Zcash Regulatory & Compliance Brief

April 2019

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

Introduction

Zcash is an open-source, decentralized virtual currency, based on the Zerocash protocol, an innovative cryptographic technique for adding privacy to a blockchain-based digital currency by using zero-knowledge proofs.

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. With Zcash, users have the option of shielding their funds, and transacting them privately.

Zcash is listed on many of the world's largest virtual currency exchanges, under the ticker "ZEC".

Confidentiality & Privacy

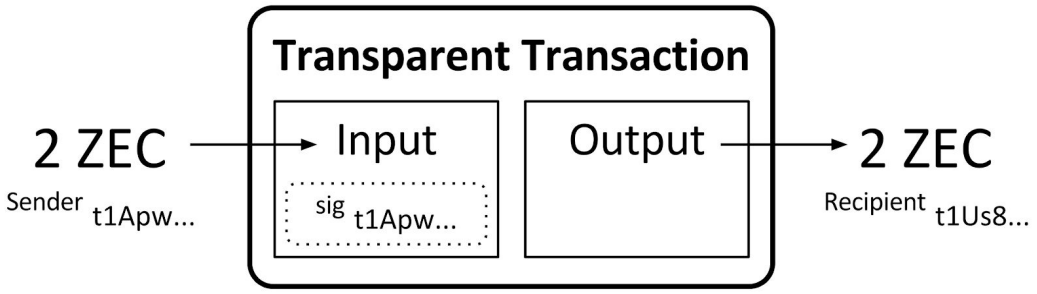
Personal financial information can reveal a huge amount of information about the subject, including how much they earn, where they shop, what newspapers, magazines and websites they subscribe to, their hobbies and interests, what causes they donate to, and how much they have saved.

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)

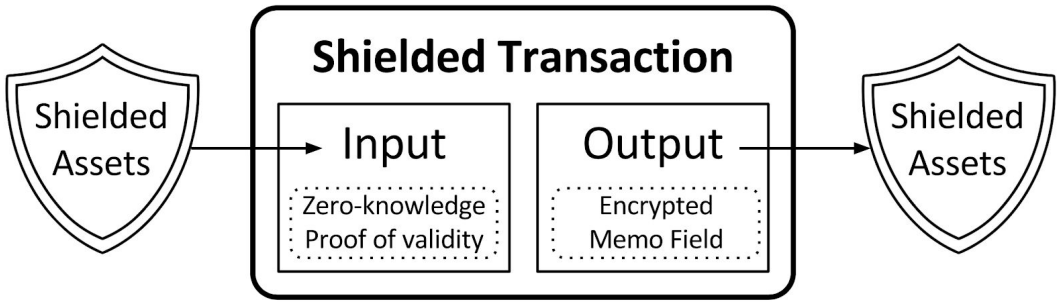
Zcash addresses this issue by supporting two types of transaction: transparent and shielded.

Transparent payment addresses are known as t-addresses (as they always start with a `t`).Transactions between t-addresses are very 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 analysis products and services.

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 shielded transactions, which preserve 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 virtual currency exchanges and payment processors, can choose to accept deposits, make payments or allow withdrawals using either or both transparent or shielded transactions.

Anti-Money Laundering & Terrorist Financing

The Zcash currency has been designed to be compatible with the anti-money laundering and terrorist financing (AML/CFT) measures recommended by the Financial Action Task Force on Money

Laundering (FATF), including rigorous customer due diligence checks (CDD), comprehensive record-keeping, and making Suspicious Activity Reports (SARs) when appropriate.

From an AML/CFT perspective, Zcash is similar in nature to cash. The techniques and processes that have been honed and perfected over decades to detect and discourage the use of cash transactions for money laundering and terrorist financing can be applied to shielded Zcash transactions.

