

March 29, 2021

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

**Re: FinCEN Docket Number FINCEN-2020-0020; RIN 1506-AB47;
Requirements for Certain Transactions Involving Convertible
Virtual Currency or Digital Assets**

Supplementary Submission

To Whom It May Concern:

Dash Core Group (“DCG”) appreciates the opportunity to submit this supplementary letter for consideration by the Financial Crimes Enforcement Network (“FinCEN”) with respect to the Notice of Proposed Rulemaking (“NPR”), published on December 23, 2020, titled “Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets.” See 85 FR 83840. Dash Core Group shared an initial letter on January 4, 2021 (<https://www.regulations.gov/comment/FINCEN-2020-0020-7259>), which is incorporated here. Due to the shortened comment period, we were unable to address in depth certain technical topics concerning CoinJoin, or to explore the specific implementation of CoinJoin on the Dash network as compared to what is available on Bitcoin. We address those issues here.

In particular, we focus in this letter on the specific implementation of Dash’s CoinJoin solution branded “PrivateSend.” In recent communications with regulatory bodies, several have expressed the concern that the Dash network may somehow constitute a unique risk compared to other CoinJoin implementations because it is “built-in” or “part of the protocol.” This concept of CoinJoin being “built-in” is broad, vague, ambiguous, and open to many interpretations. Nevertheless, regardless of the specific interpretation, we will demonstrate that differentiating cryptocurrency privacy features based on the degree to which those features are “built-in” is not only arbitrary, but also irrelevant for assessing the risks associated with so-called “anonymity-enhanced cryptocurrencies” (or “AECs”).

As we describe below, Dash’s CoinJoin implementation is a relatively standard implementation, and differs markedly from more complex CoinJoin options available on other networks, particularly Bitcoin. Indeed, there are no CoinJoin features on the Dash network that don’t also exist on the Bitcoin network. On the other hand, there are many additional CoinJoin features and other privacy-enhancing technologies that have been implemented in Bitcoin’s protocol or wallets that are not available on the Dash network.

The basic point is this: if Dash’s implementation of CoinJoin renders the Dash cryptocurrency into an illicit finance risk—which it does not—then the same must be said of Bitcoin. Likewise, if Bitcoin is not considered an anonymity-enhanced cryptocurrency, Dash should not either. This is because *Dash’s privacy feature constitutes a mere subset of the privacy features available on Bitcoin.* Because no serious observer would claim that Bitcoin “inhibit[s] investigators’ ability both to identify transaction activity involving blockchain data and to attribute this activity to illicit activity conducted by natural persons” 85 FR 83844, it stands to reason that neither does Dash.

Accordingly, we respectfully reiterate our request that FinCEN strike any reference to Dash in any future iterations of (or documents relating to) this Rule.

Isn't CoinJoin still a strong privacy feature regardless of which network it is on?

No. CoinJoin is not a particularly strong enhancer of privacy, especially when compared to the current available tools in the cryptocurrency space. Techniques such as off-chain transactions, shielded addresses, burn-and-redeem, side-chains, ring signatures, and other advancements pose far greater investigatory obstacles to law enforcement officials, and offer far greater privacy to users of blockchains whose third-party developers incorporate those features.

Below, we review just some, but certainly not all, privacy-enhancing solutions currently available to users of Bitcoin and other blockchains. Out of all of the privacy-enhancing solutions in this section, mixing/tumbling and CoinJoin are the only solutions that record all input addresses, input amounts, output addresses, and output amounts to a public and transparent blockchain, thereby allowing any third-party to freely observe and analyze all transactions. We also demonstrate that Dash offers a relatively standard implementation of CoinJoin available in the market compared with most coins—none of which are considered to be “anonymity-enhanced cryptocurrencies.”

Off-chain transactions:

These transactions are not recorded on the public blockchain, but instead pass through a peer-to-peer (p2p) payment channel or side-chain. Transactions are not only impossible to trace, but also there is no means for the servers actually routing the transactions to monitor the number or volume of transactions on the network, nor can the routing servers determine the origin or destination of funds they route, as communications are encrypted and channel balances are not published.

