ComplyFirst

COMPLIANCE BRIEF

Digital Asset | **Dash (DASH)** | **May 12, 2021**

EXECUTIVE SUMMARY:

The Dash cryptocurrency builds off of the Bitcoin codebase to add features like CoinJoin, which utilizes a network of 3rd party nodes termed masternodes to coordinate automated CoinJoin in order to improve privacy and make it more difficult for outside parties to track movement of transfers of its native value token, DASH.[1] Unlike many other privacy solutions, CoinJoin transactions do not require a modification to the bitcoin protocol.[2]

In many regards, Dash is similar to Bitcoin, with the core differences being the aforementioned masternode network and dependent services. Additional masternodes may be created through an individual "staking" 1,000 DASH, as well as satisfying certain technical requirements around the operation of the node. Masternodes serve as the core platform for protocol-level treasury and governance decisions, making Dash a form of a decentralized autonomous organization according to its proponents.[3] The presence of masternodes also enables the network to quickly reach consensus regarding the validity of each transaction through InstantSend transaction locks. The network of masternodes attempt to issue InstantSend locks on all transactions, though for various reasons the masternodes may fail to achieve sufficient consensus to issue a lock on any particular transaction. InstantSend utilizes masternodes to allow for faster (although arguably less secure) transaction processing that is independent from the traditional block mining process.[4] CoinJoin, mentioned earlier, utilizes masternodes to trustlessly combine DASH from multiple users into a common transaction and send those funds to new addresses in each user's wallet. Masternode operators are given voting rights and also receive DASH as "staking" rewards over time.[5]

Dash addresses are very similar to Bitcoin, and are composed of a hash of a public key, with a corresponding private key required for spending of DASH that has been sent to the address. Except for where CoinJoin has been used, all DASH transfers operate at the same level of anonymity as ordinary Bitcoin transfers. Where CoinJoin is in use, the operation is similar to those offered by many Bitcoin CoinJoin implementations.

With a combination of enhanced due diligence, enforcing limitations on types of customers and acceptable jurisdictions, ongoing transaction monitoring, and requesting the disclosure of additional information such as counterparty information and proofs as needed, financial intermediaries can indeed allow customers to use services related to DASH in compliance with FIN-2019-G001.[6]

BACKGROUND INFORMATION:

Originally named XCoin, and then Darkcoin, Dash was created in January 2014.[7] DASH, as a cryptocurrency, can be classified as a payment currency and by some as a privacy-preserving cryptocurrency (or "privacy coin"). In the past, Dash was commonly looked upon within the cryptocurrency community as being such, since it was the first to offer a trustless CoinJoin wallet. The project was rebranded in 2015 from Darkcoin to Dash (a play on "digital cash") largely

---

1 *See* https://docs.dash.org/en/stable/introduction/features.html#coinjoin

2 *See* https://en.bitcoin.it/wiki/CoinJoin

3 *See* https://docs.dash.org/en/stable/governance/understanding.html

4 *See* https://docs.dash.org/en/stable/introduction/features.html#instantsend for more information

5 *See* https://docs.dash.org/en/stable/masternodes/understanding.html

6 *See* FinCEN Guidance issued on May 9, 2019 (FIN-2019-G001), §4.1; see also id. at §4.5.3; see also 31 C.F.R. §1022.210.

7 *See* https://en.wikipedia.org/wiki/Dash_(cryptocurrency)#History

in an effort to emphasize its focus as a payment currency over private transactions.[8] With that in mind, Dash's focus is to be used in day-to-day commerce as a means to purchase goods and services. As detailed earlier, Dash does incorporate the privacy-enhancing CoinJoin mechanism which is overall similar (including very technically similar) to several Bitcoin CoinJoin implementations, but these are optional services which do not put it on the same privacy footing as compulsory, protocol-level blockchains such as Monero and Grin, nor as comprehensive as the optional privacy deployment in Zcash. Another notable difference is that even when used, CoinJoin only benefits the privacy of the sender, but not the receiver.

Circulating and Total Supply

As of the date of this brief, there are 10.16MM DASH in public circulation with a value of $1.808BB.[9] The total supply of DASH is dependent on several factors, and ranges from 17.74MM and 18.92MM.[10] Unlike Bitcoin, 10% of DASH block subsidy is allocated for use in the decentralized budget system, with miners and masternode operators claiming 42.03% and 47.97% respectively. Transaction fees are split 46.7% and 53.3% respectively between the miners and masternodes. These allocations change over time.[11]

Common usage

Like all cryptocurrencies, the value of DASH fluctuates considerably relative to any fiat currencies and thus, there is a large community treating it as a speculative investment in the hope that it will increase in value and can be sold for a profit. As a payment currency, DASH may theoretically be used to purchase any goods and services. However, in practice, there are a limited number of vendors accepting DASH.[12] Unlike the Bitcoin protocol, Dash utilizes the X11 proof-of-work algorithm, which merges together numerous hashing functions in an attempt to be more resistant to large-scale mining operations (normally done through custom chip fabrication known as ASICs). Despite this, a number of X11 ASIC miners are on the market, which has made mining using the traditional CPU or GPU setups unprofitable for several years.[13] 1000 DASH is required to run each masternode. Masternodes are rewarded for providing certain network features such as CoinJoin and an "InstantSend" feature.[14]

