ComplyFirst

COMPLIANCE BRIEF

Digital Asset

Zcash (ZEC)

December 7, 2020

EXECUTIVE SUMMARY:

The Zcash cryptocurrency is commonly seen as being a privacy-preserving cryptocurrency (or "privacy coin"). It offers four different types of transactions with its ZEC value token, each with different anonymity protections. This is because funds are stored in either a transparent *t-address* (which are very similar to Bitcoin addresses) or a shielded *z-address*.[1] Users can create transactions to and from any of these address types. Transacting from a t-address to a z-address is known as a shielding transaction, and allows blockchain observers to see the origination address but not the destination address. Likewise, transacting from a z-address to a t-address is known as a deshielding transaction, where blockchain observers cannot see the origination address, but are able to see the destination address. Fully shielded transactions, where a z-address sends to another z-address, are those most similar to Monero transactions. This is the only transaction type that hides the sender, receiver, and amount. Transparent transactions (t-address to t-address) transmit the majority of the network value and constitute the majority of transactions; they are to all intents and purposes the same as transparent Bitcoin transactions. Like Bitcoin, zcash supports multisignature ("multisig") transactions for transparent t-addresses, but not for z-addresses.[2] Work is ongoing to allow for use of multisig with z-addresses.[3]

While the privacy protections for fully-shielded transactions are similar to Monero transactions, they accomplish this privacy using a mathematical proving system known as zk-SNARKs. Zcash proponents argue that fully-shielded transactions provide a high degree of privacy, including possibly better protections against targeted surveillance than Monero. However, users of shielded addresses often reveal information via their interactions with transparent addresses, sometimes through mandated transparent migrations (*turnstile migrations*).[4] This revealed information is useful to law enforcement and institutions to track users who use shielded addresses.

ZEC is transferred to a shielded address by creating a *note*, which is an encrypted chunk of data that specifies an amount and destination address (which owns the value). When mined, a *note commitment* is generated on the blockchain, which may be spent by the owner of the shielded address (who is in possession of the address' private spend key) through the creation of a *note nullifier*. A note nullifier is a proof that demonstrates that the spender owns the private key for that address without disclosing the identity of the spender or specifics of the transaction to others. A Zcash transaction can include transparent inputs, outputs and scripts (similar to Bitcoin), as well as several types of *descriptions*, which allow the transaction to process shielded value by taking in shielded input notes and/or producing shielded output notes as necessary.[5]

Zcash z-addresses feature a *viewing key*, which allows users to share information about the incoming and outgoing transactions of that address with others, without having to expose their private spend key[6]. This viewing key reveals the wallet balance, value of transfers in and out of the wallet, and addresses that funds are sent to. It does not reveal the shielded addresses that the wallet receives funds from, if applicable. These view keys can be shared with a third-party to enable users, financial intermediaries and financial institutions to disclose certain transaction details associated with a given account without publicly disclosing that user's transactional information. Financial intermediaries and institutions can require up-front disclosures as part of their registration process

[1] *See* https://z.cash/technology/
[2] *See* https://z.cash/support/faq/#multisig-support
[3] *See* https://www.zfnd.org/blog/kzen-multisig/
[4] *See* https://electriccoin.co/blog/sapling-addresses-turnstile-migration/
[5] *See* https://zips.z.cash/protocol/protocol.pdf
[6] *See* https://electriccoin.co/blog/explaining-viewing-keys/

and on an ongoing basis to meet their obligations, though this is advised only in specific, higher-risk cases due to the worsened user experience.

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 ZEC in compliance with FIN-2019-G001*.[7]

BACKGROUND INFORMATION:

Zcash launched in October 2016, Zcash was the creation of researchers and developers who built a standalone coin from the Zerocash research paper. Zcash is currently based on the Bitcoin codebase with additional privacy features added, but efforts are being made to implement a new, independent Rust codebase. Zcash's primary maintainers are the Electric Coin Company (previously the Zcash Company) and the Zcash Foundation. Both entities receive a portion of the block reward. Zcash originally launched with its shielded protocol, Sprout. Today, shielded transactions use the newer and more efficient Sapling protocol with similar privacy protections.

Most Zcash transactions are functionally the same as Bitcoin transactions, with a publicly known sending address, receiving address, and amount.

Circulating and Total Supply

As of the date of this brief, there are 10.64MM ZEC in public circulation with a value of $788.37MM.[8] Like Bitcoin, Zcash has a fixed total supply of 21 million coins.[9] Approximately 536,000 ZEC is held in the shielded Sapling pool (~5% of current ZEC supply).[10]

Common usage

Like all cryptocurrencies, the value of ZEC 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, ZEC may theoretically be used to purchase any goods and services. However, in practice, there are a limited number of vendors accepting ZEC.[11] At the time of this writing, virtually all merchants and services support transparent Zcash addresses, with a smaller but increasing number (such as VPN provider PIA[12] and exchange Gemini[13]) supporting shielded addresses as well.

PRIVACY MECHANISMS:

Zcash's zk-SNARK proving system offers privacy to users of select wallets that support shielded transactions. Shielded transactions in the initial version of Zcash (codenamed "Sprout") were rather slow to generate and had considerable RAM requirements. The newer Sapling implementation (activated in 2018) is much more efficient in size and speed, and transactions are not prohibitively large.[14] Both Sprout and Sapling required trusted setups for their launches. Due to this, Zcash users must trust that the original participants of the trusted setups did not collude to print undetected funds. However, even an extreme case of a compromised trusted setup should not directly compromise privacy.

