

1. 什么是Zcash(ZEC)？

zcash的想法最早是由约翰霍普金斯大学的马修格林(MatthewGreen)和伊莱本萨松(EliBen-Sasson)教授在2013年提出的。。ZeroCoin更多的是修改比特币的隐私，但它并没有'推出后没多久，因为它需要改变比特币的主体。相反，2016年，ZookoWilcox基于ZeroCoin创造了一种新的隐私加密货币Zcash。这种货币在推出时也在加密货币社区引起了轰动。当时每个Zcash的价格被炒作到比特币价格的6倍，之后逐渐稳定。

站长推荐

全球第二家加密货币交易所，注册即可获得最高3000的数字盲盒，该节点注册费永久10%。

willcocks

和Zcash类似的，还有门罗币Monero，我们之前介绍过。。它们使用不同的机制来隐藏用户需要加密的交易信息，但都使用零知识证明来实现保密机制。目前，他们也有自己的支持者。什么' # 039 ; 加密货币的意义何在？Zcash'美国著名的支持者包括爱德华斯诺登。门罗币是莱特币的发明者，查理李。门罗币目前的市值是37亿美元，而Zcash是13亿美元。

什么是零知识证明？

零知识证明是指被验证方不需要透露任何关于验证的信息。可以知道被验证方的信息是正确的。目前，零知识证明被广泛应用于区块链技术中。下面的例子最常用来说明零知识证明：

chanalysis扩展了对隐私币Zcash和Dash的支持。

Dash和Zcash是两种最著名的隐私币。他们的日营业额接近15亿美元。Chainalysis声称，它可以通过分析交易来标记地址和现实世界的实体。。Dash和Zcash使用户能够在非常私密的情况下进行交易。

有两个球，蓝色和绿色。验证者需要证明他能够区分两个球的颜色。因为信息是隐

藏的，验证者可以' ; I don' 我用色盲眼镜分辨不出这两个球的颜色。。这时候验证者需要先把球藏起来，然后单独拿出来让验证者回答球的颜色有没有变化。因为验证者知道自己是否取出了不同的球，就可以证明验证的答案是否正确。只要增加取出球的次数，验证的答案就是正确的。你可以确认他真的能分辨出球的颜色。

2. zcash(zec)是如何工作的？

Zcash' ; 在挖掘会计和生成交易方面的机制类似于比特币。区别在于Zcash上有两种类型的账户。，即公共账户或私人账户。公共账户和私人账户可以相互交易，但私人账户的收付金额和地址不会在区块链中公开。然而，这将导致一个问题那' ; sZcash的其他用户如何知道私人账户中的交易不是伪造的，zcash被超额支付？因为比特币的所有交易记录都是透明的，其他用户可以利用空白空间确认没有人可以生产伪造的代币。。Zcash使用ZK-斯纳克(非交互式零知识证明——)来允许矿工在验证账户时确认用户没有伪造空令牌。

由于私人账户交易的详细信息是隐藏的，收款人如何确认收到的令牌确实来自指定的付款人？每个私人账户都有一个"查看密钥"。私人账户持有人可以与收款人共享查看密钥，收款人可以使用查看密钥查看具体的交易明细。以确认代币确实来自付款人。

3. 为什么Zcash(ZEC)有价值？

ZEC的总供货限额为2100万件。目前市场上流通的有1200万件，约占总供应量的58%。。剩下的代币会随着矿业刺激慢慢投放市场。

ZEC最大的价值来自于它提供的交易隐私，它的技术也广泛应用于以太坊的很多去中心化应用中。摩根大通等许多大型机构也在内部引入了类似的隐私机制。此外与比特币相比，ZEC' ; 的交易处理速度更快。目前比特币屏蔽需要10秒左右，而ZEC屏蔽只需要2.5秒左右。ZEC在推出之初就引起了轰动，但在2021年它也是一种私人硬币，它有许多对手，如门罗硬币。。而且2021年的令牌战场已经从单一功能的令牌转移到公链或者DeFi，NFTs。ZEC更有可能只是早期私币的历史价值和一些功能价值。

郑重声明：本文版权归原作者所有。。转载文章只是为了传播更多信息。如果作者' ; 的信息标记有误，请尽快联系我们修改或删除。谢谢你。

以太坊V对分布式隐私货币的未来充满期待

随着世界各国政府越来越希望推出自己的数字货币，你可能会担心加密货币无法与传统庞大的金融体系有效竞争。以太坊的联合创始人维塔利克布特林说，这种情况