Examples: Bitcoin Lightning Network, Litecoin Lightning Network

Shielding addresses or amounts, or zero-knowledge-proofs:

These techniques mask the addresses (inputs and outputs) and/or amounts of transactions. Both sending addresses and receiving addresses can be shielded from third party observers.

Examples: Monero and private Zcash transactions

Burn-and-Redeem : Users are able to destroy coins and redeem them for new coins to eliminate previous transaction history or linkages by destroying all “digital trails”.

Example: Firo (previously known as Zcoin)

Mimblewimble:

The Mimblewimble protocol aggregates inputs and outputs of multiple transactions into one unified set, and eliminates addresses accessible to third-parties. These features make it impossible to trace transaction histories via third-party observation of the blockchain.

Examples: Grin, Beam, Litecoin (plans to launch mimblewimble in Q2 2021)

Tumbling / Mixers:

Tumblers and mixers are services operated by providers that typically require users to transmit cryptocurrency to them for mixing and exchange. The centralized entity then sends back cryptocurrency originating from other customers, thus eliminating the ability of third-party observers to trace the user's true source of funds. This technique is custodial, which means that users are actually transferring value to a centralized entity prior to receiving the same value back. Centralized tumbling/mixing entities have been categorized as MSBs.

CoinJoin / Shuffling:

This privacy feature is similar to tumbling / mixing, with two distinct differences: (1) users never lose control of their coins, and (2) third-party observers can link a user's balances and transactions to an originating address (although the originating address may be difficult to attribute with 100% certainty). This is a non-custodial solution. Users simply send from one address to another within the same wallet contemporaneously with other users. All transaction details including input addresses, input amounts, output addresses, and output amounts are published to a public ledger, enabling any third-party observer to analyze these transactions.

Examples: Bitcoin, Ethereum, Litecoin, Bitcoin Cash, Dash, and most transparent BTC-based blockchains.

What is CoinJoin?

CoinJoin allows for consumer grade privacy via a trustless method for combining multiple inputs from multiple spenders into a single transaction that makes it more difficult for outside parties to determine which input address is associated with each output address. It is important to note that the reason we call this consumer grade privacy is because there are a number of blockchain analysis companies that possess tools that can provide transaction risk scoring services for transactions on almost all public blockchains (including Dash).

As mentioned, there are many examples of CoinJoin available on most public blockchains, including Bitcoin (Samourai wallet and Wasabi wallet), Bitcoin Cash (CashShuffle and Cashfusion wallet), Litecoin (Mustard wallet), and Dash (Dash Desktop Wallet).

CoinJoin is not a separate type of transaction that is subject to a different rule-set from other virtual currency transactions. Instead, CoinJoins always represent a subset of valid Bitcoin transactions. As anyone familiar with blockchain technology knows, a valid on-chain Bitcoin transaction needs to meet a certain set of criteria (e.g., output amounts cannot be greater than the input amounts, inputs must be cryptographically signed). Dash, as a Bitcoin fork, has functionally identical criteria and restrictions for a transaction to be considered valid. Any CoinJoin protocol or ruleset is actually a restriction on the base transaction protocol of Bitcoin. For example, a given CoinJoin implementation may restrict the amounts used for inputs, or may require the output addresses to be unused addresses.

CoinJoin is therefore just a more restrictive instance of a Bitcoin transaction where in order for the transaction to be valid, it has to have a specific amount of Bitcoin or Dash serve as an input from a particular set of valid unspent transaction outputs. Depending on the specific CoinJoin implementation, there might be limits where a transaction has to have the exact same number of inputs as outputs. Another restriction may be that all output addresses all have to be unique.

The important part to note is that CoinJoin transactions require no changes to Bitcoin's transaction protocol.

