

🏠 学院首页 > 区块链教程 > 新手入门 > 什么是哈希和电子签名？

什么是哈希和电子签名？

币学院 副船长 船龄 3.4年

2018-06-11 10:44:00

来源

👁 30870

💬 3

今天，我们就来把区块链拆分开，详细聊聊到底什么是区块链。我们知道，区块链背后的技术其实主要就是加密算法，其中主要包含两块，一个是哈希，另一个就是电子签名。



哈希和电子签名是什么？

哈希的意思就是引入随机数量的输入数据，将其加密，然后得出一个固定输出数据，就叫做哈希。输入可以是任何数据，只要能代表单个字节，一个MP3文件，整本小说，你的银行账单，甚至是整个互联网。关键在于输入可以无限大。哈希算法可以根据你的需求来进行选择，现在公开的也有很多种算法。关键点在于，这些算法会将无限的输入，转换成固定数量的字节。例如，256字节。

那么这个哈希有什么用呢？现在哈希通常的用处就在于指纹识别，同时也被称为检测区域。这意味着一个哈希被用来验证一个文件没有被任何人更改。假设WikiLeaks发布了使用MD5哈希的文件，任何人下载这些文件，都可以通过MD5哈希验证文件的来源。如果哈希和WikiLeaks发布的不符合，那么你就知道这个文件肯定是被改过的。

那么区块链是如何使用哈希的呢？区块链使用哈希，来表现整个区块链网络现在的状态。输入则是区块链的整个状态，也就是说近期完成的所有转账，输出就是哈希代表的区块链现在的状态。哈希就被用来在区块链网络中让各方相信，整个状态都是相同的。但是这些哈希是怎么算出来的呢？

首个哈希是为第一个区块或者是创世区块所计算的，通过区块内部的转账数据得出。初始转账的顺序被用来计算创世区块的区块哈希。后来每挖出的新区块，之前的区块哈希也会被使用，同时还有这个区块的转账信息，作为输入值，来确定区块的哈希。这就是区块链的形成方式，每个新区块哈希指向地是之前区块的哈希。这种哈希系统保证了任何转账记录都不会被改变，因为如果任何部分的转账记录改变，那么归属于这个区块的哈希值也会改变，那么任何接下来的区块哈希也会被改变。那么你可以简单地将哈希对比，就很容易去分辨出哪儿发生了改变。这就非常棒了，因为区块链上的每个人只需要对这256个字节达成共识，就可以代表区块链的状态。以太坊

推荐教程

喵懂区块链05期 | 人肉搜索如此强大

比特币qt钱包C盘数据迁移简介

共识算法的比较：Casper vs Tendermint

1982年，拜占庭将军问题首次被Lamport和Pease提出。Cosmos的Ethan Buchman

通过瑞波币搬到 Bitstamp 教程

什么是安全散列算法SHA256？

比特币如何挖矿（挖矿原理）-工作证明

加密货币交易平台 Vircorex介绍

蚂蚁矿机B3挖矿教程

什么是比特币交易确认？

恒星币概念与词汇



那么电子签名又是什么呢？电子签名，和真实签名一样，为了证明某人的身份，但是使用加密算法，会使得签名更加安全，不像手写的那种，可以很容易地修改。数字签名可以证明这个信息是从某个特定的人那儿来的，而且不是任何其他人，比如黑客。

电子签名在现今互联网中也有所应用。不论何时你通过ACTPS访问网站，你都是在使用SSL，这就是通过电子签名来保证你和服务器之间的安全性。这意味着当你访问Facebook.com时，你的浏览器可以检查跟随页面的数字签名，来验证者确实是从Facebook网页传来的，而不是从黑客。

在非对称的加密系统中，用户可以获得密钥对，这是由使用某种算法的公钥和私钥组成的。公钥和私钥是通过数学关系相互连接的。公钥的意思是公开发布的，作为从其他用户处接受信息的地址，就类似IP地址或者是家庭住址。私钥意味着隐秘的信息，用来将签署电子信息，并发送给别人。签名包含在信息中，以至于接受者可以验证发送者的公钥。这样地话，接收者就可以保证只有发送者可以发送这条消息。在区块链上创造账号，就可以获得密钥对，但是并不需要在任何地方进行注册。而且区块链上的任何交易都是由发送者使用私钥进行电子签名后才行。这个签名保证了只有账户拥有者可以转移其中的资产。

总结来看，区块链不能没有哈希和电子签名。哈希使得区块链上的人对现在的整体状态达成共识，电子签名却保证了所有交易都只由正确的人发出。我们依赖于这两个特性，来保证区块链不会存在任何欺诈和贪污现象。

全部 最佳

 **Friday7771** 船员 船龄 1.3年 2019-02-16 11:44:23

谢谢分享

👍 0 赞 ↩ 回复 🗨 0 踩

 **mia2018** 船员 船龄 1.5年 2018-12-11 09:08:39

数字签名没讲清楚啊，还有一些语句也不通顺，小韭菜一脸懵，踩

👍 0 赞 ↩ 回复 🗨 0 踩

 **68682410** 水手 船龄 3.6年 2018-07-19 12:44:42

学习了


👍 0 赞 ↩ 回复 🗨 0 踩

请发表你的真知灼见（不少于5个字）...

发表评论

👍 点赞 0 ☆ 6 次收藏 🔄 分享

下一篇：[壕撒1000万KT，持有SNET持久获空投](#)



巴比特学院是巴比特旗下的教育培训品牌，由巴比特主办，与专业培训机构合作，邀请业内区块链专家和实践者作为培训导师，通过导师现场授课、行业高端论坛、企业调研走访等方式，打造国内一流区块链培训品牌，推动区块链在中国的发展与创新。2018年，巴比特学院的品牌影响力将向杭州以外的北京、上海、南京、成都、深圳、广州等地辐射。

关于我们

关于巴比特

使用条款

版权声明

品牌素材

联系我们

联系人：学院课代表

微信：btczs001

地址：杭州市西湖区西溪首座

扫码咨询

