their funds, including locking them up for a period of time. Do MSBs have to record and retain specific records for anyone that *may* have the ability to transact, whether or not they ever take custody or control of the monetary instrument? Should an MSB file a CTR on anyone that *may potentially* be a future recipient of monetary instruments?

These types of transactions are not gimmicks or evidence of illicit activity: they are best practices and critically important for securing one's cryptocurrency and keeping it safe from

[8] "Bob" and "Charlie" might be custodians who help secure cryptoassets.
[9] Peter Wuille, Jonas Nick & Tim Ruffing, *Schnorr Signatures for secp256k1*, Github (Jan. 19, 2020), https://github.com/bitcoin/bips/blob/master/bip-0340.mediawiki.

would-be attackers.[10] More than 818,000 bitcoins have been redeemed through multisig transactions.[11] It is most certainly the case that many more bitcoins are *currently* locked up in multisig escrow, but due to Bitcoin's design this does not become visible until the bitcoins are further transferred out of the escrow.[12] Beyond Bitcoin and other cryptocurrencies, these techniques will almost certainly be critical in the design of central bank digital currency (CBDC) and other LTDA systems.

The most exciting potential use cases of the technology involve transferring coins into even more complex smart contracts or scripts. For example, consider a use case where Alice enjoys doing Sudoku puzzles but has come across one she cannot solve. Alice might post the puzzle publicly on the internet and ask for a solution, offering to pay a fee to whomever can supply an answer. Bob sees the puzzle and has a solution—but there remains counterparty risk: should Alice pay Bob first, or should Bob give Alice the solution first? Alice and Bob are both strangers, and either might renege after the other has gone. It also might be difficult to find a mutually trusted third party to escrow the solution and funds, and the third party would introduce new counterparty risk. This is the classic problem of *fair exchange*.[13]

Blockchain-based cryptocurrencies provide an answer to the fair exchange problem without relying on a trusted third party to escrow the solution and payment. A coin may be transferred into a script escrowing the funds on the blockchain attached to a pre-specified question. This was demonstrated on Bitcoin in 2016 with a *zero-knowledge contingent payment*.[14] The user transferred bitcoin into a script which specified a Sudoku puzzle. Later, a different user presented a transaction and some auxiliary data which simultaneously provided the answer to the puzzle and claimed the bitcoin (by creating a new transaction that transferred the bitcoin into an address under his control). In this type of scenario, at the time the initial transaction (specifying the puzzle) is created, the *transaction creator does not know who will actually claim the coins, if anyone at all*.

We have described in detail how transactions in Bitcoin can be conducted without a well-specified recipient; Ethereum supports even more complex, but useful, smart contracts in

[10] Digital asset wallets such as Bitgo (https://www.bitgo.com/services/custody/wallet-platform/) and GreenAddress (https://greenaddress.it/en/) that require multiple digital signatures provide enhanced security to their users. Access to multisig wallets requires that all stakeholders are compromised at the same time, which mitigates security risks.

[11] TXStats, *P2SH repartition by type,* https://txstats.com/dashboard/db/p2sh-repartition-by-type?orgId=1 (last visited Jan 4, 2021).

[12] The current best practice for creating multisig transactions uses Pay to Script Hash (P2SH) addresses. In this type of transfer, the script (the requirement for multiple signatures) is not revealed on the chain until the coins are transferred *out* of the multisig escrow. 30% of all Bitcoin are currently in P2SH addresses, *see* TXStats, *P2SH statistics*, https://txstats.com/dashboard/db/p2sh-statistics?orgId=1 (last visited Jan 4, 2021), and 60% of P2SH addresses are currently unspent, *supra* note 11, so it is possible up to 18% of all outstanding Bitcoin is in this type of multisig escrow.

[13] For more discussion of this example, see Matteo Campanelli et al., *Zero-Knowledge Contingent Payments Revisited: Attacks and Payments for Services*, http://stevengoldfeder.com/papers/ZKCSP.pdf. One could imagine more useful applications for science and commerce such as the Netflix Prize. https://en.wikipedia.org/wiki/Netflix_Prize.