In order for the users to create and broadcast a CoinJoin transaction, they must first identify other users wishing to enter into a CoinJoin transaction, and information from each of the participants must be shared amongst the participants. Specifically, the users need to know the full set of input addresses, amounts, and output addresses which each of the other users wish to include in the transaction. The transaction must then be passed between each of the participants to sign before it can be broadcast. While these tasks are most efficiently performed by a computer, the coordination can take place directly between two or more users without the aid of automated information handling. Indeed, CoinJoin transactions can be orchestrated through IRC chats, online files (e.g., Google Sheets), telephone calls, or even via postal service. For obvious reasons, using automated software is the most convenient method of identifying other users with whom to CoinJoin, and coordinating the information needed for the transactions themselves.

Individual CoinJoin implementations follow a set of rules which are typically enforced by a coordinating server. The software each of the participants use (e.g., wallets) will similarly check to ensure the rules have been followed before signing the transaction (which is necessary to make the transaction valid).

With this basic explanation of CoinJoin, we can now contrast and compare what privacy techniques are available on Bitcoin versus Dash:

	Dash	Bitcoin	
More Transparency	Fully transparent Blockchain	✓	✓
	Transparent Input Addresses	✓	✓
	Transparent Input Amounts	✓	✓
	Transparent Output Addresses	✓	✓
	Transparent Output Amounts	✓	✓
More Privacy	CoinJoin Desktop Wallet Availability	✓	✓
	CoinJoin Mobile Wallet Availability	✓	✓
	Chaumian CoinJoin Availability		✓
	Off-chain transactions Availability		✓
	Third Party tumbling Service Availability		✓
	Mimblewimble*		
	Batch Spending		✓
	Boltzmann clustering resistance		✓
	BIP47 payment codes		✓
	Transaction hopping		✓
	Shielded Addresses		
Shielded Amounts			
Compliance	Third-Party AML Analytics Providers	✓	✓
	Travel Rule Compliant	✓	✓

First, let us reiterate the main point in Dash Core Group's first NPRM letter. Dash's network features a transparent auditable blockchain that does not have **any** hidden addresses or hidden transaction details. All transactions list the complete set of input addresses, output addresses, input amounts, and output amounts all the way back to the genesis block. Dash features a relatively vanilla implementation of CoinJoin on its network that is available in a Dash desktop wallet as well as in an Electrum wallet. Bitcoin CoinJoin implementations are also available on desktop and mobile wallets. However, the number of privacy enhancements on the Bitcoin network far exceed those on the Dash network, and in fact there are no privacy features present on Dash that Bitcoin does not also support. Dash does not offer support for many advanced privacy techniques such as Chaumian CoinJoin, off-chain transactions (which are not auditable on the blockchain), or any of the remaining options listed above. By contrast, the Bitcoin Network and ecosystem support the vast majority of these advanced privacy techniques. In short, while Dash's PrivateSend has not materially changed since its implementation in 2014, Bitcoin's privacy options have.

To further illustrate the complexity of privacy on public blockchains, we explore here just the various CoinJoin implementations on the Bitcoin network. Many enhancements to regular "vanilla" CoinJoin have been introduced over the years. Please note that **none** of these additional techniques are available on the Dash network.

Chaumian CoinJoin: Typically, CoinJoin transactions leverage a coordinating server that collects information from each of the participants wishing to enter into a CoinJoin transaction with other users. The users need to know the full set of input addresses, amounts, and output addresses which other users wish to include in the transaction. In the process of collecting and disseminating this information, the coordinating server is aware of which inputs and outputs belong to the same participant.

Chaumian CoinJoin was introduced in 2017 as an improvement meant to address this problem. Chaumian CoinJoin obscures transaction details from the coordinating server so that even the coordinator is not able to definitively link the inputs and outputs produced by a Chaumian CoinJoin transaction. This means the coordinating server gathers no greater data on the transaction than is available to any other third-party observer of the public blockchain. Again, Dash does *not* feature Chaumian CoinJoin.

BIP-47: Bitcoin Improvement Proposal 47 or "BIP-47" allows for reusable Payment Codes for Hierarchical Deterministic Wallets. This proposal introduced the notion of "stealth addresses" on the Bitcoin network. BIP-47 addresses the public and transparent nature of Bitcoin transactions by providing users with reusable Payment Codes tied to unique Bitcoin addresses, instead of users reusing identifiable Bitcoin addresses. Payments conducted through Payment Codes are indistinguishable from regular Bitcoin payments and are therefore unidentifiable.

