什么是小硬币zcoin(xzc)

为什么会建立这个货币？

zcoin(xzc)是一种加密货币，使用zerocoin协议保证账户的私密性。

。它是首个实现零币协议的加密货币，通过零知识证明确保交易双方的相关地址信息不被泄露。

这个货币可以做什么？

私有地址为了进一步增强Zcoin网络的匿名性，

，允许Zcoin用户公开自己的地址，但无法找到任何与该地址相关的历史交易信息。这意味着Zcoin的一个公共私有地址可以公开，但这不会影响地址的匿名性。。通过零知识证明机制，可以完全分离铸币和兑币之间的关系。当你施放一枚Zcoin的时候，你也销毁了一枚Zcoin，会生成一个证书证明你烧毁了一枚Zcoin。。这张证书只证明你烧了一枚Zcoin，但你没有&#039；不需要证明你烧了一个特定的。然后用这个凭证就可以兑换一枚全新的有完整交易历史的硬币。同样，与其他匿名方法相比，也没有用于分析的交易图表。

这样隐私匿名性提高了好几倍。

因为哪些技术、或是机制，导致他可以做这个？

零知识证明创造投资人奖励MTPPOW算法提高公平性计算：MTP算法最大的好处是可以快速高效低能耗验证匿名方案，MTP也使得智能手机这样的轻量级硬件设备进行挖掘认证成为可能。这可以&#039；其他算法做不到。在钱包终端中实现TOR和I2P功能：Zcoin钱包终端通过使用TOR和I2P网络，并在连接到Zcoin网络时隐藏真实的IP地址，进一步增强了Zcoin的匿名性和私密性。

为何很多人选择零币而不是用ZCASH进行交易？

Zcash打算在Zerocoin上进一步优化，但是有一些不足。最大的缺点之一是优化后需要复杂的信任设置。

这一点一直存在争议，因为交易金额也隐藏在Zcash中。如果有人找到漏洞，大量挖掘Zcash，就很难被察觉，这也会让洗钱变得更容易。对于Zcoin来说，如果有人找到漏洞，挖掘出大量硬币进行流通。因为Zcoin的货币供应总量是可以查询的，

所以大家都可以很容易的检测出来。

从可用性上来说，即使Zcash的证明块很小，也需要强大的计算机来计算。Zcoin完成同样的工作只需要几秒钟，这使得Zcoin在移动设备这样的低计算量设备上进行挖掘有了进一步的优势。Zcash目前只能在Linux系统上使用。而Zcoin已经可以在Windows、Mac、Linux等多个平台上运行，这也是Zcoin受欢迎的原因之一。