Zcash Regulatory & Compliance Brief

June 2020

Introduction

This note is intended to provide an overview of Zcash for regulators, policy-makers, and compliance professionals.

Zcash is an open-source, decentralized virtual currency, similar in nature to Bitcoin, which protects users’ privacy through the use of an innovative cryptographic technique based on zero-knowledge proofs.

Zcash is fully compliant with the anti-money laundering and terrorism financing (AML / CFT) requirements set forth in the FATF Recommendations adopted in June 2019. Required originator and beneficiary information can be attached directly to shielded Zcash transactions, facilitating compliance with Travel Rule requirements.

Zcash is listed on many of the world’s largest virtual currency exchanges, under the ticker “ZEC”.

Confidentiality & Privacy

Personal financial information can reveal a huge amount of information about the subject, including how much they earn, where they shop, what newspapers, magazines and websites they subscribe to, their hobbies and interests, what causes they donate to, and how much they have saved.

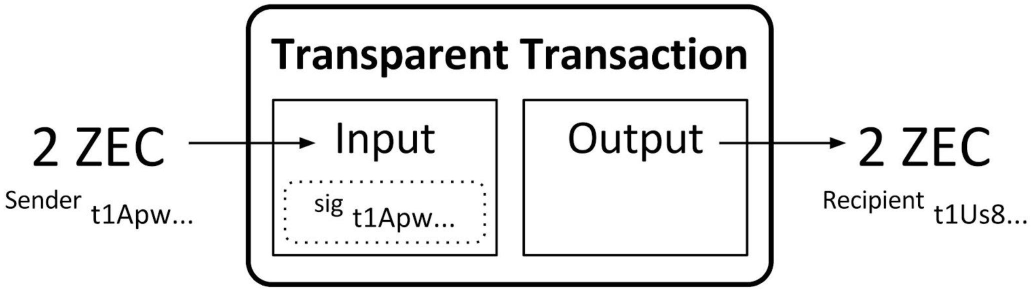
Governments of the world's largest economies have recognised the importance of personal financial privacy, and have enacted legislation to protect it. Examples include the Gramm-Leach-Bliley Act in the United States, the EU's General Data Protection Regulation, and Japan’s Act on the Protection of Personal Information. The growing threat from cyber-criminals and identity thieves, and high profile incidents such as the Experian data breach have raised public awareness of the importance of robust privacy protections.

> It is the policy of the Congress that each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers’ nonpublic personal information. (Gramm-Leach-Bliley Act)

First-generation blockchain technology (as implemented in Bitcoin) requires that the sender’s and recipient’s payment addresses, and the amount being transferred, is revealed on the blockchain. As a result, any third-party observer who knows a Bitcoin user's payment address can see all the transactions received and sent by that address.

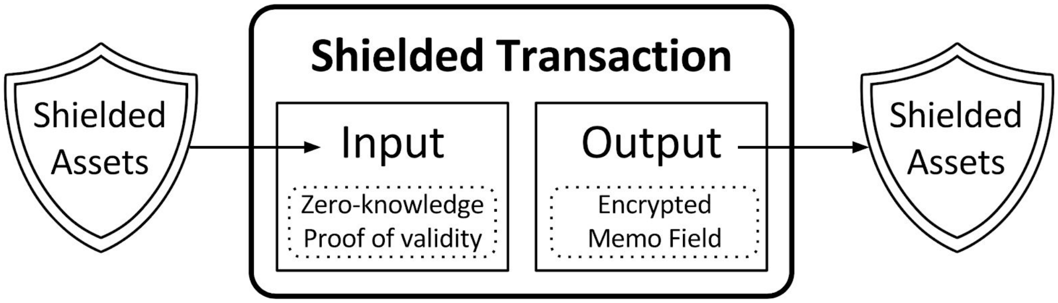
Zcash addresses this issue by giving users the option of shielding their funds and transacting them privately. To this end, Zcash supports two types of transaction: transparent and shielded.

Transparent payment addresses are known as t-addresses (as they always start with a `t`). Transactions between t-addresses are similar in nature to Bitcoin transactions - the t-addresses of both the sender and the recipient, as well as the amount being transferred, are visible on the blockchain.



Zcash has re-used the Bitcoin protocol for its t-addresses and transparent transactions, making it simple and straightforward to add support for Zcash to existing transaction monitoring systems.

If a user prefers to transact privately, she can *shield* her funds, by transferring them to a z-address (so named because they always start with a `z`). Shielded funds held in a z-address are no longer visible on the public blockchain, and can be transferred to another z-address using a shielded transactions, which preserves the privacy of both the Sender and the Recipient, as well as keeping the amount transferred confidential.



Shielded funds can be subsequently *unshielded* again, by transferring them to a t-address, which reveals them to the public blockchain once more.