Batch transactions: Batched transactions in cryptocurrencies have traditionally been used to group transactions in order to save on miner costs, because the size of one large transaction is smaller than the sum of many smaller transactions. However, because aggregated inputs and outputs produce more complexity, batched transactions are naturally more difficult to analyze as well, so they infer some privacy advantage over separate transactions. A few different forms of batched transactions are implemented in privacy-oriented Bitcoin wallets, including batching between different users. Again, Dash wallets do *not* support batch transactions.

Boltzmann Clustering Resistance: While this is technically not a CoinJoin transaction type, transactions can be made to look like CoinJoin was used. In essence, it is an imitation of a

CoinJoin conducted by a single user. A Boltzmann score is used to measure the entropy of a transaction, or put another way, the resistance a transaction has to identity clustering tools utilized by blockchain analysis companies. Tools that use Boltzmann scores within their privacy features attempt to lower the confidence of blockchain analysis tools and introduce doubt of ownership of addresses within a cluster. This allows an identified user plausible deniability. A Boltzmann score is determined by identifying the number of feasible links or mappings of inputs to outputs in a transaction. Dash does *not* offer imitation CoinJoins.

Transaction hopping: Transaction hopping adds a number of additional “hops” to a transaction. Hops refer to moving cryptocurrency from one address to another address. Since chain analysis companies typically scan the history of the last four transactions associated with the incoming transaction, transaction-hopping introduces extra hops of history in order to further “distance” an exchange deposit from any previous history, in effect attempting to stump chain analysis forensic tools. This technique is often used in conjunction with – and in the same wallet as – CoinJoin. This could prevent an exchange’s analytics from determining that CoinJoin was used, for example. Dash does *not* offer automated transaction hopping.

Receiver Mix-ins: Receiver mix-ins are CoinJoin transactions in which the receiver provides one or more of the inputs to the transaction. This obscures and complicates analyzing a transaction because it counters an assumption that underpins the structure of typical Bitcoin transactions. Specifically, it violates the assumption that all inputs into a valid, cryptographically signed transaction are from the same entity. This approach may trick observers into concluding that the transaction was simply a consolidation of UTXOs within the user’s own wallet, and that a transaction between two parties had not even taken place. Dash does *not* offer receiver mix-ins.

All of these enhancements have been introduced to CoinJoin wallets on the Bitcoin network. **None of them exists on the Dash network.**

Here is a link to a video providing a presentation of the various CoinJoin technologies for those more visually inclined: <https://www.youtube.com/watch?v=iRhFrXD84Og>

In addition to existing privacy techniques, Bitcoin developers plan to further enhance its privacy features through its Taproot upgrade, expected to be released within the next couple of weeks. This upgrade will allow for the following features to be deployed on the Bitcoin network:

CoinSwap: Typical CoinJoin transactions are relatively easy to spot, even without analytics software. There are usually many inputs and outputs of the same size within the same transaction. CoinSwap essentially fixes this by enabling coin mixing to take place without being detected. Essentially, these will be CoinJoins that appear to be regular transactions. They work by breaking CoinJoins into many separate transactions using scripts that are indistinguishable from any other Taproot single signature transaction. In essence, this creates stealth mixing sessions, rendering coin mixing undetectable to blockchain analytics.

Point Time Lock Contracts: This is one of the innovations that makes CoinSwap possible. This improves the types of scripts possible and keeps the contents of the scripts private so that third parties cannot determine that a CoinSwap was used.

Ring Signatures: Taproot will also provide users the ability to use “ring signatures” in order to cryptographically prove that they own a certain number of coins without revealing exactly which coins they own. For example, if you need to prove that you own over 100 BTC, you would be

able to do so by performing a ring signature over all the Taproot UTXOs worth more than 100 BTC. This improves Lightning network node operator privacy who now have the opportunity to prove ownership of a payment channel without compromising privacy.