PRIVACY MECHANISMS:

Dash's primary privacy mechanism is the CoinJoin method of combining transactions with other users. The compliance profile of Dash's CoinJoin implementation is similar to many of Bitcoin's CoinJoin implementations, or a 3rd party Bitcoin mixing service. Dash CoinJoin transactions are coordinated "off-chain" by masternodes and the Dash wallet software, and performed by a series of on-chain transactions made by the parties involved.[15]

ANTI-MONEY LAUNDERING COMPLIANCE:

DASH presents a curious case for compliance, with often-used transparent transactions and less-frequent CoinJoin transactions. Especially since CoinJoin transactions are not commonly used, these transactions pose an inherent AML risk in the approximate range of transactions which use Bitcoin privacy tools such as CoinJoin wallets or mixers. If Dash's CoinJoin transactions are ever widely adopted to cover a wider set of speculators, miners, and other users (which is unlikely due to more complex user experience, lack of support in most wallets, added time, and added cost[16]), they may instead pose an AML risk in the approximate range of traditional payment types such as cash, card,

---

8 See https://www.newsbtc.com/news/darkcoin-rebranding-dash-digital-cash/

9 *See* https://coinmarketcap.com/currencies/dash/

10 *See* https://docs.dash.org/en/stable/introduction/features.html

11 *See* https://docs.dash.org/en/stable/introduction/features.html#block-reward-allocation

12 A useful resource of online retailers and service providers accepting DASH as payment can be found at https://www.dash.org/where-to-spend/

13 See https://docs.dash.org/en/stable/mining/

14 *See* https://docs.dash.org/en/stable/masternodes/understanding.html

15 See https://docs.dash.org/en/stable/wallets/dashcore/coinjoin-instantsend.html#

16 See https://docs.dash.org/en/stable/introduction/features.html#coinjoin

or paper payment instruments. Through the use of appropriate controls, these risks can be mitigated considerably in either case. These include:

A. Enhanced Due Diligence (EDD)

Intermediaries providing services relating to DASH and DASH transactions should require customer due diligence at onboarding. To take FinCEN rules as an illustration, this would include requiring collection and verification of a customer's name, date of birth, address, and identification number.[17] FinCEN and other regulatory agencies, following the FATF recommendations, indicate that the use of privacy features (including the use of privacy-preserving cryptocurrencies) could indicate higher risk and could signal a need for institutions to conduct enhanced due diligence. In cases where institutions deem enhanced due diligence is necessary to manage risk, institutions should expect to collect more information about the source of funds to limit the risk of these privacy features shielding illicit activities. They should also consider collecting a user's profession and proof of address. Should the intermediary request a reason for the customer's transacting in DASH or the customer's specific use of CoinJoin, this information would not only help the intermediary determine whether that customer is unlikely to use the DASH for money laundering, but also to construct a robust and detailed customer profile against which the customer's ongoing activity could be assessed. Of course, the use of DASH or of Dash's CoinJoin feature should only be one factor in a risk-based approach in determining if EDD is necessary, and other factors may increase or lessen risk. Institutions may determine that their AML controls are already sufficient to reasonably handle the additional risks inherent to DASH, for example if this information is already collected or if reasonable limits are already in place.

B. Limitations on types of customers and geographies

Certain categories of customers (e.g., politically exposed persons) and certain geographies (e.g., jurisdictions on the FATF's "grey list") pose a presumptively higher inherent AML risk. Although it would be a blunter instrument for risk mitigation than per-customer analysis, an intermediary could reasonably and effectively lessen the overall AML risk by categorically prohibiting customers who are in higher risk categories or geographies from accessing and or using DASH-related services.

C. Ongoing transaction monitoring and diligence

Use of traditional methods and tools when tracking customer transactions enables a VASP to determine a customer's typical activity and allows for identification of atypical activity. In addition, there are a number of private blockchain-specific monitoring tools which may be employed. Intermediaries could also require supplemental information from a customer before processing a DASH transaction (e.g., details regarding purpose of a transaction, name and address of recipient, and contact information of recipient). Collecting this information could help deter illicit activity in the first instance, while also providing verifiable data that could assist the intermediaries' compliance and audit processes. Even if it is impractical to verify all such information before a transaction is executed, implementing risk-based policies and procedures to verify supplemental information from a certain percentage of such transactions (whether before or after execution) could still help an intermediary detect and address a significantly greater amount of suspicious activity involving DASH. Finally, and arguably as a last resort, an intermediary could limit all incoming and outcoming transactions involving DASH to originating or receiving addresses that the account holder demonstrably controls. This too is a blunt measure that should generally not be necessary for the vast majority of cases.

17 31 CFR § 1022.210(d)(1)(iv).