The use of z-addresses is entirely optional. Virtual asset service providers (VASPs), such as exchanges and payment processors, can choose to accept deposits, make payments or allow withdrawals using either or both transparent or shielded transactions.

z.cash

Anti-Money Laundering & Terrorist Financing

Zcash has been designed to be compatible with the AML / CFT measures recommended by the Financial Action Task Force on Money Laundering (FATF), including customer due diligence, record-keeping, reporting suspicious transactions, and providing required originator and beneficiary information for virtual asset transfers between VASPs (often referred to as the “Travel Rule”).

Zcash is also compatible with the requirements imposed by the EU’s Fifth Money Laundering Directive, and the United States’ Anti-Money Laundering regulations.

Customer Due Diligence (CDD)

Under the FATF recommendations, VASPs are required to undertake CDD measures when establishing a business relationship. The fact that a VASP supports Zcash or that a customer intends to trade Zcash does not impact the VASP’s ability to carry out CDD checks.

In this respect, Zcash is no different from other virtual currencies such as Bitcoin or Ethereum, and VASPs can apply the same CDD processes.

Transaction monitoring

Zcash’s privacy-preserving technology does not prevent a VASP from being able to monitor a customer’s transactions with that VASP (e.g. deposits, withdrawals, trades), and comparing transaction patterns and volumes with the expected behaviour, based on the VASP’s understanding of the nature of the customer or their business (as determined during the CDD checks).

As a party to its customers’ Zcash transactions (either as a recipient, in the case of deposits, or a sender, in the case of withdrawals), a VASP has visibility of the transaction details. This allows the VASP to detect transaction patterns that do not match that customer’s expected behaviour, and investigate further to determine whether the unexpected behaviour is suspicious.

Zcash requires the use of payment addresses for all transactions. This allows VASPs to issue a unique deposit address to each customer, thus allowing Zcash deposits to be unequivocally attributed to a specific customer. Zcash also requires that customers provide a payment address in order to receive withdrawals, allowing VASPs to conduct sanctions screening, or restrict withdrawals to whitelisted addresses.

In this respect, Zcash is no different from other virtual currencies, and the same tools and procedures for transaction monitoring can be applied to Zcash.

Blockchain Analytics

Because Zcash re-uses the Bitcoin protocol for transparent transactions, transactions set between transparent addresses are visible on the Zcash blockchain. Chainalysis and Elliptic provide support for analyzing transparent Zcash transactions.

Record-keeping

In the same way that VASPs can monitor a customer’s Zcash transactions, they can also keep records of those transactions.

For deposits, VASPs can record the customer’s identity, the amount of Zcash that was deposited, the destination address (i.e. the deposit address the VASP created for that customer), the source address (where the customer deposits funds from a t-address), and the transaction ID.

For withdrawals, VASPs can record the customer’s identity, the amount of Zcash that was withdrawn, the source address (i.e. the VASPs’s address from which the coins are being sent), destination address (whether it is a t-address or a z-address) and the transaction ID.

It is important to note that the VASP always knows the payment address that a Zcash withdrawal is sent to.

The only difference between Zcash and other virtual currencies in terms of the information available to be recorded by the VASP is that if the customer makes a deposit from a z-address, the VASP will not automatically have visibility of the source address. If it wishes to do so, the VASP can request that the customer provide the source address for the VASP’s records. However, this is not a requirement under the FATF Recommendations.

Suspicious Transaction Reports

The ability to carry out transaction monitoring ensures that a VASP is able to detect any suspicious activity on the part of its customers. The ability to maintain records of its customers’ transactions ensures that the VASP possesses adequate information to make suspicious transactions reports where appropriate.

Travel Rule

Zcash was designed to be compliant with the Travel Rule. The required originator and beneficiary information can be attached directly to a shielded transaction using the encrypted memo field. As the name implies, the contents of this field are encrypted when the transaction is added to the blockchain, thus preventing inappropriate or unauthorised disclosure of personal information.

The AML / CFT Risk Associated with Zcash is Low

In May 2020, the RAND Corporation released a report detailing the findings of a study into the extent to which Zcash is used for illicit or criminal purposes.

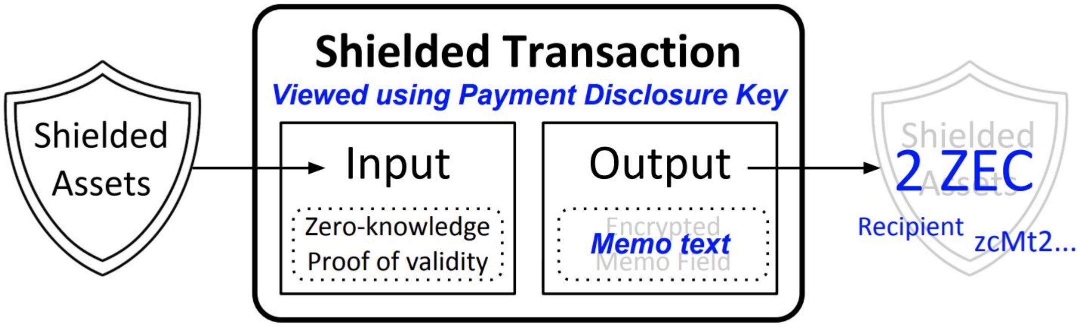
The study found no credible evidence pointing to large scale use of Zcash for money laundering, terrorism financing or the trade in illicit goods and services. Furthermore, despite the intuitive benefits of privacy coins to conducting illicit or criminal transactions, Zcash does not have a significant presence on the dark web marketplaces, and the less private Bitcoin is the most dominant cryptocurrency on the dark web.