MuSig2: From a privacy perspective an outside observer will no longer be able to tell whether a single signature transaction or a multisig transaction took place on the blockchain because of so-called “scriptless scripts”, since all Taproot transactions have the same digital footprint when broadcast to the network.

Dispelling the “Built-In” Myth

One point we have heard on several occasions in informal conversations with regulators is that Dash’s PrivateSend CoinJoin implementation is somehow distinct from other CoinJoin implementations because it is “built-in” or “part of the protocol.” We do not know how to interpret this statement, which is arbitrary, ambiguous, vague, and unarticulated in any official U.S. government definition of AECs. The concept of CoinJoin being “built-in” could be in reference to Dash’s CoinJoin implementation ruleset being included in the same executable file as a “full node” wallet (e.g., a wallet that stores a full copy of the blockchain to enable independent validation of transactions). It could also be in reference to Dash’s end-user wallets utilizing a special class of full nodes called “masternodes” within the network to act as coordinating servers for users wishing to participate in a CoinJoin. Either interpretation is flawed for many reasons.

As already explained, a blockchain “protocol” is simply a set of rules, similar to how HTTPS is a protocol. These rules can be implemented in any piece of software, similar to how HTTPS is implemented in Firefox, Safari, Chrome, Edge, or Brave. Any CoinJoin protocol or ruleset is actually a restriction on the base transaction protocol of Bitcoin which incorporates privacy best practices (e.g., using a new address to receive funds) and rules that make the CoinJoin more effective. For example, a given CoinJoin implementation may restrict the input amounts to specific denominations, and requires the output addresses to be unused addresses in the user’s wallet. These rules are enforced by the coordinating server and by each of the participants to a particular CoinJoin protocol. Participants that fail to follow the rules of the CoinJoin would not be allowed to participate by the coordinator. Even if a coordinator failed to enforce broken rules, the end-user wallets would check to ensure the rules were followed, and would refuse to sign the transaction if those rules were broken.

Importantly, all CoinJoin transactions are perfectly valid Bitcoin transactions. They must meet all regular Bitcoin transaction rules (e.g., the input amounts must be greater than or equal to the output amounts, and all transaction inputs must be signed by their respective private keys). In other words, they aren’t a “new transaction type” at all.

If FinCEN’s “built-in” distinction is referring to the masternode information coordination, which specific server helps users coordinate the user CoinJoin requests has no bearing on the information available to third-party observers of the blockchain, i.e., it doesn’t “inhibit investigators’ ability both to identify transaction activity involving blockchain data and to attribute this activity to illicit activity,” which (according to the NPR) is a defining characteristic of AECs.

If, on the other hand, FinCEN’s “built-in” distinction is referring to the end user wallets being full-nodes, whether end users are operating software code designed to include the additional CoinJoin transaction rules using an executable file that also includes the Bitcoin full-node also has no effect on the information recorded on the blockchain, or in terms of how effective the

resulting CoinJoins are. Again, the inclusion of CoinJoin rules in the same executable file does not affect the privacy level of the resulting transactions.

In either of the two preceding interpretations of this “built-in” distinction, FinCEN is clearly focused on the wrong thing; the packaging. It is akin to the ATF regulating gun sales based on whether the gun is sold in the same package as an ammunition clip. In this analogy, the government has taken the position that a pistol sold with an ammunition clip is problematic, while freely allowing a far more potent automatic machine gun to be sold simply because the manufacturer sells the ammunition belt separately. The concept that FinCEN is concerned by Dash’s “built-in” CoinJoin is as absurd as the above analogy, and in fact more so due to the difficulty in even determining the point at which a feature is “built-in” when it comes to software, which is far less certain than a physical package. We will expand on this point later.

Furthermore, if this aspect of Dash is a reason FinCEN has classified Dash as an AEC, this classification does not have any basis in the published exposition of what FinCEN believes an AEC to be. It seems to constitute a “privacy-enhanced definition” of an AEC.

