Policy Division
Financial Crimes Enforcement Network
P.O. Box 39
Vienna, VA 22183

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

To whom it may concern:

Blockchain Capital is one of the oldest and most well-known venture capital firms in the blockchain / cryptocurrency industry. Over the last nearly eight years, we have made over 90 investments in companies building and servicing decentralized protocols or creating digital assets. We have deployed and manage nearly $500 million dollars for a broad set of investors predominantly residing in the United States, including financial institutions, corporate strategic investors, endowments and high net-worth individuals. We have a team of 15 professionals who operate out of an office in downtown San Francisco, California. Our perspective as investors exclusively in this burgeoning digital asset industry is unique in that we do not simply own and transact with certain convertible virtual currencies ("CVCs") or work on a single specific protocol or distributed ledger; rather, we interact with hundreds of innovators and developers on a yearly basis and have reviewed thousands of projects during our tenure in the industry. As such, we are very familiar with the extremely complex and often idiosyncratic challenges that attend to developing, custodying, transacting in and regulating digital assets. It is with this extensive experience that we write this comment on FinCEN's proposed rule to implement new recordkeeping requirements for CVC transactions over $3,000 and apply existing currency transaction report (CTR) requirements to CVC transactions over $10,000 (the "Proposed Rule").

We believe in the importance of an open, free, fair and safe global financial ecosystem that allows for increased financial access and innovation as well as protection from nefarious actors and illicit financial activity. The role of FinCEN and regulated financial institutions in supporting the integrity of our financial and payments systems is paramount, and combating money laundering, terrorist financing and other illicit financial activity is critical to the ongoing health and growth of an evolving financial infrastructure. However, regulations aimed at protecting our financial infrastructure must be appropriately tailored to both effectively combat illicit activity while also protecting individual freedoms and promoting innovation. We are deeply concerned that, if implemented, the Proposed Rule would have substantial adverse effects both to the United States public via the imposition of unprecedented burdens on privacy and restrictions on financial access and on this innovative industry still in its infancy via an unreasonably high cost of compliance and a resultant dampening of innovation here in the US. We believe the rule as proposed is both faulty and ineffective in a plethora of respects, which we discuss below, and accordingly, we request that FinCEN abandon the Proposed Rule.

1. **The Proposed Rule unduly infringes on financial privacy and limits financial access while also hampering law enforcement efforts to combat illicit financial activity.**

You have requested comment on whether the Proposed Rule strikes a reasonable balance between financial inclusion and consumer privacy on the one hand and combating illicit financial activity on the other. It is our strong view that the Proposed Rule fails to strike this balance quite substantially. The scope of information required by the Proposed Rule and the way in which this information allows for extensive identification of individuals and their financial transactions beyond the specific transactions contemplated by the Proposed Rule would allow both regulated commercial entities and the federal government to have unprecedented access to uniquely auditable information about an individual's financial transactions using CVC. The Proposed Rule would require banks and money services business ("MSBs") (collectively, "Financial Institutions" or "FIs") to record, in the case of transactions with "unhosted wallets" in amounts greater than $3,000, or to directly report to FinCEN, in the case of transactions with unhosted wallets in amounts greater than $10,000, identifying counterparty information for each such transaction that includes a "minimum" of the name and physical address of the FI's client's counterparty in the transaction (the "Recording and Reporting Requirements").

This requirement in itself imposes greater informational recording and reporting obligations for CVC payments than are required for legacy payment systems. When a Financial Institution engages in a transaction with its client using the legacy payment system in any amount, there is no requirement that the Financial Institution record or report identifying information for any prospective *counterparty* of the client. For example, when an individual withdraws $4,000 from an account with a Financial Institution, that FI is not required to verify and record the name and address of the prospective recipient of that $4,000. That prospective recipient could be physically waiting outside of the bank to receive that $4,000. This is also the case with legacy currency transactions greater than $10,000 where FIs are required to record and report identifying information of the individual client making such a withdrawal but not demand any information on the subsequent recipient of that $10,000. This, of course, is highly concerning because the Proposed Rule is not technology neutral but rather unfairly prejudices users of CVC and the Financial Institutions that serve them without providing any justification for this prejudicial treatment.

