## Zcash挖矿过程高度中心化？有专家称其为“企业币”

原创 2016-11-01 Joseph

过去的几个月以来，越来越多的加密货币爱好者和投资者都开始强调Zcash的重要性，说明了其隐私性和匿名性对数字货币生态系统的潜在影响。不过，社区中仍有相当多的专家和用户对Zcash的炒作狂潮并不买账。

**优势**

包括比特币风投企业潘泰拉资本（Pantera Capital）首席执行官丹.莫尔黑德（Dan Morehead）在内的大量投资者和专家都对Zcash抱有极大期望，称其能弥补比特币的不足。Morehead列出了Zcash的几个优点：

有选择性的透明度

GPU挖矿有效防止中心化

更高效的管理

由于投资者对Zcash十分看好，Zcash一经发布，市值就达到了4000亿美元。据CNBC高管布莱恩•凯利（Brian Kelly）所说，Zcash市值一度超越了Facebook。

虽然Zcash的价格一路飙升，但其中心化的操作模式仍引来了不少的批评。

**缺陷和批评**

Zcash这一“去中心化的”、“私有”加密货币的主要缺陷在于其基金会和开发团队的中心化。Zcash的运维由一家美国公司全权负责。

针对Zcash这种由开发者和网络运营商主导的中心化特质，加密货币社区部分开发者和爱好者为它取了个别称——“企业币”（corporate coin），因为执法机关或政府机构能够轻易对Zcash进行操控，并且可以滥用职权，影响其开发过程。

天使投资人彼得•布莱克（Peter Black）同时也是一名比特币专家。他指责了Zcash的中心化控制。作为一种加密货币，Zcash违背了数字货币的基本概念，其运维并不是在分布式环境中进行的。

Zcash（ZEC）是一种企业币。数字货币不应该由任何单一的团体、企业或央行进行管控。

Black和其他加密货币专家对Zcash的中心化担忧是合乎情理的，因为这会给挖矿过程带来不良影响。

对于数字货币来说，挖矿机制和通胀率是两大重要技术难点，通常，开发者会花费大量的时间研究这两点。Zcash则十分特殊，整个挖矿过程基于创始密钥（Genesis keys）或“主私钥”（master private key），而这个密钥是由6个人共同持有的。

简单来说，这种主私钥是Zcash创始人兼首席执行官Zooko Wilcox口中的“有毒废料”，但事实上却是Zcash网络匿名混合功能正常运作的关键。密钥一旦外泄，不怀好意的持有者就能够创造无数个Zcash。而这种高强度的生成方式很可能导致网络崩溃。

问题在于，这6个有权获取主密钥的人都来自同一家企业。假设该企业经营不善，或者密钥被盗用，整个Zcash网络很容易遭到交易攻击。

多个加密货币社区，特别是门罗币社区，强烈谴责了Zcash这种中心化的挖矿和部署过程，因为这种方式违背了密码朋克（cypherpunk）和分布式数字现金的基本原则。

随着Zcash挖矿进程的展开，越来越多的问题接踵而至。比如说，**上文提到的6个人可以获得挖矿利润的10%，作为他们的运作经费**。部分支持者将这种机制与ICO相比较，但和预挖矿以及比特币和门罗币等其他匿名货币的部署过程相比，这种机制仍然在很大程度上代表了系统的高度中心化。