Perhaps FinCEN wrongfully believes that including both the transaction protocol and CoinJoin software into a single package somehow makes it easier for users to use CoinJoin. In fact, in many respects, the prerequisite for users wishing to use CoinJoin to download and maintain a full copy of the Dash blockchain just to use its CoinJoin implementation is a significant burden. We frequently receive requests for a “light” wallet version of CoinJoin. This prerequisite is also a burden on anyone wishing to operate a coordinating server.

Lastly, it isn’t even the case that Dash is unique in its inclusion of CoinJoin into a full-node implementation of a wallet. Software containing both a Bitcoin full node and a CoinJoin protocol has also been implemented within the same executable file. For example, Dojo is a Bitcoin full node software with CoinJoin “built-in” which both enables users to construct CoinJoin transactions (i.e., it is an end-user wallet that can send CoinJoin transactions) and can act as the coordinating server for users. So again, there is no justification for Dash’s distinct treatment as Dash is not unique in this “built-in” aspect in the first place.

If FinCEN nonetheless takes the position that CoinJoin rules contained in the same executable defines a coin as an AEC (which the government has never articulated in the past), then Dash Core Group could respond to regulators by — trivially — separating the CoinJoin rules module from the rest of its software and republishing the software separately as two distinct pieces of software, in the same way that Microsoft could publish Word and Excel separately or as a package. Publishing these functions separately would have no impact on the user experience, no impact on the efficacy of Dash’s CoinJoin, and would have no impact on the ability of law enforcement to analyze the transactions; it would simply be box-checking to placate a definition.

Indeed, to illustrate the absurdity of this “built-in” distinction, anyone with programming skills could modify any open-source wallet for any existing “non-AEC coin”, add some CoinJoin rules to it, and release the software. Under the government’s apparent reasoning, that act would instantly reclassify the asset itself as an AEC. This would make it possible for any individual to unilaterally make any coin of his or her choosing—and with minimal effort and without permission from anyone—meet the government’s apparent definition of an AEC, without any impact one way or the other on “investigators’ ability both to identify transaction activity involving blockchain data and to attribute this activity to illicit activity.”

In fact, to illustrate the untenability of this criteria, *FinCEN itself* could create wallets or full node software implementations with CoinJoin rules for every open-source cryptocurrency that features a transparent and auditable blockchain, publish the software, and instantly reclassify any cryptocurrency of its choosing to meet the apparent definition of an AEC! And it could do so without permission or participation from anyone.

This is in stark contrast to more privacy-oriented techniques like shielded transactions or a burn-and-redeem model where introducing the privacy feature would actually result in a hard-fork of the underlying blockchain protocol (requiring a change to the ruleset of what a valid transaction is), where that new protocol would need to be adopted by the consensus mechanism of the respective network (e.g., miner adoption, staking adoption, validator node adoption).

The idea that the government could enforce a “built-in” rule for open-source software is laughably absurd in the first place. When exactly is code “built-in”? What if two executable files are installed by the same installation package? What if they can be downloaded separately, but each will automatically install the other once launched? What if the open-source code is published on Github, but not yet compiled into an executable? What if two software packages are published separately, but the software is specifically designed to interface with one another? We could go on, but trying to draw a distinction between these is meaningless for the government’s stated purpose in regards to illicit activity. It is akin to requiring that a book be published in two volumes to prevent the information contained in it from being utilized.

U.S. Government’s AEC Definitional Deficiencies

Because no detailed explanation has ever been given by the U.S. government’s decision to label Dash an AEC, we decided to decode the government’s current definitions of an AEC. FinCEN’s definition from May 2019 states: “Anonymity-enhanced CVC transactions are transactions either (a) denominated in regular types of CVC, but structured to conceal information otherwise generally available through the CVC’s native distributed public ledger; or (b) denominated in types of CVC specifically engineered to prevent their tracing through distributed public ledgers (also called privacy coins).” (1, FinCEN).