Fully shielded transactions are usually the types of transactions that people refer to when discussing Zcash, though they only are approximately 4.7% of all Zcash transactions at the type of writing.

---

[7] *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.
[8] *See* https://coinmarketcap.com/currencies/zcash/
[9] *See* https://zcash.readthedocs.io/en/latest/rtd_pages/basics.html
[10] *See* https://explorer.zcha.in/statistics/values
[11] A useful resource of online retailers and service providers accepting ZEC as payment can be found at https://paywithz.cash/
[12] *See* https://www.privateinternetaccess.com/blog/private-internet-access-now-accepts-anonymous-zcash-shielded-payments/
[13] *See* https://www.theblockcrypto.com/linked/79098/gemini-supports-shielded-zcash-withdrawals
[14] *See* https://www.coindesk.com/zcashs-next-upgrade-to-make-private-transactions-100x-lighter-and-6x-faster

Most Zcash transfers are either transparent (like Bitcoin, ~80.3%), or partially shielded (~14.9%).[15] Fully shielded transactions hide the sender, receiver, and amount especially well, including much better transaction graph protection than Monero and other coins in theory. (Although in practice, shielded activity may be identifiable via transaction clustering heuristics.[16])

ANTI-MONEY LAUNDERING COMPLIANCE:

ZEC presents a curious case for compliance, with often-used transparent transactions and less-frequent shielded transactions. Especially since Zcash shielded transactions are not commonly used, these transactions pose an inherent AML risk in the approximate range of the use of Bitcoin privacy tools such as mixers. If fully shielded transactions are widely adopted to cover a wider set of speculators, miners, and other users, they may instead pose an AML risk in the approximate range of traditional payment types such as cash, card, 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 ZEC 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. Higher-risk users may be more likely to transact in transparent Zcash than Bitcoin because of a misconception of Zcash privacy features. *However, illicit usage of Zcash in general does not currently appear to be common.*[18] 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 ZEC, this information would not only help the intermediary determine whether that customer is unlikely to use the ZEC 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 ZEC 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 ZEC, for example if this information is already collected or if reasonable limits are already in place.

B. Watch for shielded funds

Since fully shielded transactions on the network are currently rare, entities should proceed with caution when users hold funds in shielded addresses. While this is not necessarily indicative of illicit use, most chain analysis software that provides support for Zcash assigns some sort of medium risk score to users who transact using shielded addresses. Users who transact using shielded addresses might be considered high enough risk to prompt EDD requirements similar to the EDD entities would conduct for users of Bitcoin mixing tools. In both cases, users most likely would have opted in to having greater privacy protections. This may change in the future if more Zcash wallets support shielded

[15] Data calculated from the "Past Month" row at https://explorer.zcha.in/statistics/usage as of 11/18/2020; alternatively see https://forum.zcashcommunity.com/t/measuring-shielded-adoption/35022

[16] See https://www.usenix.org/system/files/conference/usenixsecurity18/sec18-kappos.pdf

[17] 31 CFR § 1022.210(d)(1)(iv).

[18] See https://www.rand.org/pubs/research_reports/RR4418.html

transactions by default and if these sort of transactions become more common and thus a less useful risk indicator.

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 prohibiting customers who are in higher risk categories or geographies from accessing and or using ZEC-related services (and especially ZEC shielded services).

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. In addition, there are a number of private blockchain-specific monitoring tools which may be employed. However, none of these have had much success at monitoring activities in the Monero protocol due to its privacy-centric design.[19] Intermediaries could also require supplemental information from a customer before processing a ZEC 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 ZEC. Finally, and arguably as a last resort, an intermediary could limit all incoming and outcoming transactions involving ZEC 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.

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 ZEC 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 ZEC therefore does not hinder compliance with the Travel Rule.[20]

F. ZEC-specific controls - disclosure of the viewing key

As discussed earlier, users can reveal a ZEC transaction's details that are specific to their account via key-based functionality that is built into the Zcash protocol. Specific keys can be shared with any third-party to grant insight into the account associated with the keys.

[19] *See* https://beincrypto.com/chainalysis-adds-dash-monero-still-too-strong/
[20] *See* https://getmonero.org/2019/12/05/funds-travel-rule.html

This enables users, financial intermediaries and financial institutions to disclose certain transaction details associated with a given account to a third-party, without publicly disclosing that user's transactional information. In addition, financial intermediaries and institutions can require up-front disclosures as part of their registration process and on an ongoing basis to meet their obligations. Institutions should bear in mind that while this option is available, disclosure of this information adds friction on both ends, and is most likely not needed except for high-profile investigations, for example at the request of law enforcement.

Through the mechanisms detailed above, financial intermediaries can indeed allow customers to use services related to ZEC in compliance with FIN-2019-G001.[21]

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 shielded Zcash purchases and sales 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. Zcash transparent addresses should be screened using chain analysis tools; customers and all Zcash addresses should be screened against sanctions lists. Substantial shielded Zcash use should be investigated by entities and justified by customers.

B. Cryptocurrency Exchange

Cryptocurrency exchanges may decide to only allow shielded Zcash deposits, withdrawals, and trades 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 Zcash, or to trade Zcash with higher limits. Customers and their requested Zcash 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 shielded Zcash use should be investigated by entities and justified by customers.

C. Payment Processor or Money Transmitter

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

[21] *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.

should screen customers, businesses, and Zcash addresses against sanctions lists and report suspicious transactions to appropriate regulators. Zcash transparent addresses should be screened using chain analysis tools. Substantial shielded Zcash 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