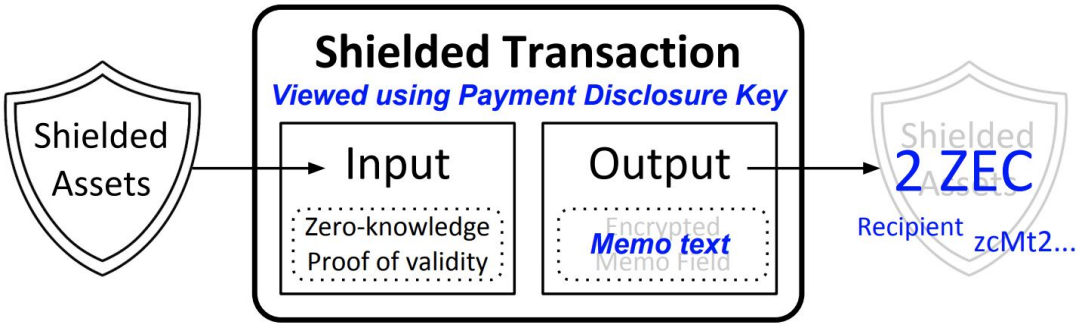
Like most virtual currencies, the Zcash protocol requires the use of payment addresses for all transactions. Payment addresses are unique addresses that are used to receive, hold and send Zcash coins. This allows VASPs to issue a unique payment address to each customer for their exclusive use when depositing funds, which means that each deposit can be attributed to a specific customer. It also requires that customers provide a payment address in order to receive payments or withdrawals from a VASP. This enables record-keeping and transaction monitoring, both of which are necessary to enable the detection and reporting of suspicious transactions. It also allows VASPs to prevent customers from withdrawing funds to payment addresses that have been identified as being associated with sanctioned persons or organizations.

FATF also recommends that originator and beneficiary information be attached to wire transfers. In the United States, this recommendation is implemented as the Bank Secrecy Act's Travel Rule. Zcash enables compliance with the Travel Rule through the use of an Encrypted Memo Field, which allows the sender of a shielded transaction to send information along with the transaction. As the name implies, information in the Encrypted Memo Field is encrypted such that it is only visible to the recipient.

Sharing Visibility of Shielded Transactions with Third Parties

On occasion, it may be necessary to share 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 known as Payment Disclosure. This allows either party to a shielded transaction to generate a key which they can provide to a third party, thereby allowing them to view the details of the transaction (including the contents of the Encrypted Memo Field), while ensuring that it remains shielded from the world at large.



The second feature is the ability for the owner of a z-address to create a Viewing Key, which can be shared with a third party who can then use it to view all transactions sent to and/or from that z-address.

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, as part of self-regulatory efforts, or between VASPs and statutory regulators, to facilitate market surveillance and the identification of suspicious transactions.

Governance

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, bugs and problems, and provides information and resources support to Zcash's users through a number of online channels, including GitHub, online forums and chat.

ECC works in partnership with the independent Zcash Foundation, which was formed in March 2017 and was granted 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.

Consumer Protection

Zcash was designed to align the incentives of its developers with those of its users. Like Bitcoin, the Zcash monetary supply is capped at 21 million coins, which are released over time, according to a schedule embedded in the Zcash protocol. Most of the coins (90%) are distributed to the miners who maintain the Zcash blockchain. The remaining 10% are released to ECC over the first four years of the currency's operation. These coins (commonly referred to as the Founders' Reward) are distributed to ECC's shareholders and the Zcash Foundation.

[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)

This approach reduces the risk of consumer harm by ensuring that no single individual, group or company controls a significant amount of Zcash coins. Furthermore, it ensures that ECC is incentivized to support the development and growth of Zcash over the long-term. The latter is intended to foster high level of stability and confidence, that appears to be absent in virtual currencies with less clearly-defined governance and incentive structures.

Conclusion

Zcash was designed to protect consumers' financial privacy while retaining compatibility with global AML/CFT standards. Importantly, the privacy provided by Zcash does not prevent regulated entities from fulfilling their KYC/AML obligations.

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 states that, "Virtual currency license applicants are subject to a rigorous review of anti-money laundering, capitalization, consumer protection and cyber security standards."

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