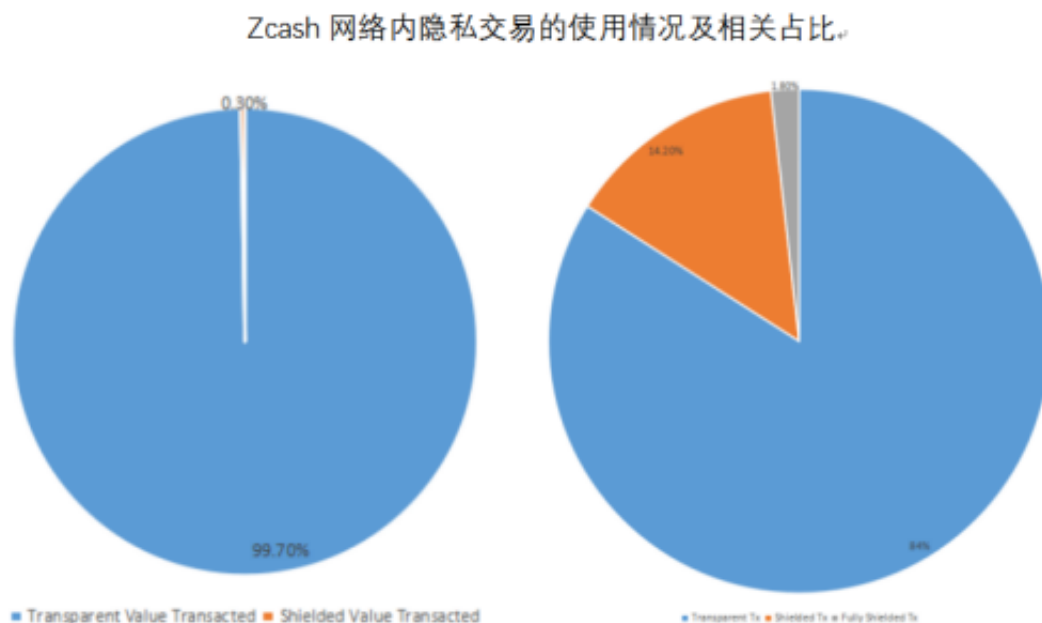


未正式开挖，期货价格已在BitMEX上炒到1400美元左右；创始块刚诞生，价格随即哄抬至200万美元/枚——2016年推出的Zcash，无疑是当时的币圈黑马。其上线不到半年便被暗网第一黑市AlphaBay接受，相关匿名技术还相继获得以太坊、波场、摩根大通旗下企业级区块链Quorum、以色列技术开发商Starkware等等项目以及公司的青睐。



左图为近一月内通过透明交易与隐私交易的Zcash在网络内的占比情况；右图为近一个月网络内透明交易与隐私交易的占比情况（数据源自：explorer.zcha.in）

还未找到自身定位的Zcash

与Zcash以及达世币不同，三大匿名币种中门罗币所有的交易都是匿名进行的，再加上其抗ASIC的决心，使得门罗币能够快速且大范围地打入暗网市场，同时获得新晋暗网币王的称号（详情可查看哈希派之前发布的《价格低迷的门罗币，凭什么挤掉BTC成为「暗网币王」》）。而匿名性相对较弱的达世币，则凭借着其即时交易属性以及市场化策略，逐渐在拉美地区流行起来；至于同样具有隐私交易选择弹性的Zcash，当前在市场的定位以及具体适用场景却依旧模糊。

从项目以及部分大公司的态度可知，Zcash匿名技术zk-SNARKs的市场关注度高于门罗币采用的环形签名技术；但是依照暗网以及隐私交易的使用情况来看，前者的匿名特性并没有得到充分发挥。如上文所说，月内Zcash用户选择使用隐私技术的交易低于20%（其中完全匿名交易占比不足2%），而且网络中95%左右的ZEC均存