Prejudicial treatment under a regulatory regime is alarming in and of itself; however, because of the nature of blockchain technology, the Proposed Rule would also result in unprecedented opportunities for the financial surveillance of private citizens by both corporate entities and the federal government. The vast majority of CVCs represent digital assets that are native to one form of public, permissionless peer-to-peer distributed ledger or "blockchain" or another. Users of CVCs transact by authorizing transfers of digital assets under their control via the "ownership" of an alphanumeric private key by "signing" their private key to a cryptographic hash function, instructing the transfer to an alphanumeric public address (or "wallet"), which the network then validates. Currently, when a Financial Institution completes a transfer to an unhosted wallet, the Financial Institution has two pieces of information (apart from the KYC on the FI's account holding client): (1) the unique transaction hash and (2) the public wallet address of the transaction counterparty (which may or may not be the FI's account holding client). The Proposed Rule would add (3) the name and (4) the address of the owner of the receiving or sending wallet. The combination of these four pieces of personally identifiable information is extremely invasive because it allows the holder of such information (the FI or, in some cases, the federal government without warrant or cause) to have additional and extensive information about the individual wallet holder, i.e. the transaction counterparty, and his, her or its financial holdings and

activities on the blockchain record far beyond the particular transaction subject to the Proposed Rule. An individual's name and address coupled with the hash of the transaction and their wallet address would allow anyone (FI or government) to identify not only the transaction in question but also all prior transaction involving that wallet and all future transactions involving that wallet, resulting in a level of financial surveillance not ever before seen in American society. This information would be obtainable whether those prior or future transactions are subject to the Proposed Rule and whether or not such transactions were of an illicit nature. We emphasize that these pieces of information would result in such unprecedented access to data *because* of the auditable and transparent nature of public blockchain networks.

This indeed would be a powerful tool for policing illicit users and uses of CVC; however, it would also be a powerful tool for manipulation of personal data and information for corporations or abuse by central governments. Further, it would create massive centralized depositories of personal data that would be vulnerable to leaks or hacks, putting CVC users in enormous potential danger. We do not believe that the Treasury has shown that the severity and frequency of the threat of illicit uses of CVCs reasonably justifies such a massive incursion on individual privacy.

We also believe that the Proposed Rule will have significant unintended consequences for financial access with respect to underrepresented populations in the US. The requirement that the owner of the counterparty wallet provide a physical address would prevent potentially several million US persons from being able to engage in digital asset transactions with regulated FIs and their clients. Many US persons lack a physical address and many of those who do are part of underrepresented or marginalized populations.[1] One of the hallmarks of blockchain technology and CVCs is the opportunity to allow for greater financial access to all US persons regardless of class, socioeconomic status, geographic location or any other distinction. The implementation of this rule would significantly jeopardize that opportunity. In addition to millions in the US who would potentially be excluded from an entire technological ecosystem, there are an estimated billions of individuals around the world who lack a physical address.[2] Unfortunately, the Proposed Rule would have the effect of diverting a growing number of CVC uses away from regulated US financial institutions likely toward disfavored, non-regulated service providers, not for nefarious reasons but simply from a literal inability to comply with unreasonably burdensome informational requirements.

2. The Proposed Rule is substantively vague in its application and will lead to unintended consequences.

In addition to the Recording and Reporting Requirements, the Proposed Rule also requires FIs to "follow risk-based procedures to determine whether to obtain additional information" about a transaction's counterparty or whether to take further steps to verify any received information. There are no standard, generally agreed upon frameworks within the blockchain industry for identifying the "owner" of a digital asset wallet. In fact, the concept of "ownership" of a digital asset wallet is a point of some philosophical debate[3] and has not yet been substantially defined in US legal jurisprudence. Many industry participants have experimented with methods for identifying wallet ownership with varying outcomes and there is

