## Vitalik：ETH将整合Zcash隐私功能

原创 2016-11-01 Andrew [巴比特资讯](https://mp.weixin.qq.com/javascript:void(0);)

以太坊（分叉）创始人Vitalik Buterin近日表示，ETH智能合约即将添加绝对的隐私功能。

零知识证明（zero knowledge proofs）纳入ETH发展计划已经有两个月的时间了。

在接受CCN采访时，Buterin说，ETH要完全实现类似Zcash（Zec）的隐私性还需要至少4个月到1年的时间。

一个拥有绝对隐私性的ETH能够解决区块链长期存在的棘手问题：如何在世界范围内进行隐私交易，并且同时能够与指定的对象共享交易信息。Zcash创始人Zooko Wilcox在参加devcon2时，发表了题为“Zcash+ETH=爱”的演讲。他表示，在过去的4年时间里，研究者发现，一笔交易在完全隐私的操作模式下也可以实现选择性的信息共享。

然而，Zooko说，这一发现与中本聪的理念存在冲突，因此他一直无法对其进行合理利用。而如今，随着Zcash研究者在数学方法上的改进，他们逐渐完善了这一过程：矿工可以在不知晓交易信息的前提下，根据预先设定的网络规则验证交易；同时，某些特定的对象，比如说公司员工、监管者、客户也能在不透露任何细节的情况下进行交易验证。

因此，Zcash带来的不是简单的匿名性，而是解决重要问题的机制。也就是说，Zcash可以确保我们在享受公有链公开透明的优势的同时，确保数据的真实性，我们可以进行选择性的信息共享。

Zcash与智能合约的结合可以使这项技术变得更加强大，对当前的架构进行渐进式的改进，从而达到提高系统生产能力和效率的目的。

Buterin也有同感：

区块链技术和隐私性的结合是新一代应用安全发展的重要因素。

**延展性和实用性考虑**

整合Zcash的隐私度还需要考虑到ETH区块链的延展性和实用性问题。零知识证明是一种复杂的数学方法，这种方法在解决大量问题的同时需要占用极大的内存。因此有人建议整合过程仅需涉及合约或项目，而ETH协议应排除在外。

提到延展性问题，Buterin说道：

零知识证明（ZKP）交易的处理时间的确比普通交易要长。所以说每秒15笔ZKP交易是不太可能的（将来我们的虚拟机经过改进说不定可以解决这一问题，但是目前还很难说）。

至于是要整合到合约层还是协议层，Buterin表示“我们还需要几次预编译进行优化”。

ETH的sharding解决方案对解决延展性问题大有帮助。它能通过指定节点和交易对应的方式创建一个复杂的网络，该网络运作效率极高，其交易验证能力相当于全节点。

ETH智能合约整合Zec代码框架的工作早已开始。另外，Zooko还表示Zec和ETH开发者之间会进行人才共享，建立紧密的合作关系。这个世界即将见证两位智者的合作——Zooko Wilcox和Vitalik Buterin，为我们带来精彩的脑力冲击。