Anonymity v Bitcoin: a delve into the world of privacy coins

06 MARCH 2018

Elisa Wahnon
ASSOCIATE | UK

CATEGORY:
ARTICLE

The Ceremony aka creation day for 'Zcash', an alternative cryptocurrency, was an elaborate affair. It involved six participants in six separate locations around the world setting up highly secure stations from which to create a part of the secret key that generated the currency Zcash. Apparently Zooko Wilcox, the master of the Ceremony and leader of Zcash, also wore a Gandalf hat to mark the wizardry of it all.

The problem with Bitcoin

Zcash offers a solution to the issue of privacy that continues to plague Bitcoin. Bitcoin transactions are open for all users to see and verify before they are added to the blockchain, which serves as public ledger. Users have pseudonyms that in theory are meant to hide their identities. This is why the currency was initially famous for being a money-laundering mechanism for fraudsters, drug dealers and the like.

However, it turns out that this pseudonym can be matched to its human user more easily than one would expect and once it is, that person's entire transaction history can be traced on the public ledger. This would be akin to the whole world seeing your bank statement.

So whilst this is good news in terms of tracking down criminals who hold Bitcoins it is likely to still make most regular Joes feel uneasy. It also allows fraudsters to look at the public ledger and target wealthy individuals.

Zcash runs on similar blockchain technology except the transactions on it are completely anonymous. A mathematical invention called a 'zero knowledge proof' proves that a Zcash transaction is true, without revealing any details about it. This allows the currency to be legitimate whilst the hiding the value of the transaction as well as the identities of the sender and recipient.

A crypto Ceremony

The Ceremony was a necessary way to start Zcash because the maths used to create it was vulnerable to attack. In order to create the currency, Wilcox had to produce a very large alphanumerical key, which formed the basis of the mathematical wizardry that generated Zcash. The problem was if someone got hold of this key they could counterfeit the currency and users would not be able to tell since all Zcash transactions are anonymous.

To overcome this, Wilcox split the task of creating the key with five other people. On 22 October 2016 (creation day), they took pains to ensure they were not being tracked by hackers. They dumped their smartphones in favour of good old-fashioned paper road maps and bought a new computer to ensure no hacker could have already implanted any malware on it.

They got all of this to a random hotel room, filmed the whole generation of the key with surveillance cameras and then physically destroyed the computer to make sure no one could ever get hold of the secret key. They then uploaded this footage online to prove to users that the Ceremony had not been compromised and therefore Zcash was safe to use.

The currency was created a few days later and had an overwhelming response. It is now one of the best performing cryptocurrencies.

Alternative coins

Zcash is not the only cryptocurrency that has attempted to address some of the privacy failings in Bitcoin – though perhaps it had the most dramatic creation.

Dash, another privacy-focused cryptocurrency, uses 'CoinJoin'. This is an anonymization method by which several users agree to join a single transaction where some of the outputs of the transaction have the same value. This means that a person looking at the blockchain (or public ledger) cannot see which output of the transaction relates to which sender, thus providing a further layer of anonymity.

Dash grew by 9,265% in 2017 making it one of the best performing cryptocurrencies of the year. By comparison, Bitcoin grew by 1,318%.

Monero, like Zcash also offers totally private transactions using the blockchain and has been heralded as the drug dealers' coin of choice. It uses 'ring signatures' to hide the identities of the sender and recipient of a transaction. This is a type of digital signature which can be signed by any member of a group of Monero users, the aim being that it is impossible to determine which of the group of users signed for the transaction.

In a downturn for the reputation of privacy coins, in 2017 Monero was linked to the WannaCry Ransomware attack, whose victims included the NHS. The attack targeted 200,000 computers across the world by encrypting data and demanding ransom payments in Bitcoin. Researchers have since linked Bitcoin wallets to the attackers and found that these wallets were emptied and the coins transferred to Monero. Because of Monero's privacy features, this money can no longer be traced.

Is the Bitcoin heyday over?

Despite the plethora of alternative coins that offer more privacy, the big names in the crypto world still rule. Bitcoin currently has a market cap of around $170bn compared to Dash (around $5bn) and Zcash (around $1bn). If Bitcoin manages to implement some more privacy features such as Confidential Transactions it could manage to stave off competition from the privacy coins.

As more privacy coins make their way into the crypto-sphere and the established coins ramp up the privacy features to compete, it is inevitable that law enforcement agencies will have to step up the game in order to prevent fraudsters from using these currencies to hide and launder their money.

Regulators will also have to strike a balance between allowing this lucrative market to thrive and preventing the crypto-sphere from becoming a dark ether where illicit funds go in and can never be traced. But for now, the heyday is certainly not over.

Authors

Elisa Wahnon

ASSOCIATE | LONDON

Litigation & Arbitration

☎ +44 20 7597 6328

✉ elisa.wahnon@withersworldwide.com