lab10 - Research #17

Research Zcash

17.10.2016 13:27 - didi

Status:	In Progress	
Priority:	Normal	
Assignee:		

Description

Zcash is a clone of the bitcoin software, with added privacy.
It uses zero-knowledge proofs to allow hiding of sender, receiver and amount of transactions.
A much criticized side effect is that the overall coin supply at a given moment can not be checked by anybody.
Another implication was the creation of *toxic waste* which needed to be destroyed in a so called ceremony right before the start of the main chain. See report of a participant.

The project is quite experimental, because the used crypto is fairly new.
Obfuscation of transaction is optional, unlike with Monero where it's always on.
According to (TODO: insert source) the creation of obfuscated transaction currently requires a lot of computing power (several GB of RAM), rendering it unsuited for mainstream use for now.

The mainnet started on Oct 28 with mining reward linearly transitioing from 0 to 12,5 ZEC block reward during the first 840.000 blocks (~34 days) source.

The mining algo is named Equihash and intended to be ASIC resistant.
Pool: https://zec.suprnova.cc/

CT for mining set up at zcash.d10r.net

History

#1 - 22.12.2016 20:33 - didi

- Tracker changed from Feature to Research

- Project changed from Lab to lab10

- Subject changed from Research zcash to Research Zcash

- Description updated

- Status changed from New to In Progress

So, it had a rocket start (at one point 1 ZEC was about 1M USD), then stabilized somewhere around 50 USD.
Miner efficiency was increased several times in the days around the start.

There was also already a fork: Zclassic considers the initial 20% mining fee unfair and thus set up a chain with that fee removed. Seems to not have reached much traction. Not listed on Poloniex (ZCL).

#2 - 29.03.2017 23:43 - didi

The backup process is quite confusing: https://forum.z.cash/t/wallet-dat-private-key-z-t-addresses-what-to-backup/4506/11

The mining pools I know support only t-addresses.

My addresses:
zcash
zclassic