## 号称终极匿名的数字货币ZCash强势发布，它究竟有什么好处？

2016-11-01 [区块宝](https://mp.weixin.qq.com/javascript:void(0);)

日前，基于区块链技术的替代数字货币ZCash正式发布，开发者宣称，ZCash利用加密隐藏用户的身份，是第一种真正匿名的数字货币。据悉，ZCash发布之初便异常火爆，火爆到了甚至还没开始挖矿，网上的期货价格最高达能到1.9BTC。

而同为数字货币，ZCash在很多方面都和比特币有相似之处，首先它也是基于分布式账本（区块链）之上进行交易。但ZCash有一点和比特币有着很大的区别：ZCash是完全匿名的。

据介绍，ZCash利用了名叫零知识证明（被称为“zk-SNARK”）的技术验证交易的真实性，利用一个公共区块链来展示交易，但会隐藏掉交易的金额，而查看密钥的所有者（即币的拥有者），可允许他人查看这个密钥相关联的信息。

简单来说，这种计算方式可以让用户证明他们拥有了他们想要的币，而不用暴露关于币来自哪里或要去哪里的信息。就好像，零知识证明允许你在网站上输入密码，并由网站的服务器进行验证，而不会真正传输密码。

相比较之下，尽管比特币等数字货币以交易的隐蔽性著称，但在现实生活中却常常可以通过普通的比特币区块链的记录追踪交易，人们可以准确获知比特币的发送者和发送地点。如今，ZCash实现了通过加密的形式交易原数据，而不是像比特币那样要将交易数据公布于众。斯诺登日前参与讨论时也表示，匿名Zcash项目可解决比特币的监视风险。



所以，ZCash这样一个对隐私保护极致追求的匿名功能，其首先被认为在金融业有巨大的价值。外媒指出，传统金融业对信息保护有着非一般的需求，尽管很多人认为比特币和其他区块链系统的隐私性要求来自于加密无政府主义者和自由主义者，事实却是，传统金融业在推动将交易信息隐藏于区块链上。

Zcash的CEO和资深加密技术爱好者Zooko Wilcox-O’Hearn称，与他交谈过的传统金融机构从业者都表示需要增加区块链的隐私性。因为人们还不清楚，该技术的颠覆性会给金融业带来什么，因此必要的隐私保护是区块链技术应用于金融业的关键。所以，Zooko认为，无论从监管还是企业角度看，都需要实现区块链的加密读取。这是ZCash的价值所在。

而当然，ZCash的诞生也引来一些反对的声音，有人认为，市场有了深黑的比特币也足够满足当前加密的需求，并不需要ZCash这样一种纯黑的模式。加强金融的隐私性可能也会助长罪犯的业务，因为这些业务由于隐私我们无法看到。