Digital Asset

Bitcoin (BTC)

December 7, 2020

EXECUTIVE SUMMARY:

Bitcoin (BTC) is the most popular cryptocurrency. It is supported by most cryptocurrency exchanges, wallets, and other services.

Bitcoin transactions are largely transparent, and while most Bitcoin transactions do not include substantial obfuscation techniques, there are several platform-level, second-layer, and even protocol-level privacy enhancements that some users may use. Given this, it is appropriate in our view to consider Bitcoin a privacy-preserving cryptocurrency, or "privacy coin" in certain contexts. Even though most transactions do not use these privacy features, their adoption is in the approximate level of privacy features available for other coins that people typically describe as such. These include Dash and Zcash, which feature optional and/or conditional privacy features. When one considers this, it is inadequate and dismissive to describe Dash and Zcash as "privacy coins"without also including Bitcoin in a similar definition.

Users may decide to use second-layer solutions like the Lightning Network. The Lightning Network allows users to more efficiently transfer funds between selected counterparties. While the privacy implications of this network are still debated, the network can provide greater anonymity in some cases than a public Bitcoin transaction.

Users may also use a platform anonymity-enhancing tool. For instance, in the past, users would send funds to a centralized entity called a "mixer." This mixer would accept funds from other users, and then send random Bitcoin outputs to these participants. Centralized mixing services are still available and used by some, but they are generally frowned upon by Bitcoin users due to their custodial nature. Today, users are more likely to use a more decentralized mixing service provided by an anonymity-enhancing wallet.

Compliance professionals need to be aware of the activities of Bitcoin users. Even though Bitcoin is largely a highly traceable asset with many capable blockchain analysis tools, users may still undertake actions such as mixing or second-layer transactions that increase AML risks.

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 BTC in compliance with FIN-2019-G001.*[1]

BACKGROUND INFORMATION:

Bitcoin launched in January 2009. Bitcoin is the most adopted and well-known cryptocurrency. It was launched by an anonymous individual (or group of individuals) named Satoshi Nakamoto. It is supported on most wallets and exchanges.

Circulating and Total Supply

As of the date of this brief, there are 18.56MM BTC in public circulation with a value of $352.32B.[2] Bitcoin has a fixed total supply of 21 million coins.[3] It is speculated by Coin Metrics that at least 1.5MM BTC are lost, or about 7% of the total supply.[4]

Common usage

Like all cryptocurrencies, the value of BTC 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

[1] *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.
[2] *See* https://coinmarketcap.com/currencies/bitcoin/
[3] *See* https://en.bitcoin.it/wiki/Controlled_supply#Projected_Bitcoins_Long_Term
[4] *See* https://coinmetrics.substack.com/p/coin-metrics-state-of-the-network-d2e

increase in value and can be sold for a profit. As a payment currency, BTC may theoretically be used to purchase any goods and services. However in practice, there are a limited number of vendors accepting BTC, though more accept BTC than virtually all other cryptocurrencies.[5] Bitcoin has been criticised for being expensive to transact at times, with Bitcoin transaction fees occasionally costing more than $5 for quick confirmations.[6]

PRIVACY MECHANISMS:

Bitcoin has limited privacy offered for regular transactions. Regular transactions are protected by pseudonymity only. While addresses and transactions include no direct personal information, they can be connected to personal information quite trivially by counterparties and blockchain analysis software. Quite often, users of Bitcoin who want privacy will use a platform-level application (such as a wallet) that includes anonymity-enhancing features. Usually, this relates to Bitcoin mixing. Bitcoin mixers are interactive tools where users will create transactions in such a way where the links between the origin and destination of funds are not especially clear. Some groups advocate mixing funds regularly. While centralized mixers are still occasionally used, more decentralized CoinJoin mixers are increasingly common. The most popular of these wallets are Samourai Wallet and Wasabi Wallet. Previous users of centralized mixers may instead use no-KYC exchanges.

