挖矿比特币的过程类似于抽奖。比特币矿工竞相生成哈希值——固定长度的字母数字字符串，根据任意长度的数据计算得出。。他们通过组合以下三个数据生成一个hash:一个新的比特币交易块；区块链的最后一个街区；和一个随机数。在本文中，我们将分析哈希和数字签名过程，以了解它们在单独用于比特币交易验证之前的用途。

深入研究一些简化的技术细节。签署任何数字签名的第一步是对签署的内容进行哈希运算。安全散列并不容易，但256位安全散列算法(SHA-256)可以保证两个关键内容。

首先，对散列算法的强力攻击必须与所有256位的二进制组合一样计算量大。但是，目前指望攻击者完成对小额比特币交易的搜索是不现实的，比如因为有256个二进制位的2256个组合(2*2*2*.256次)。这是一个大数字。第二，对散列算法的另一种强力攻击必须与处理256位的所有二进制组合的大部分一样计算昂贵。其中很大一部分是一个复杂的、可证明的公式，它与理论输入大小有关(对于SHA-256，它是不受限制的。

，万维网上常用的限制除外)，而256位无疑会需要并支持这一点。

碰撞？那是什么？

9个输入必须碰撞成具有8个孔的3位散列。为了简单和清楚起见

这个简化的示例生成一个3位哈希，而不是256位哈希。三个二进制位(每个为0或1)有2*2*2=8种组合。然而，如果有一个9项散列，则有两个输入至少会导致相同的3位散列输出。通过一般逻辑，您可以立即看到一些输入，因此您必须散列到相同的输出。

在对hash有了更好的理解之后，让&#039；让我们回到它的用法：法律合同是一个目的，但以太坊中的比特币矿工和伪造者也严重依赖hash谋生。。加密货币投资者也通过传递性(传递性，简化为：A=B，且B=C，因此A=C)以某种方式使用它们。

篡改数字签署的合法合同是如此明显，却从未发生过。。即使改变了一个字符，SHA-256也会产生一个完全不同的散列，比如

。

&quot；比特币区块链&quotis:b43636e6232a977b6a614c93da701f938f9FAA90d355a74d71aa8210474c8BF

。

&quot；比特币区块链&quotis7c96cf30947914aB1d9844d93707BAF2435f9F9b290c8258622ab635054c8041

。

It&#039；这只是一个字符的差异-
大写字母&quotb&quot和哈希是完全不同的位集。

工作量证明与权益证明

工作负载证明(PoW)方法，用于在类似比特币的区块链型网络中网络计算资源的网络分配。

，在相反的方向大量使用散列。如前所述，暴力方法是计算密集型的。所以一个全面的黑客攻击是有一些子问题的，可能难度比较大。通过增加问题的难度(但只是略微增加)，比特币运行在工作负载证明模型上，其中矿工们通过解决这些超级问题证明了他们花费了大量的资源和努力来运行网络(首先，他们自称&quot先行者&quot).奖励&quot).然而，这种模式的能源效率极低，而且不是针对比特币和区块链技术的。

权益证明(PoS)的能效要低得多，因为&quot矿工&quot(在衡平法的网络证明中，那些表现出网络能力的人被称为伪造者，并获得&#039；从第一个进来的人那里不收取任何费用，而是通过一个确定性的系统获得奖励)在网络上提供计算资源。，进而伪造自己的新币。从经济角度来看，矿商&#039；工作是有回报的，而造假者其实是在投自己的钱。

但是，在这两种情况下，哈希都用于解决这些计算密集型问题。这些问题自然会给网络分配新的资金。请记住，比特币将只能铸造2100万枚硬币，其中许多硬币已经在流通，因为其代码中内置了指数补偿功能。以太坊是一种大规模的PoS加密货币

。在伪造者的参与下，

以太坊也将不得不限制其新增货币流出，因为如果控制不当，可能会导致不良的通货膨胀。

结论

因此，哈希提供了一种强大的机制来混淆数据，尤其是在数字签名中。

但在其他应用程序中也是如此。此外，尽管散列的确切原因是它的逆问题(用于解码散列值)现在被用于在基于区块链的网络上民主化网络资源的使用。