It appears that FinCEN’s categorization of Dash as an AEC might be based on a mistaken belief that Dash is “denominated in types of CVC specifically engineered to prevent their tracing through distributed public ledgers (also called privacy coins)” (Fincen <https://www.fincen.gov/sites/default/files/2019-05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf>). The assessment appears to be based on the specific intent of blockchain engineers. This is problematic for many reasons. First, it is difficult to attribute intent to engineers since software development typically represents a trade-off that balances addressing a solution to multi-dimensional problems. Second, if engineers’ intent is a primary factor in determining an AEC, then clearly Satoshi Nakamoto also planned for Bitcoin to be an AEC based on his intent outlined in the Bitcoin white paper (<https://bitcoin.org/bitcoin.pdf>):

“10. Privacy

The traditional banking model achieves a level of privacy by limiting access to information to the parties involved and the trusted third party. The necessity to announce all transactions publicly precludes this method, but privacy can still be maintained by breaking the flow of information in another place: by keeping public keys anonymous. The public can see that someone is sending an amount to someone else, but without information linking the transaction to anyone. This is similar to the level of information released by stock

exchanges, where the time and size of individual trades, the "tape", is made public, but without telling who the parties were. As an additional firewall, a new key pair should be used for each transaction to keep them from being linked to a common owner. Some linking is still unavoidable with multi-input transactions, which necessarily reveal that their inputs were owned by the same owner. The risk is that if the owner of a key is revealed, linking could reveal other transactions that belonged to the same owner."

Finally, if Dash is considered an AEC because of its implementation of CoinJoin, then every other cryptocurrency that has a CoinJoin wallet should also be categorized as an AEC based on developer intent. This brings us back to our original point that given the vague definition of an AEC, anybody in the world with the necessary technical skills can release a CoinJoin wallet to transform any publicly available, Bitcoin-based blockchain into an AEC.

Regardless, it is hard to justify that Dash's CoinJoin implementation is designed to "prevent their tracing through distributed public ledgers" as CoinJoin transactions make no attempt to "conceal information otherwise generally available through the CVC's native distributed public ledger" in the first place.

The Department of Justice has also attempted a definition of an AEC: "Other cryptocurrencies, however, use non-public or private blockchains that make it more difficult to trace or to attribute transactions. These are often referred to as 'anonymity enhanced cryptocurrencies' ('AECs') or 'privacy coins.' Examples of AECs include Monero, Zcash, and Dash (2, DoJ)." At this point even a reader who has made it this far in the letter but who has never been exposed to any aspect of blockchain technology understands that Dash is not based on a non-public or private blockchain. Again, every Dash transaction contains the input addresses, input amounts, output addresses, and output amounts. No transaction details are obfuscated in any way.

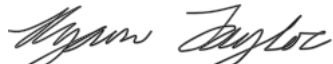
Conclusion

We sincerely appreciate FinCEN's acceptance of our submissions, but we must strongly object to FinCEN's inclusion of Dash in the NPR as an AEC that poses a law enforcement and national security threat. It is unacceptable to reference Dash in this light, especially where we have:

- proactively reached out to FinCEN to describe how the Dash cryptocurrency works;
- where reputable third parties (with whom we have no connection) have independently confirmed our points (see Dash Core Group letter 1 for statement by Chainalysis);
- where, to our knowledge, there is no evidence showing that Dash is actually used in illicit ways;
- where Dash's implementation of CoinJoin is less sophisticated than Bitcoin's;
- where CoinJoin is a comparably basic privacy technique compared to other privacy techniques available on public blockchains that FinCEN evidently does not consider as AECs;
- where we have received no clarification from FinCEN as to why the agency believes Dash to be an AEC, and where it has never articulated a response to our fact-based arguments.

Meanwhile, we continue to suffer real (and possibly irreversible) harm as a result of the U.S. government's actions. Dash Core Group is available to resolve any questions and is happy to continue to engage with FinCEN. But as stated in our earlier letter, we ask you to act quickly. There is simply no justification for the U.S. government's continued behavior in labelling the Dash cryptocurrency an AEC. Until the definitional issue is resolved, please remove any and all references to Dash in the pending Rule (and in any materials surrounding it).

Very Truly Yours,



Ryan Taylor
/s/ Ryan Taylor

Ryan Taylor
Chief Executive Officer
Dash Core Group, Inc.