Zcash Regulatory & Compliance Brief

Background

Zcash is an open-source, decentralized virtual currency, based on the Zerocash protocol, an innovative technique for adding privacy to blockchain-based digital currencies using zero-knowledge proofs. It was developed over the course of several years, and launched in October 2016 by the Zerocoin Electric Coin Company LLC ("ZcashCo"), a Delaware corporation. ZcashCo was financed with $3 million in funding from reputable and well-known investors, including Pantera Capital, Fenbushi Capital, and Naval Ravikant.

The team at ZcashCo 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.

Since launching in October 2016, Zcash has reached a market capitalisation of over $1bn. A large portion of Zcash-related exchange activity occurs on state-regulated exchanges and/or exchanges that are registered with FinCEN as money service businesses (MSBs). Though ZcashCo cannot control which exchanges list Zcash, it is important to ZcashCo that the proportion of regulated exchanges selling Zcash continue to grow. ZcashCo continues to educate regulated exchanges wishing to list Zcash to ensure that they have the information needed to meet their regulatory and consumer protection obligations.

On May 14, 2018, the New York Department of Financial Services (NYDFS) issued a press release explaining their decision to grant Gemini custodial and listing services for Zcash. That press release is available here: https://www.dfs.ny.gov/about/press/pr1805141.htm. 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." While the specific criteria used by NYDFS is unknown, ZcashCo did meet and provide information to the NYDFS as part of their process.

Governance

The ZcashCo team provides technical leadership and a point of contact for both users and regulators. Importantly, the ZcashCo 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.

---

[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)

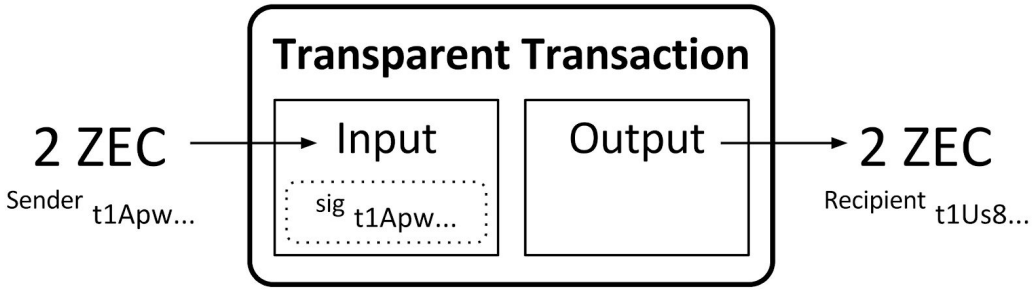
ZcashCo works in partnership with the independent Zcash Foundation, which was formed in March 2017 and was granted granted 501(c)3 public charity status in October 2017. The Foundation's chairman is Andrew Miller, who is an assistant professor at the University of Illinois, and associate director of 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. In time, responsibility for developing the Zcash protocol is expected to transition from primarily ZcashCo to a decentralized development process led by the Foundation.

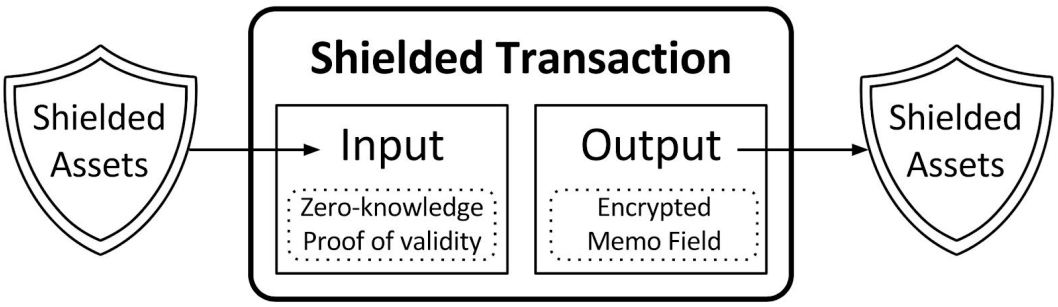
Confidentiality & Privacy

Zcash supports two types of transaction: transparent and shielded. Money services business (MSBs), such as virtual currency exchanges and payment processors, can opt to accept deposits and make payments or allow withdrawals via one or both methods.

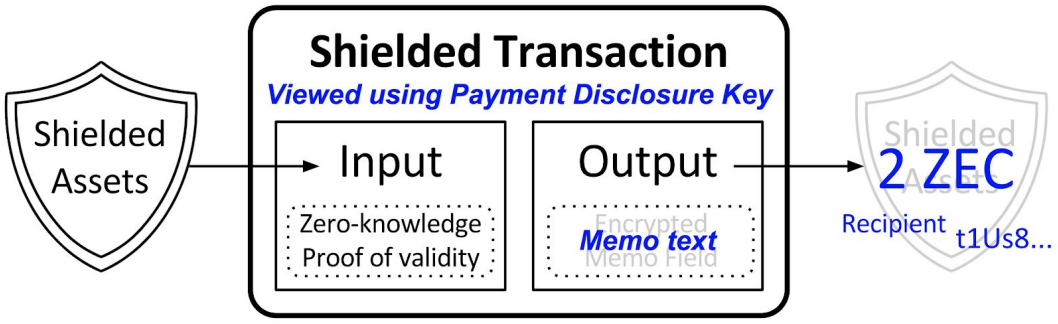
Transparent transactions are identical in nature to bitcoin transactions - the payment addresses of both the sender and the recipient, as well as the amount being transferred, are visible on the blockchain. Zcash has re-used the bitcoin protocol for its transparent transactions, making it simple and straightforward to add support for Zcash to existing transaction analysis products and services.



If a user opts to shield her funds, they are no longer visible on the blockchain. Once shielded, funds can be transferred using shielded transactions, which preserves the privacy of both the Sender and the Recipient. This facilitates compliance with regulations that mandate privacy for personal financial information, such as the Gramm-Leach-Bliley Act in the US, and and the General Data Protection Regulation in the EU. An encrypted memo field allows the Sender to attach information to a shielded transaction, facilitating compliance with the Bank Secrecy Act's "Travel" rule.



A “Payment Disclosure” feature was recently released. This allows either party to a shielded transaction to generate a viewing key which they can provide to a third party, thereby allowing them to view the details of the transaction, while ensuring that it remains shielded from the world at large.



This will allow users to provide evidence regarding the source of funds, which can be verified by using the viewing key to decrypt the transaction on the Zcash blockchain, without compromising users' privacy or leaking any personally identifiable information. This process can be automated by adding support for Payment Disclosure viewing keys to transaction analysis products and services, allowing MSBs to automatically record the source and counterparty details for all shielded transactions, while ensuring that their customers' personal financial information is protected.

Consumer Protection

Zcash was designed to align the incentives of its developers with those of its users. Like bitcoin, Zcash’s 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 ZcashCo over the first four years of the currency’s operation. These coins are distributed to ZcashCo’s shareholders and the Zcash Foundation.

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 ZcashCo 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.

Links

- Zcash homepage: https://z.cash/
- Zcash Foundation: https://z.cash.foundation/