Though Samourai and Wasabi operate differently, these differences are beyond the scope of this compliance brief. Both non-custodial wallets break user funds into set denominations of BTC (for example, 0.01 BTC, 0.05 BTC, 0.5 BTC). These funds are then mixed with other users of these wallets who desire to also use the mixing feature within the same timeframe. After several rounds of this interactive mixing process, users end with the mixed funds in their wallets. If done correctly, it is difficult to determine the original origin of funds withdrawn from a mixer, or to determine the ending wallet of the starting source of funds. Mixers can be challenging to compliance professionals, since it makes their blockchain analysis tools less reliable. In some cases (especially before Bitcoin implements Schnorr signatures, as described below) chain analysis software can identify transactions related to this decentralized "CoinJoin" mixing process. Depending on which blockchain analysis tool is used, they may tag wallet associations with mixing where known, or tag wallet as having associations with activities related to all participants. Thus, if one user of one of these wallet softwares has funds tagged as related to an undesired activity, then all users who mix with this user may be tagged with this activity, perhaps in addition to being tagged as relating to mixing generally.

Schnorr is a type of signature scheme which will bring slightly greater privacy to Bitcoin.[7][8] Until its implementation, it is trivial to detect transactions created from a multisignature wallet from other transactions. With Schnorr, this is often no longer possible. There are many misconceptions that Bitcoin's forthcoming implementation of Schnorr provides more privacy than it does. For example, it does not enable the "cross-input signature aggregation" feature necessary to make CoinJoin transactions appear as regular (single signer) transactions (albeit still with input amounts still split at set denominations, such as .01 BTC, .05 BTC, etc).[9] With future post-Schnoor protocol-level improvements that may or may not ever be merged into Bitcoin, such as Generalized Taproot and Pay-to-Endpoint (P2EP), it could one day be possible that CoinJoin transactions are largely indistinguishable from regular transactions.[10]

An increasingly common type of CoinJoin transaction is called a "PayJoin" transaction (or "Stowaway" transaction in Samourai Wallet) whereby two users collaborate to make a payment from the first user to the other user.[11] These transactions are less identifiable as CoinJoin transactions on the Bitcoin network since they have only 2 inputs and 2 outputs; thus, they more easily blend into typical Bitcoin spending behavior. BTCPay supports PayJoin.[12]

---

[5] A useful resource of retailers and service providers accepting BTC as payment: https://99bitcoins.com/bitcoin/who-accepts/
[6] *See* https://bitinfocharts.com/comparison/bitcoin-transactionfees.html
[7] *See* https://academy.binance.com/en/articles/what-do-schnorr-signatures-mean-for-bitcoin
[8] *See* https://en.bitcoin.it/wiki/Schnorr
[9] *See* https://bitcointalk.org/index.php?topic=5140134.msg53720057#msg53720057
[10] *See* https://medium.com/digitalassetresearch/schnorr-signatures-the-inevitability-of-privacy-in-bitcoin-b2f45a1f7287
[11] *See* https://en.bitcoin.it/wiki/PayJoin
[12] *See* https://docs.btcpayserver.org/Payjoin/

While not specific to Bitcoin, users may briefly swap their BTC with another cryptocurrency asset through instant exchangers or so-called "Decentralized Exchanges" (DEXs) to mask the origin and destination of funds.[13] These exchanges may have limited or no KYC, especially certain types of DEXs that do not have a clear operator. In fact, many so-called decentralized exchanges are not legal entities at all, but simply software that performs the asset exchanging using purely technical means.[14] The process of obfuscating funds through the (sometimes temporary) use of another coin is called "chain hopping."[15] This is simplest in Ethereum since it has the most DEX infrastructure, but chain hopping is sometimes also done with Bitcoin via underlying "atomic swap" mechanisms that the DEX software utilizes. Chain hopping is best detected by watching for unique transaction amounts, which may persist for specific high-profile transfers. These activities are difficult for blockchain analysis tools to detect, but they are useful in investigations. In some cases however, enough information is available publicly or through a blockchain analysis tool to learn the new received asset by the user and to continue tracing the transaction.

