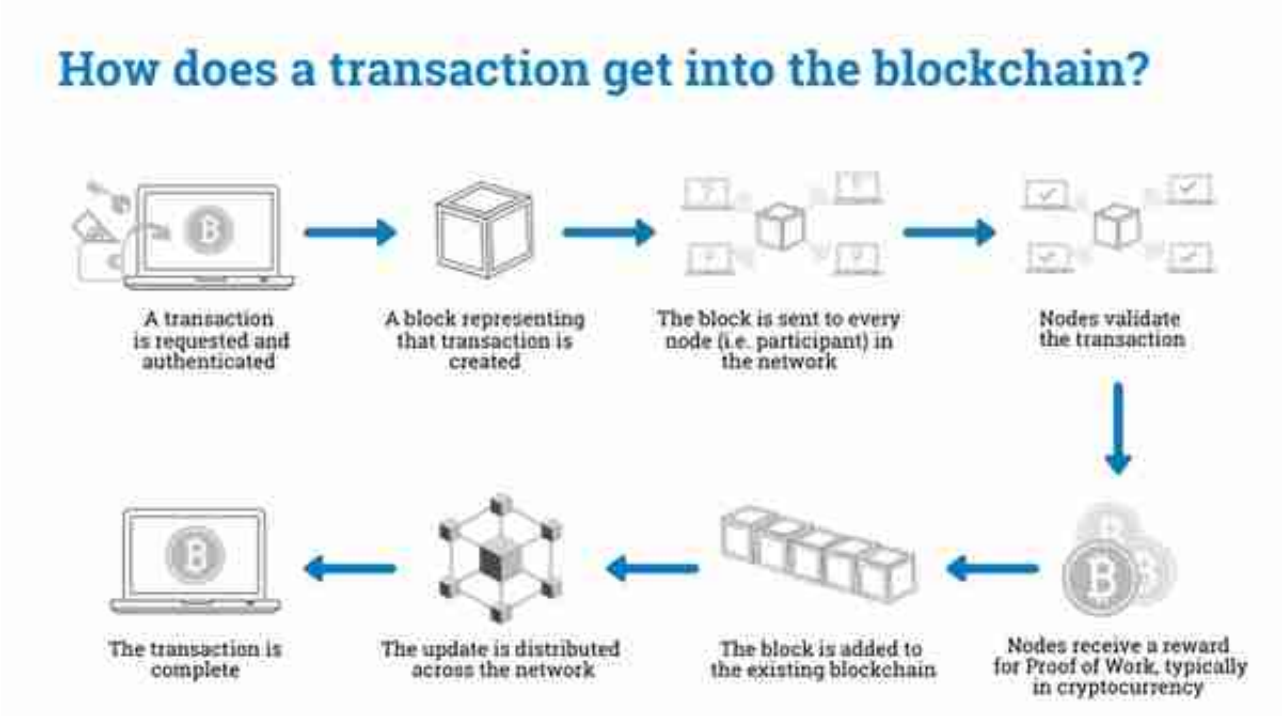
在将交易添加到区块链之前，必须经过几个关键步骤。今天，毛球科技将带大家了解使用加密密钥进行身份验证、通过工作证明进行授权、挖掘的作用，以及在后来的区块链网络中最近采用的权益证明协议。



1.验证

最初的区块链旨在在没有中央权威的情况下运行（即没有银行或监管机构控制谁进行交易），但交易仍然必须经过身份验证。

这是使用加密密钥完成的，这是一串数据（如密码），用于识别用户并允许访问他们在系统上的“帐户”或“钱包”。

每个用户都有自己的私钥和每个人都可以看到的公钥。使用它们都可以创建一个安全的数字身份，以通过数字签名对用户进行身份验证并“解锁”他们想要执行的交易。

2.授权

一旦交易在用户之间达成一致，就需要获得批准或授权，然后才能将其添加到链中的区块中。

对于公共区块链，将交易添加到链中的决定是通过共识做出的。这意味着大多数“节点”（或网络中的计算机）必须同意交易有效。网络中拥有计算机的人被激励通过奖励来验证交易。这个过程被称为“工作量证明”。

3.工作证明

工作量证明要求拥有网络中计算机的人解决一个复杂的数学问题，以便能够向链中添加一个区块。解决这个的问题被称为算力节点，“算力节点”通常会因其在加密货币方面的工作而获得奖励。

但这个计算过程并不容易。数学问题只能通过反复试验来解决，解决问题的几率约为5.9万亿分之一。它需要使用大量计算能力。这意味着进行计算的回报必须超过计算机的成本和运行它们的电力成本，因为仅一台计算机就需要数年时间才能找到数学问题的解决方案。

4.工作量证明的问题

为了创造规模经济，算力节点通常通过聚集一些节点将他们的资源集中在一起。然后这些节点分享区块链网络提供的奖励和费用。

随着区块链的发展，越来越多的计算机加入来尝试解决问题，问题变得越来越难，网络也越来越大，理论上可以进一步分配链，并使破坏或黑客攻击变得更加困难。但在实践中，计算权已集中在少数矿池手中。这些大型组织现在拥有维护和发展基于工作量证明验证的区块链网络所需的巨大计算能力和电力。

5.股权证明

后来的区块链网络采用了“权益证明”验证共识协议，参与者必须在区块链中拥有权益——通常是通过拥有一些加密货币——才有机会选择、验证和验证交易。这节省了大量的计算能力资源。

此外，区块链技术已经发展到包括“智能合约”，它在满足某些条件时自动执行交易。