[1] "Many people living on Indian reservations have only P.O. boxes or no specific address." *https://www.census.gov/library/stories/2019/12/counting-people-in-rural-and-remote-locations.html*

[2] https://www.technologyreview.com/2018/11/29/138883/four-billion-people-lack-an-address-machine-learning-could-change-that/

[3] https://medium.com/coinmonks/what-do-you-legally-own-with-bitcoin-97b083ed6a04

no “industry best practice” to make any such determination. Setting aside any legal determination, it is technically impossible to “prove” ownership of a digital wallet. At most, you can prove that an individual or entity has specific knowledge of the private key that controls a wallet and that they are willing and able to sign a transaction from that wallet. However, other individuals could also have specific knowledge of that private key and could be ultimate controlling persons of the wallet. In the midst of this ill-defined concept, legally speaking, and impossible to define concept, technically speaking, FinCEN does not provide any particular guidance to FIs as to (a) how they should make efforts to obtain counterparty identifying information or obtain further information to confirm such information’s accuracy or (b) how FinCEN will enforce those efforts.

As one might expect, the result of this vague Proposed Rule will be a chilling effect on FI interactions with unhosted wallets. Given that there is no industry consensus or “best practices” to which FIs can point in the event of inquiry by FinCEN, FIs will likely favor a risk averse approach of refusing to allow clients to transact with unhosted wallets altogether, rather than risk penalty from FinCEN for non-compliance if the regulator does not favor an FI’s chosen method. This would have several regrettable consequences, primary among them being that clients of US regulated FIs would be left without recourse to remove their CVCs from a regulated FI into a personally custodied unhosted wallet. The second major unintended consequence would be that the rule would end up not providing law enforcement with any useful information on suspicious or potentially illicit activities. US regulated FIs would, instead, “go dark” while illicit activity would very likely continue via exchanges and custodians not subject to US regulation.

We urge FinCEN to consider the significant damage that could be done to the industry and its own law enforcement efforts by authorizing this hastily- and vaguely-conceived rule. For that reason, we also urge FinCEN, as we discuss further below, to extend the period for comment on the Proposed Rule. These concerns are highly complicated and technical in nature and require careful examination prior to establishing an adequate regulatory framework.

3. There are many circumstances under which compliance with the Proposed Rule will be technically impossible.

The Proposed Rule is further deficient in that it incorrectly assumes that the counterparty wallet for every regulated transaction necessarily belongs to or is controlled by an entity with a legal name and physical address. One of the most important blockchain innovations is the ability to enable distributed systems to autonomously intermediate transactions between entities. A regulated Financial Institution’s client may desire to send or receive CVC from an unhosted wallet that is neither a centralized financial institution nor an individual with a legal identity or physical location. Instead, such an unhosted wallet may be controlled by a smart contract, such as an “automated market maker” that allows individuals to engage in peer-2-peer transactions without utilizing a centralized intermediary otherwise subject to the Bank Secrecy Act regulations. There are many instances in which a Financial Institution’s client may want to send CVC to such a smart contract where the FI would not be able to obtain identifying information for the receiving wallet. For such transactions, a Financial Institution subject to the Proposed Rule would be technically incapable of satisfying the record keeping or reporting requirement regardless of how robust its compliance and information gathering efforts may be. In response to this inability, we expect that Financial Institutions will choose instead to prohibit their clients from engaging in such sending transactions.

There are also instances in which a Financial Institution's client may be the recipient of CVC in a transaction implicating the Recording and Reporting Requirements in which the sending wallet is a decentralized protocol or a blockchain network itself. For example, there are instances in which a distributed ledger may undergo a network "fork" causing a Financial Institution's client wallet to receive a significant number of "new" CVC assets resulting from the fork. There are also instances in which wallets that hold certain types of CVC receive "air drops" of new CVC from new decentralize protocols, sometimes in substantially valuable amounts.[4] In each of these instances, regulated FIs will not be able to gather the required identifying information for the sending wallets, putting them out of compliance. FIs would also not easily be able to prevent receipt of such CVCs in order to avoid falling out of compliance. Further, even if FIs could prevent hosted wallets from receiving new CVCs, to do so would set a very concerning precedent of regulation actively disallowing an FI's client from receiving digital assets it may be legally entitled to receive.