D. Requesting additional information for Travel Rule compliance

In the United States, the Funds Travel Rule requires, among other things, the transmitting financial institution or intermediary to include the name of the transmitter and the amount of the order for transmittal orders to another financial institution. In usual circumstances, the sender's intermediary will already know the required information about the sender (i.e., its customer) through its own KYC process, and can require the sender to provide all other required transactional and beneficiary information as a prerequisite to executing the transaction. Notably, the Travel Rule applies only to transactions involving more than one regulated intermediary, so an exchange is not required (for example) to transmit a sender's Travel Rule information to a beneficiary's unhosted DASH wallet. Since the sending and receiving intermediaries are required to conduct KYC on their respective customers prior to providing services, the privacy-preserving nature of DASH therefore does not hinder compliance with the Travel Rule.[18]

Through the mechanisms detailed above, financial intermediaries can indeed allow customers to use services related to DASH in compliance with FIN-2019-G001[19]

ANTI-MONEY LAUNDERING COMPLIANCE EXAMPLES:

Here are some example applications of the above AML compliance suggestions for specific types of cryptocurrency businesses:

A. Cryptocurrency ATM

Cryptocurrency ATM companies may decide to only allow CoinJoin Dash deposits from low-risk geographies. They may determine to collect basic identifying information such as the user ID and residential address of customers with low transaction volumes, such as trades under $3,000. This customer information should be properly screened against sanctions lists and against other risk factors. Cryptocurrency ATM companies should place reasonable upper-limit transaction volumes, and they should report all transactions deemed suspicious to the appropriate regulators. Dash addresses should be screened using chain analysis tools; customers and all Dash addresses should be screened against sanctions lists. Substantial CoinJoin Dash use should be investigated by entities and justified by customers.

B. Cryptocurrency Exchange

Cryptocurrency exchanges may decide to only allow CoinJoin Dash deposits from low-risk geographies. They may require users to only deposit or withdraw USD or other fiat currencies to verified bank accounts. Exchanges should collect basic information on users, including their ID and address. Exchanges may require users to pass a higher verification level to trade Dash, or to trade Dash with higher limits. Customers and their requested Dash withdrawal addresses should be screened against sanctions lists. Suspicious trading, deposit, or withdrawal histories should be reported to the appropriate regulators. Exchanges should have a record of expected trading volumes and activities, and they should have monitoring in place to see if users exceed these expected activities. Substantial CoinJoin Dash use should be investigated by entities and justified by customers.

C. Payment Processor or Money Transmitter

Payment processors may choose to only allow CoinJoin Dash deposits from customers in low-risk geographies to entities in low-risk geographies. Payment processors should more closely scrutinize the businesses that receive Dash payments, possibly prohibiting high-risk business types from accepting Dash payments or requiring these businesses to

18 *See* https://getmonero.org/2019/12/05/funds-travel-rule.html

19 *See* FinCEN Guidance issued on May 9, 2019 (FIN-2019-G001), §4.1; *see also id.* at §4.5.3; *see also* 31 C.F.R. §1022.210.

provide more information. Payment processors can lower risk by requiring the recipient business to convert and withdraw funds to a verified bank account or to withdraw cryptocurrencies to a compliant cryptocurrency exchange. Processors and transmitters should screen customers, businesses, and Dash addresses against sanctions lists and report suspicious transactions to appropriate regulators. Dash addresses should be screened using chain analysis tools. Substantial CoinJoin Dash use should be investigated by entities and justified by customers.

ABOUT COMPLYFIRST

This report reflects an independent analysis by ComplyFirst and is intended as a tool to help law enforcement, regulators and industry participants understand and evaluate information that may be relevant to AML compliance. ***The report does not reflect a legal conclusion and is no indication of qualitative value of an asset or suitability for investment or any other purpose and is solely for use by the ComplyFirst and not for reliance by any other party.***

ComplyFirst's analytical framework is based on relevant federal law, including FinCEN Guidance issued on May 9, 2019 (FIN-2019-G001). Neither the report nor our framework constitute an exhaustive treatment of the legal and regulatory issues relevant to conducting an analysis of AML compliance and ComplyFirst does not analyze other laws or regulations which may apply. The analysis concerning AML compliance may evolve over time as the nature of digital assets, applicable precedent and FinCEN statements and interpretations change and evolve. ComplyFirst's framework has not been endorsed by FinCEN or any other government authority.

The report is based on a limited review of factual information publicly available or otherwise made available to ComplyFirst. Not all potentially relevant factual information has necessarily been reviewed and no independent investigation or analysis, apart from ComplyFirst's own efforts, has been taken to confirm information on which this analysis is based. We do not assume any responsibility for the completeness of the information upon which our analysis and determination is based. It is possible that if additional facts where known or assumed or understood facts prove to be incorrect, the analysis would be materially different.

DOCUMENT HISTORY

Date	**Description**
11/20/2020	Initial public release
12/7/2020	Terminology changes
05/12/2021	Updates from the Dash team