ANTI-MONEY LAUNDERING COMPLIANCE:

BTC presents a curious case for compliance. While most transactions do not use any meaningful anonymity-enhancing feature, a small number of users may attempt to obfuscate the Bitcoin they send and receive. While many users may do this for additional privacy relating to legal activities, some users attempt to obfuscate illegal activities. Entities should watch for these higher risk behaviors and ask additional information of these customers or counterparties if necessary. Through the use of appropriate controls, these heightened risks can be mitigated considerably. These include:

A. Enhanced Due Diligence (EDD)

Intermediaries providing services relating to BTC 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.[16] FinCEN and other regulatory agencies, following the FATF recommendations, indicate that the use of privacy features (including the use of mixers) 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 BTC, this information would not only help the intermediary determine whether that customer is unlikely to use the BTC 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 mixing or other anonymity-enhancing tools 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 BTC anonymity-enhancing tools, for example if this information is already collected or if reasonable limits are already in place. Even so, institutions should try to understand user intent, especially when using or having connections with any anonymity-enhancing tools.

B. Watch for funds related to anonymity-enhanced tools

Since mixing and similar transactions are currently rare, entities should proceed with caution when their customers use these tools. While these tools are not necessarily indicative of illicit use, most chain analysis software that provides support for Bitcoin

[13] *See* https://arxiv.org/abs/1907.12221
[14] See https://www.coincenter.org/theres-no-such-thing-as-a-decentralized-exchange/
[15] *For an example case see* https://blog.chainalysis.com/reports/lazarus-group-north-korea-doj-complaint-august-2020
[16] 31 CFR § 1022.210(d)(1)(iv).

assigns some sort of medium risk score to users who transact using privacy tools. Users who transact using privacy tools might be considered high enough risk to prompt EDD. ComplyFirst provides a free anonymity-enhancing tool questionnaire.

C. 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 setting lower alert thresholds for these customers who also use anonymity-enhancing tools.

D. 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. Many Bitcoin blockchain analysis tools are available; these can be used to observe for any flagged activities. Intermediaries could also require supplemental information from a customer before processing a BTC transaction (e.g., details regarding purpose of a transaction, name and address of recipient, and contact information of recipient) if the transfer is not clearly related to the activities described at onboarding. 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 BTC.

E. 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 transmittor 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 BTC wallet. Since the sending and receiving intermediaries are required to conduct KYC on their respective customers prior to providing services, the use of any particular anonymity-enhancing tool related to BTC therefore does not hinder compliance with the Travel Rule.[17]

Through the mechanisms detailed above, financial intermediaries can indeed allow customers to use services related to BTC in compliance with FIN-2019-G001.[18]

ANTI-MONEY LAUNDERING COMPLIANCE EXAMPLES:

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

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

[18] *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.

A. Cryptocurrency ATM

Cryptocurrency ATM companies should screen customer BTC deposits with chain analysis tools. For users who have funds relating to an anonymity-enhancing tool, companies should ask additional information about the user and deposits. For example, companies may consider collecting the ID and address of users who sell small amounts of Bitcoin, including amounts 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. Substantial anonymity-enhancing tool use should be investigated by entities and justified by customers.

B. Cryptocurrency Exchange

Cryptocurrency ATM companies should screen customer BTC deposits with chain analysis tools. For users who have funds relating to an anonymity-enhancing tool, companies should ask additional information about the user and deposits. ComplyFirst provides a free anonymity-enhancing tool questionnaire. 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. Customers and their requested BTC withdrawal addresses should be screened against sanctions lists and other undesired activities. 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 anonymity-enhancing tool use should be investigated by entities and justified by customers.

C. Payment Processor or Money Transmitter

Payment processors may choose to only allow Bitcoin payments from customers in low-risk geographies to entities in low-risk geographies. Payment processors should more closely scrutinize the businesses that receive Bitcoin payments, possibly prohibiting high-risk business types from accepting Bitcoin payments or requiring these businesses to 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 Bitcoin addresses against sanctions lists and report suspicious transactions to appropriate regulators. Bitcoin addresses should be screened using chain analysis tools. Substantial anonymity-enhancing tool 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
11/30/2020	Initial public release
12/7/2020	Terminology changes