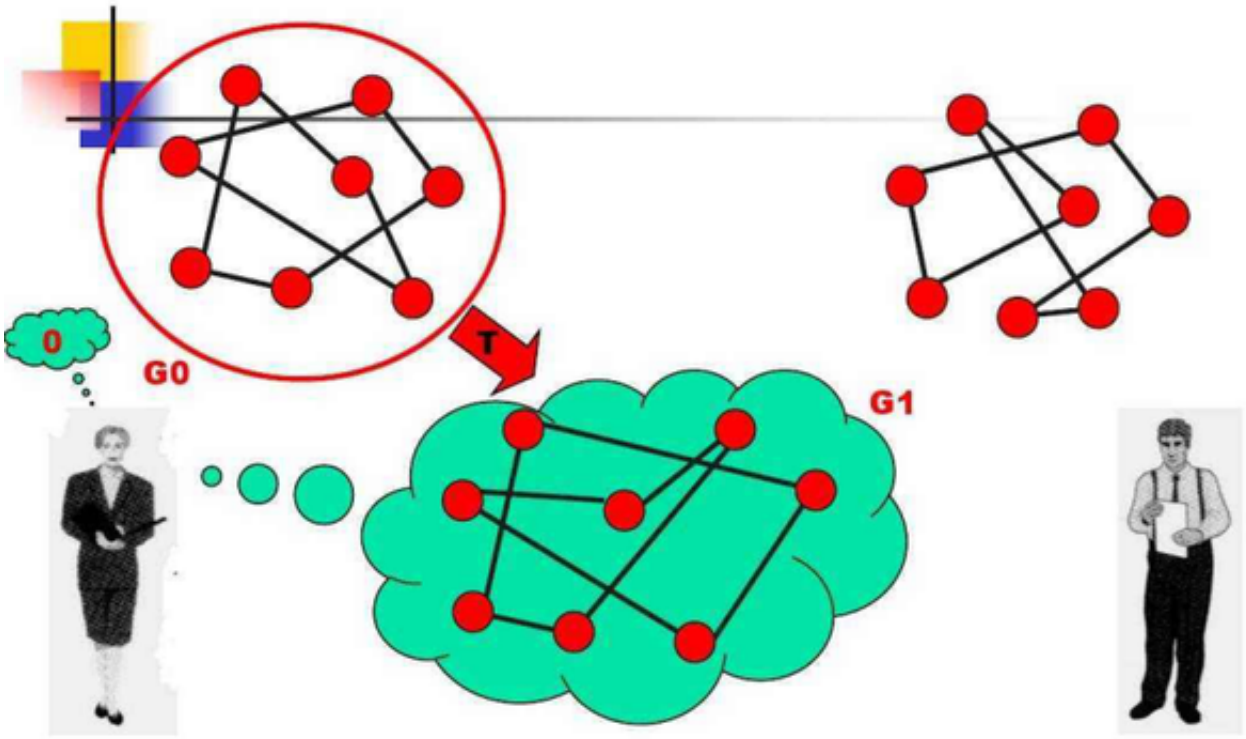
区块链的零知识证明最近再次引起了人们的兴奋，因为它们可能会增加区块链应用程序的隐私和安全性。这个概念本身并不新鲜，因为密码学家多年来一直致力于零知识证明。但这项技术刚刚开始重新定义在线隐私的概念。



要运行ZKP，必须满足以下参数：

完整性：如果陈述为真，则诚实的验证者可以被诚实的证明者说服。可靠性：如果证明者不诚实，他们可以&#039；don’不要通过撒谎来说服验证者这个陈述是可靠的。。

零知识：如果语句为真，那么验证者无法知道该语句是什么。

举一个零知识证明的例子。让&#039；让我们来看看阿里巴巴洞穴是如何运作的。在这个例子中，证明者(P)对验证者(V)说他知道洞穴后面暗门的密码，并提出在不向验证者透露密码的情况下证明它。然后，验证过程如下图所示：

-图片提供：Scotttwombly(YouTube频道)-

证明者可以走路径A或路径B，假设他们最初决定走路径A到达暗门。同时督v来到

入口，他没有&#039；t不知道证明者选择了哪条路径，并声明他们希望看到证明者出现在路径b中。

如图所示，证明者确实出现在路径b上。但如果这只是巧合呢？也有可能证明者在出发时侥幸选择了路径B，但却被困在了门口，因为他没有&#039；我不知道密码。

所以，我们需要做很多实验来确定测试的有效性。如果证明者每次都能出现在正确的道路上。那么证明者就可以真正证明他知道密码，而不用向验证者透露。零知识证明在

区块链是如何应用的？

许多基于区块链的技术正在使用Zk-Snarks。实际上在大都会阶段，以太坊计划引入Zk-Snarks，并将其加入以太坊的函数库。Zk-Snarks是&quot零知识简明非交互式知识认证&quot，这是一个在不暴露数据本身的情况下证明一些数据操作的零知识证明。

以上内容可以用来生成一个证明，其有效性可以通过创建每笔交易的简单快照来验证。这足以向信息接收方证明交易的有效性，而不暴露交易的实质。

这实现了以下两种情况：实现了交易的完整性和私密性。实现了系统的抽象。由于不需要显示整个交易的内部工作模式，该系统非常易于使用。因此，以上是区块链使用的一些重要的加密函数。现在让&#039；让我们看看它的第二个支柱，经济学。其他基于区块链的系统已经将零知识证明整合到他们的解决方案中，以在验证交易的同时保护用户/交易隐私。让消费者重新掌控自己的数据。