Zcash要如何平衡区块链的隐私与透明性？

原创 2016-11-01 Lalita 巴比特资讯

Zcash这个上周才刚刚推出的加密货币，承诺了一种新的公有链交易隐私。这可能会使分布式账本技术对金融机构更具吸引力，但监管机构可能就不太那么高兴了。

Coin Center研究主管Peter Van Valkenburgh说：

“在使用公有区块链的情况下，如果你是摩根大通，那么你就可以看到所有的瑞士信贷银行的账簿，所以无论是摩根大通还是瑞士信贷都不适应这种程度的透明度。”

通过Zcash，软件开发者兼Zcash创始人祖科•威尔科克斯（Zooko Wilcox）为这个问题提供了一种解决方案。如果这种技术按照构想运行，那么不仅能够使区块链更加适合银行，而且还能帮助解决银行与反洗钱法规之间长期存在的紧张局势。剩下的就要看政府如何看待这种交易能够审计而披露由参与者控制的系统。

从与比特币一样的基本框架开始，Wilcox为区块链添加了一种新近的加密创新——零知识证明（zero-knowledge proof）。

这个Zcash系统允许用户进行私人交易，同时还能维护支持交易的区块链的完整性。对于比特币，用户通过匿名的交易地址来进行识别。那些字母数字字符串本身并不能保证隐私，因为资金的流动是可以通过区块链和相同用户掌控的地址进行跟踪的，因此这些用户是可以被联系的。

对于Zcash，它具有两种类型的地址，‘透明的’和‘屏蔽的’。对于透明的地址，来回发送的金额可以像比特币那样出现在区块链上。但是如果用户选择使用一种屏蔽的地址，交易将被掩盖在公共账本上。如果资金的发送者和接收者都选择使用屏蔽的地址，那么发送的数量也将被加密。

Zcash创始人祖科•威尔科克斯（Zooko Wilcox）

最后，Zcash开发团队将会添加‘查看密钥‘，用户可以分享给第三方来透露自己的交易信息——而其他人则看不到。

Wilcox表示：

“我们将此称之为‘选择性披露’，它还附带了一个加密的备忘录字段，允许机构将敏感的信息附加在交易中，而那些获得授权的机构能够看到这些信息。”

Van Valkenburgh说，零知识证明的潜力在于‘让你能够证明有关数据结构的一些东西，同时还不会暴露数据结构内部的数据’。

Wilcox在《美国银行家》的区块链+数字货币会议上表示：

“在通过加密，你实际上可以同时获得很多或者大多数的透明度，隐私和数据安全性的属性。你可以以这种方式向区块链中添加加密数据，并且只有授权方才能够对这些数据进行解密，而不是所有人。”

但它保留了区块链的重要属性。

他还说：

“Zcash与其他区块链一样，你向不同的人提供的交易信息不可能不一样，并且你也不能改变你的信息。”

在暂停零知识证明方面的工作以确保Zcash能够按时且安全地发布之后，该公司目前趋向于同时进行两个项目的研究。

Wilcox在周一发布的邮件中表示：

“我们的代码正在接受互联网领域的检测。”

一个明显的问题就是：Zcash货币（ZEC)的隐私特点会不会使金融机构更加难以参与进来——例如数字货币交易所和钱包服务或者其他银行业务提供商——以遵循反洗钱法规定。

一方面，Zcash的’选择性披露‘能力，结合对中介机构遵守反洗钱规则的压力，将会确保大多数交易都是可跟踪的。

收集基础的交易数据以符合AML目的的工作将可能由第三方机构来执行，如钱包和交易所。

为遵守货币服务业务规则，或者由于需要满足银行合作伙伴的需要，这些公司（钱包或交易所）将不得不获取交易参与者的相关数据和其他信息，以此确保他们可以标记可疑交易。

Arnold & Porter法律公司的一位副研究员Pratin Vallabhaneni说：

“所有的相同的合规基础设施仍然需要到位。如果你是一个Zcash用户并认为‘哦，我可以进行更加匿名的交易。那么这样想是不正确的，因为如果你不披露基本的身份信息，你将无法进入[金融]生态系统的其余部分。”