



资讯 ▾

快讯 ▾

视频 ▾

专栏 ▾

学院 ▾

产业区块链 ▾

NEW 海盗号

更多 ▾



搜索...

[学院首页](#) > [区块链教程](#) > [新手入门](#) > 什么是哈希现金（HashCash）机制？

什么是哈希现金（HashCash）机制？

无主之地 副船长 船龄 7.7年 2015-10-07 01:30:00 来源

👁 52925 💬 5

比特币工作量证明（POW）机制是要求对方服务前，必须要出据某种工作证明的机制。主要用于防止拒绝服务攻击和反垃圾信息。通常这种“工作证明”会花费一定的时间计算才能得到。最常见的例子是CAPTCHA。另外用于防止DoS和垃圾信息的机制是HashCash，比特币使用的原理就类似于HashCash。



哈希现金（hashcash）的灵感来自于这样一个想法，即一些数学结果难于发现而易于校验。一个众所周知的例子是因数分解一个大的数字（尤其是因数较少的数字）。将数字相乘来获得它们的积的代价是低廉的，但首先找到那些因数的代价却要高得多。

对交互式质询来说，因数分解足以胜任。比如，希望客户端能象征性地为其付出代价方能访问在线资源。这个时候可以定义协议，首先服务器向客户端发送一个消息，说“只要您能因数分解这个数，我将让您得到这个资源”。没有诚意的客户端将无法得到我的资源，只有那些能够证明自己有足够的兴趣、付出一些CPU周期来回答这个质询的才能得到这个资源。

不过，有一些资源无法很方便地进行交互式协商。比如电子邮件反垃圾或者支付交易，怎样才能避免邮箱不被垃圾邮件所占据？“我并不介意陌生人给我写信，但是，我希望他们能以稍微认真的态度，亲自通过对我有价值的邮件与我取得联系。至少，我不希望他们是垃圾邮件制造者，那些人向我和上百万的其他人发送包含同样消息的邮件（double-spending），期望我们中的某些人能购买某种产品或者落入一个骗局。”而对于电子货币，内容的复制几乎是没有什么代价的，如何保证电子货币（内容）没有被交易（发送）多次？这和反垃圾邮件是同样的问题。

hashcash的解决之道就是在电子邮件的消息头中，增加一个hashcash戳记（hashcash stamp）散列值。该散列值中包含收件人地址，发送时间，salt，该散列值特别之处在于它至少前20位必须是0才是一个合法的hashcash戳记。为了得到合法的散列值，发送者必须经过许多次尝试（改变salt值）才能获得。一旦生成戳记，不希望每一个给我发送邮件的垃圾邮件制造者都能重复使用它。所以，hashcash戳记要带一个日期。这样可以指定时间更早的戳记是非法的。另外hashcash的接收端要实现一个double-spending数据库，用来记录戳记的历史信息。

推荐教程

什么是黑币（BLK）？

中文名：黑币英文名：BlackCoin简称：BLK
作者：rat4（Bitcointalk论坛）黑币诞生于

区块链中的共识机制分析与对比

喵懂区块链15期 | 拒做吃瓜群众，关

轻松读懂以太坊上的 Gas、GasLimit

如何在以太坊区块链上写一段话——

BTC-E交易平台充值提现教程

超级账本Fabric 1.0 多节点集群的部

比原链BTM用户手册

以太坊 2.0 信标链中的状态转换

区块链技术（八）：以太坊公开拍卖

全部 最佳

👍 点赞 0

☆ 1 次收藏

🔗 分享

下一篇：[相对于比特币有创新的山寨币有哪些？](#)

 **山寨币开发** 禁止发言 船龄 4.9年 2016-05-12 17:05:33

不停的变更区块头中的随机数即nonce的数值，并对每次变更后的的区块头做双重SHA256运算（即SHA256(SHA256(Block_Header))），将结果值与当前网络的目标值做对比，如果小于目标值，则解题成功，工作量证明完成。
该过程可以用下图表示：

👍 0 赞 ↩ 回复 📄 0 踩

 船龄 2015-11-23 20:48:49

//@巴比特资讯: 转发微博

👍 0 赞 ↩ 回复 📄 0 踩

 船龄 2015-11-23 17:38:12

流言蜚语再多，我们陪在你身边。我们只专注于你的音乐，只专注于你。@GEM

👍 0 赞 ↩ 回复 📄 0 踩

 船龄 2015-11-23 16:55:15

#比特币# 什么是哈希现金（HashCash）机制? <http://t.cn/RyTSTuQ>


👍 0 赞 ↩ 回复 📄 0 踩

 **人在旅途** 水手 船龄 4.6年 2015-10-23 16:23:05

学习了，才有提高。

👍 0 赞 ↩ 回复 📄 0 踩

登录 账号发表你的看法，还没有账号？立即免费 注册



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