As distributed systems continue to develop, innovation around and utilization of autonomous protocols will be critical to achieving the benefits of "improving access to financial services, reducing inefficiencies, and lowering costs" inherent in legacy payments systems.[5] However the Proposed Rule would result in the complete inability of regulated banks and MSBs to engage in this decentralized financial infrastructure. Such an outcome would hinder the ability of US Financial Institutions to participate in and promote new innovation around financial infrastructure while also failing to achieve the Proposed Rule's stated objectives of combating illicit financial activity through gathering additional information. In most cases, FIs will be incapable of gathering such information. Meanwhile, this rule will not actually prevent illicit financial transactions from occurring. Nefarious actors will instead elect to use unregulated intermediaries not subject to US regulation or compliant with global AML and CFT standards.

4. The Proposed Rule will have a significant negative impact on US innovation and global competition.

The Proposed Rule will have detrimental effects on ongoing US innovation in developing blockchain and distributed systems technologies. Such a hinderance to the ability of US entrepreneurs and investors to promote innovation will cause the US to fall behind in expertise and leadership among global competitors for dominance in this burgeoning and potentially paradigm-shifting technology. As noted above, this rule will functionally exclude millions of US residents from participating in blockchain markets via regulated Financial Institutions, and beyond the market for American users of CVCs, the rule will also disallow participation of potentially billions of global users from engaging with regulated Financial Institutions in scaling this financial ecosystem. It would also be more difficult for existing US clients of regulated FIs to transact with distributed systems and decentralized protocols directly. Entrepreneurs will be keenly aware of these added frictions and limitations to utilizing and scaling new CVCs and will, as a result, seek out jurisdictions with regulations that are more carefully considered and better suited to the unique challenges this technology contemplates. This flight of innovation to jurisdictions that have taken the time and effort to appropriately understand the technology and apply sensible regulation will also result in a flight of investment capital to such jurisdictions.

---

[4] For the concept of forks, air drops and receipt of new digital assets, see https://www.coincenter.org/education/key-concepts/forks/.

[5] "Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets," Notice of Proposed Rulemaking, Financial Crimes Enforcement Network of the U.S. Treasury Department, https://www.federalregister.gov/public-inspection/2020-28437/requirements-for-certain-transactions-involving-convertible-virtual-currency-or-digital-assets.

As US investors in San Francisco, California, we fear that the rapidly advancing global technological ecosystem supporting the blockchain industry will continue to advance at its blistering pace whether the US regulatory system empowers US entrepreneurs, FIs and CVC users to participate in this innovation or not. For example, in 2020 alone we have seen the estimated market capitalization of decentralized financial ecosystems known as Decentralized Finance or "DeFi" grow from less than $1 billion to over $15 billion. While many of the developers and entrepreneurs building out the DeFi ecosystem are US persons, many are not. We have seen development teams contribute significantly to the space from all over the world, including Europe, Asia and South America. It is our strong preference as US investors to support US entrepreneurs and developers and ensure that the US continues to benefit from hosting the most technologically vibrant community of entrepreneurs, investors and users in the world. However, venture capital investors have obligations to their various stakeholders to make the best investment decisions and back the most valuable projects, regardless of geographic location (apart from sanctioned or embargoed jurisdictions identified, e.g., by OFAC). We expect that even US venture investors will seek out the best investment opportunities outside of the US, provided they are lawfully occurring within the framework of a legitimate regulatory regime.

The loss to US innovation and competition under the Proposed Rule would be significant and unfortunate, especially given the excessive haste with which this rule is being proposed. There are sensible opportunities for ensuring appropriate regulatory oversight for blockchain technology. However, in order to arrive at those opportunities, FinCEN and other US regulators should take a much more deliberate and thoughtful approach to crafting new regulation for a new asset class and industry.

5. Participants in the blockchain industry desire to engage with regulators to create sensible regulation; however, the process attending the Proposed Rule is entirely insufficient.