Sharing Visibility of Shielded Transactions with Third Parties

On occasion, it may be necessary to share shielded transaction information with third parties. The Zcash protocol has been designed to support two features that enable the disclosure of shielded transaction information.

The first is **Viewing Keys**. The owner of a z-address can create a Viewing Key, which they can then share with a third party. Anyone who possesses the viewing key for a z-address can use it to view all transactions sent to or from that z-address. Viewing key functionality is fully-supported.

The second feature that enables sharing of shielded transaction information is known as **Payment Disclosure**. This feature is similar in nature to Viewing Keys but, instead of providing visibility of all transactions sent and received by a z-address, it provides visibility of a single transaction. The sender or recipient of a shielded transaction can generate a payment disclosure key which allows a third party to view certain details of the transaction (specifically the recipient's z-address and the contents of the Encrypted Memo Field).



Payment disclosure is an experimental feature and is not yet fully enabled in the Zcash software for the most recent version of the protocol (Sapling). Here are some examples of transactions that use an older version of the protocol (Sprout), that can be viewed using the third-party Blockchair blockchain explorer, which supports the experimental payment disclosure feature:

- Example Transaction 1: Public View and with Payment Disclosure
- Example Transaction 2: Public View and with Payment Disclosure
- Example Transaction 3: Public View and with Payment Disclosure
- Example Transaction 4: Public View and with Payment Disclosure

The fourth example demonstrates how Travel Rule information can be attached to a shielded Zcash transaction.

These features will allow VASPs to share visibility of shielded transactions and z-addresses with appropriate authorities or auditors in a confidential manner. We also anticipate that they may be leveraged as part of information-sharing arrangements amongst VASPs, or between VASPs and statutory regulators, to facilitate market surveillance and the identification of suspicious transactions.

z.cash

Development

Zcash was developed over the course of several years, and launched in late 2016 by the Electric Coin Company (ECC), a Delaware corporation. ECC was financed with $3 million in funding from reputable and well-known investors, including Pantera Capital, Fenbushi Capital, and Naval Ravikant.

The team behind Zcash includes respected professors and academic researchers from MIT, Johns Hopkins University, Technion, and Tel Aviv University[1] whose work was funded in part by DARPA, the US Air Force Research Laboratory, and the Office of Naval Research.

The ECC team provides technical coordination and leadership, and a point of contact for both users and regulators. Importantly, the ECC team investigates and responds to issues and bugs, and provides information and support to Zcash's users through online channels, including GitHub, forums and chat.

ECC works in partnership with the independent Zcash Foundation, which was granted 501(c)3 public charity status in October 2017. The Foundation's chairman is Andrew Miller, who is an assistant professor at the University of Illinois, and associate director of the Initiative for Cryptocurrencies and Contracts (IC3) at Cornell.

The Foundation's mission is to build internet payments and privacy infrastructure for the public good. It complements the work of ECC by funding independent research and development relating to Zcash.

Conclusion

Zcash was designed to protect consumers' financial privacy while retaining compatibility with global AML / CFT standards, including the FATF Recommendations that were adopted in June 2019, the EU's Fifth Money-Laundering Directive, and the United States' Anti-Money Laundering regulations.

Importantly, the privacy provided by Zcash does not prevent regulated entities from fulfilling their regulatory obligations.

An independent study by the RAND Corporation published in March 2020 found that there is no evidence of widespread illicit use of Zcash.

A large percentage of Zcash trading in the United States occurs on exchanges that are registered with FinCEN as money service businesses (MSBs), including Kraken, Poloniex, Coinbase, and Gemini. The latter two exchanges also hold a New York state BitLicense.

In May 2018, the New York Department of Financial Services (NYDFS) issued a press release explaining their decision to grant Gemini permission to provide custodial and listing services for Zcash. Of note, the NYDFS stated that, "Virtual currency license applicants are subject to a rigorous review of anti-money laundering, capitalization, consumer protection and cyber security standards."

[1] Ben-Sasson, E., Chiesa, A., Garman, C., Green, M., Miers, I., Tromer, E., Virza, M.: Zerocash: Decentralized anonymous payments from bitcoin. In: Security and Privacy (SP), 2014 IEEE Symposium on. pp. 459–474. IEEE (2014)

The Electric Coin Company engages proactively, constructively, and cooperatively with policy-makers and regulators. We aim to provide accurate and objective information to help inform and support a risk-based approach to regulation. We welcome the opportunity to discuss regulatory or compliance concerns, and answer questions relating to how the Zcash works, and its implications for AML / CFT compliance.

To discuss any of the issues covered in this note, please contact Jack Gavigan (regulatory@z.cash).

z.cash