[14] Gregory Maxwell, *The first successful Zero-Knowledge Contingent Payment* (Feb. 26, 2016), https://bitcoincore.org/en/2016/02/26/zero-knowledge-contingent-payments-announcement/.

which it is challenging if not impossible to identify a recipient.[15] The proposed rule as written would prohibit MSBs from supporting this *entire class* of customer transactions. This would make transacting with CVCs and LTDAs less secure and greatly inhibit the innovation and growth of this exciting new technology.

2. These Technology-Specific Rules Could Distort the Market and Degrade US Competitiveness

It is generally understood that principles-based regulation is preferable to technology-specific regulation.[16] Principles-based regulation promotes innovation and competition, while technology-specific regulation may create market inefficiencies, and risk obsolescence. Blockchain-based CVC like Bitcoin and Ethereum create opportunities for meaningful innovation in both financial and non-financial sectors because they are open networks, much like the design of the Internet. However, there is a clear risk that, like the Internet,[17] these open networks will come to be dominated by a handful of firms that close off competition and innovative business models.[18] Technology-specific rules like the ones proposed here risk ossifying the dominant market position of a few incumbent MSBs who already have tailored compliance infrastructure in place and will benefit from early data-collection efforts; this could be bad for consumers by stifling competition. In order to avoid repeating the failure to promote a competitive market for Internet infrastructure and services, further analysis, research and discussion is critical.

Applications built on blockchain technology that aren't primarily engaged in the creation or transmission of monetary instruments may also be caught up in and stymied by these regulations. Unique models and methods for peer production and cooperative ownership are emerging from open blockchain networks.[19] As noted above, the architecture of these applications may not readily lend itself to a simple "one address equals one person" approach to identity and risk mitigation. MSBs may not be able to support or interact with these new applications, making it more difficult for these innovative new business models to compete. Further, to the extent MSBs are able to interact with these applications, identification and

[15] Note that since these blockchains are publicly readable, transactions can be traced after the fact to find and prevent future illicit activity.

[16] *See, e.g.*, Press Release Number 8081-19, CFTC, Op-ed by Chairman Heath Tarbert, *ICYMI: Fintech Regulation Needs More Principles, Not More Rules* (Nov. 19, 2019), https://www.cftc.gov/PressRoom/PressReleases/8081-19.

[17] Consider antitrust lawsuits recently filed against tech giants Google (https://www.justice.gov/opa/pr/justice-department-sues-monopolist-google-violating-antitrust-laws), Facebook (https://www.ftc.gov/news-events/press-releases/2020/12/ftc-sues-facebook-illegal-monopolization), Amazon (https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2077), etc.

[18] Advertising-based surveillance capitalism came to be the dominant form of Internet economics, rather than peer production or direct user monetization. In the cryptocurrency market, we see some troubling trends in this direction.

[19] Unique use cases for blockchain technology do not necessarily involve the exchange of monetary instruments. Many non-financial use cases exist, including non-fungible tokens (NFTs) that use blockchain to identify ownership of unique assets, *see Nonfungible tokens; Quick Guide*, Cointelegraph, https://cointelegraph.com/magazine/nonfungible-tokens/#NFT-use-cases, and decentralized storage tokens (DSN) that use blockchain to allow peer sharing of cloud storage space (for example, SIA https://sia.tech/about, and Filecoin https://filecoin.io/) to name just a few.

record-keeping requirements may expose non-financial users to unwarranted surveillance. FinCEN should take care to allow for continued business model innovation and competition between blockchain-based services and their counterparts in traditional markets (including advertising-based internet services).

Most concerning, these rules could encourage more economic activity to "go dark," negatively impacting MSBs' ability to adequately surveil and interdict illicit financial activity. The enhanced reporting and record-keeping requirements that would be required of MSBs under this rule could encourage users[20] of blockchain-based CVC to migrate to off-shore and "non-custodial"[21] exchanges, depriving FinCEN and law enforcement of valuable tools to prevent criminal activity and money laundering. FinCEN would be wise to heed Ernie Allen, former President and CEO of the International Center for Missing and Exploited Children, when he testified before the Senate Homeland Security and Governmental Affairs Committee: "You [Congress] can ensure that the response of government to this fragile, emerging area is not so draconian that the effect is simply to push these new enterprises outside the United States to countries where there is little or no regulation."[22] It is in the best interests of FinCEN to encourage a robust, competitive US-based market for CVC and LTDA services as this will lead to greater surveillance and tools for interdiction of illicit finance, money laundering and terrorist financing.