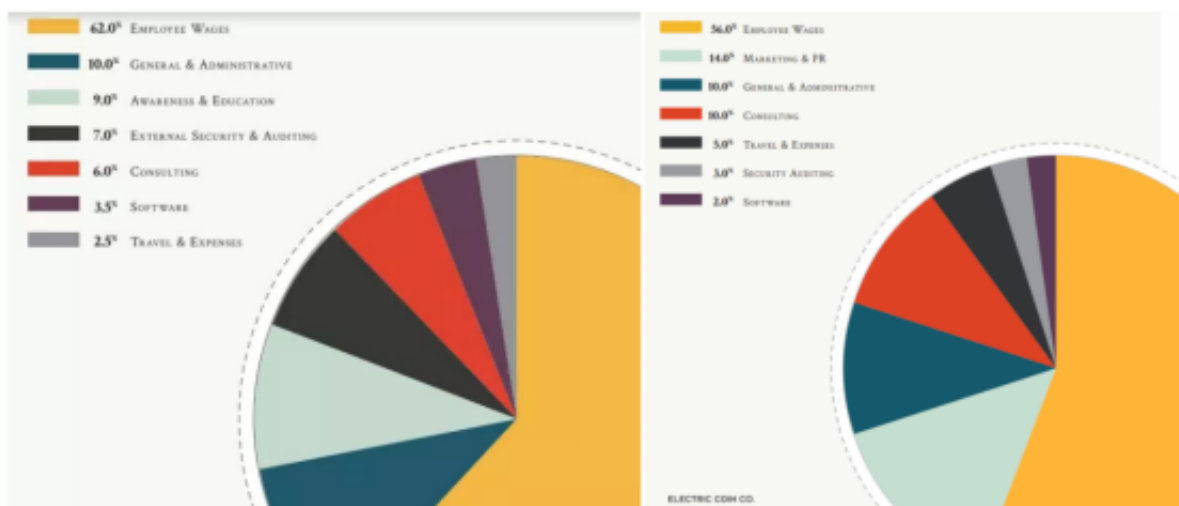
储在没有屏蔽保护的公开地址内。此外值得关注的是，当前接受Zcash的暗网市场不及7%，低于占比16%的达世币，而与末位的VTC相比，仅多出一家支持其支付的暗网市场（数据源自：The Block本月发布的分析数据）。

	门罗币	达世币	Zcash
上线交易所数量	54	117	93

数据源自：Coinmarketcap

事实上，前期Zcash的隐私交易未能广泛应用还与其生成成本有关。在Sprout以及Overwinter阶段，为了生成可让矿工使用的零知识技术证明，每创建一笔完全私密交易时发送方都必须经历一系列精确的计算，耗时数十秒，交易占用内存高达3 GB；迫使当时大部分用户干脆放弃使用隐私技术直接进行透明交易。直至去年十月Sapling升级优化过后，其发起匿名交易的用时才缩短至一秒之内同时所需内存也下降至40 MB左右，让移动端交易成为可能；而下一阶段Blossom升级并添加链下轻量级交易技术BOLT过后，其隐私交易技术还将进一步加快。

	门罗币	达世币	Zcash
支持其支付的相关商家	142	4900+ (其中近半数位于委内瑞拉)	173



左图为，2018年下半年ECC公司的支出类别；右图为，2019年第一季度ECC公司的支出类别（图片源自：ECC公司发布的Zcash透明度报告）

根据报告显示，2018上半年ECC就已出现入不敷出的问题，而下半年则显现出赤字进一步扩大的迹象。按照该时间段每枚ZEC均价60美元来计算，ECC去年下半年的总收入为220.5万美元；减去每月70万美元的总支出以及95万美元的额外推广经费，其2018下半年将近亏空300万美元。而且Zcash这种亏损状态还延续至今，在ECC对其支出份额进行调整后，该公司2019年Q1依旧出现了55.8万美元的亏损。

A Personal Letter About The Possibility of a New Zcash Dev Fund



Zooko Wilcox [Follow](#)
Aug 1 - 13 min read

Note: This letter was written as a response to the intense conversation that was initiated and is being driven by members of the Zcash community, starting with mineZcash, Gareth Davies, Aristarchus, et al and joined by an increasing number of other community members. If you're not following the Zcash community very closely then this might be the first you've heard of it, but they've been working on it for months. They are the ones who are serving the Zcash mission by driving this discussion.

※八月初，ECC首席执行官Zooko Wilcox发布公开信谈论“创始人奖励”计划，希望以另一种方式将其延长下去，从而解决后续的资金问题（图片截自：Medium）

谋事在人，Zcash团队可否渡过难关现在还难说，但是留给他们的时间真的不多了。距离上次Zooko发布公开信表示将“很快”公布一项社区程序已经过去两个多月，我们依旧没有看到任何进展；如果解决问题只停留在口头上，Zcash的后续发展不容乐观。