We at Blockchain Capital, along with many of the entrepreneurs behind our over 90 portfolio investments, are eager to engage with FinCEN and the treasury department to craft effective and measured regulation for decentralized systems. There are thousands of other industry participants who are eager to do the same. Perhaps contrary to popular belief, we view regulation as a necessary and integral part of the maturation process of this novel industry. Far from being "anti-regulation," we firmly agree that recent regulatory actions from the CFTC, FinCEN and the DOJ involving violations of the Bank Secrecy Action regulations by reckless actors, BitMEX[6] and Helix/Coin Ninja[7], are appropriate and necessary not only for the protection of the US (and global) financial system, but also to create additional space for legitimate, regulatorily compliant actors to continue innovating in the space. However, we emphasize that regulation will be most effective when utilizing a collaborative approach that leverages meaningful consideration of law enforcement objects, technological challenges and the protection of individual freedoms.[8]

---

[6] CFTC v. HDR Global Trading Limited, et al., CIVIL ACTION NO: 20-cv-8132, US Dist. Ct. for the Southern Dist. of New York, Oct. 1, 2020; https://www.justice.gov/usao-sdny/pr/founders-and-executives-shore-cryptocurrency-derivatives-exchange-charged-violation

[7] https://www.fincen.gov/news/news-releases/first-bitcoin-mixer-penalized-fincen-violating-anti-money-laundering-laws; https://www.justice.gov/opa/pr/ohio-resident-charged-operating-darknet-based-bitcoin-mixer-which-laundered-over-300-million

[8] "Government and industry should work together and design and implement a modern, robust, efficient, effective, and near real-time AML detection system that incorporates necessary privacy, safeguards, and oversight." https://www.wsj.com/articles/is-anti-money-laundering-working-no-its-failing-1511262616

The complexities of the global and distributed nature of the blockchain industry warrant additional time for industry participants to consider the impact of the Proposed Rule, research its effects on industry and provide critical feedback to regulators. We are greatly dismayed over the extremely limited period of public comment accompanying this Proposed Rule. Proving a truncated period of fifteen days spanning both the Christmas and New Year's holidays is woefully inadequate to allow for meaningful engagement from the public. Most significant administrative rulemakings allow 60 days' notice period for comment, and even less complicated and consequential rulemakings provide a minimum of 30 days.

The requirement for a period of notice and comment is not a courtesy extended to the public; rather, it is a federal law requirement meant to provide the public with a meaningful opportunity to engage with and respond to the proposed regulations. If given more time, we would have included substantial additional research around the effects of the Proposed Rule on industry participants, as well as more educational materials help FinCEN better understand the technical challenges facing the Proposed Rule.

Conclusion

FinCEN has made an alarmingly hasty and ill-considered rulemaking proposal. The Proposed Rule, if implemented, will disproportionately infringe on individual rights of privacy and disenfranchise underrepresented populations in the US from the benefits of open financial access. As drafted, the rule does not provide clear guidance for compliance by regulated entities, which will result in a chilling effect on participation by those entities in this new technology industry. Even if regulated entities were to attempt to comply with the rule as contemplated, there would be several instances in which compliance would be technically impossible, thus further incentivizing Financial Institutions to not support interaction with decentralized systems. These frictions will cause both entrepreneurs and investors involved in building out this new technology to offshore jurisdictions that are more thoughtful and deliberate in crafting functional regulation. The blockchain industry stands eager to engage with FinCEN and other regulators to ensure regulation of the space is effective and appropriate, but the process prescribed for this Proposed Rule denies the opportunity for adequate public engagement. For those reasons, we respectfully urge FinCEN to refrain from enacting the Proposed Rule, or in the alternative, significantly extend the notice and comment period to allow for genuine engagement with the public and consideration of the rule's effects.

Respectfully yours,

P. Bart Stephens

P. Bart Stephens
Co-Founder & Managing Partner

H. Joshua Rivera

H. Joshua Rivera
General Counsel & Chief Compliance Officer