3. These Rules Could Deter Innovation in "Digital Dollars" and Central Bank Digital Currency

There is a tremendous amount of interest from central banks in investigating the direct issuance of digital currency built on a cryptographic platform and with programmable features.[23] However, innovation in digital dollars and central bank digital currency (so-called "Legal Tender Digital Assets") is nascent, and currently no MSBs are providing related services. Yet the proposed rule is already establishing that digital dollars will be treated differently from analog dollars. This is putting the cart before the horse. There are many technical and policy discussions yet to happen, including those around a proper balance between surveillance and privacy as well as data collection and retention and cyber risks. Establishing rules now would preempt these discussions and foreclose innovation that could lead to better tools to detect and deter illicit finance with less cyber risk and intrusion on privacy.

[20] As other commentators have noted, there are significant privacy and personal security concerns arising from the data collection and retention that would be required of MSBs under these proposed rules, particularly linking identity and physical addresses to blockchain wallets.

[21] "Non-custodial" or "decentralized" exchanges do not use intermediaries to provide custody of funds or to execute trades. Instead, they provide a forum for third parties to consummate the trade themselves, and are exempt from money transmitter status. *See* FinCEN Guidance FIN-2019-G001, "Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies," pp. 23–24 (May 9, 2019), https://www.fincen.gov/sites/default/files/2019-05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf.

[22] Testimony of Earl Allen for the United States Senate Committee on Homeland Security and Governmental Affairs, *"Beyond Silk Road: Potential Risks, Threats and Promises of Virtual Currencies"* (Nov. 18, 2013), https://www.hsgac.senate.gov/imo/media/doc/Testimony-Allen-2013-11-18.pdf.

[23] *See* Codruta Boar et al., *Impending arrival--a sequel to the survey on central bank digital currency*, Bank for International Settlements (Jan. 2020), https://www.bis.org/publ/bppdf/bispap107.htm.

The disparate treatment of digital dollars to analog dollars may make any future US CBDC or other LTDA less appealing as compared to other nations' CBDC projects, like the digital yuan or a digital euro. The US has enjoyed the benefits of the dollar's status as the global reserve currency, but it should not be complacent. It is of vital economic and national security interest that the US maintain the position of the dollar in the global economy. FinCEN should take care not to limit the potential for innovation in this area by projecting rules onto undefined future technologies and services.

In Conclusion

We appreciate FinCEN's continued approach to providing clarity for MSBs and other market participants involved in blockchain-based CVC and the development of future LTDAs. In particular, we generally support technology-neutral rules that would treat CVC and LTDAs as monetary instruments including the requirement to file CTRs. However, we are concerned with the technology-specific approach that these particular proposed rules have taken, in particular the assumption that blockchain addresses directly map to individual persons or entities. The rules as tailored to blockchain technology are simply not coherent.

We have further concerns these rules could blunt the greatest potential for blockchain technologies by distorting the market for CVC and LTDA services, pushing the market structure in a direction that replicates the concentration and reliance on platforms that we see in traditional finance (and repeating the mistakes of the Internet economy). The proposal would impact innovation beyond MSBs regulated by FinCEN. Lastly, FinCEN should not proactively regulate technology that does not yet exist and is still being designed. There is no benefit to FinCEN trying to divine the future of digital dollars. There is, however, substantial risk that premature action now will foreclose innovative new approaches to detecting and deterring illicit finance and could undermine the US efforts to maintain the status of the dollar in the global economy in years to come.

In addition to asking you to consider our comments herewith, we reiterate our concern that the abbreviated notice and comment period has precluded a meaningful and thoughtful analysis of these proposed rules. We encourage FinCEN to reconsider a longer comment period that would allow for a fulsome analysis of the questions presented by us and others. We would look forward to further dialog and expanding on the brief comments we have submitted today.

Thank you for your time and attention.

Sincerely,

/s/ Neha Narula
Neha Narula

/s/ Patrick Murck
Patrick Murck