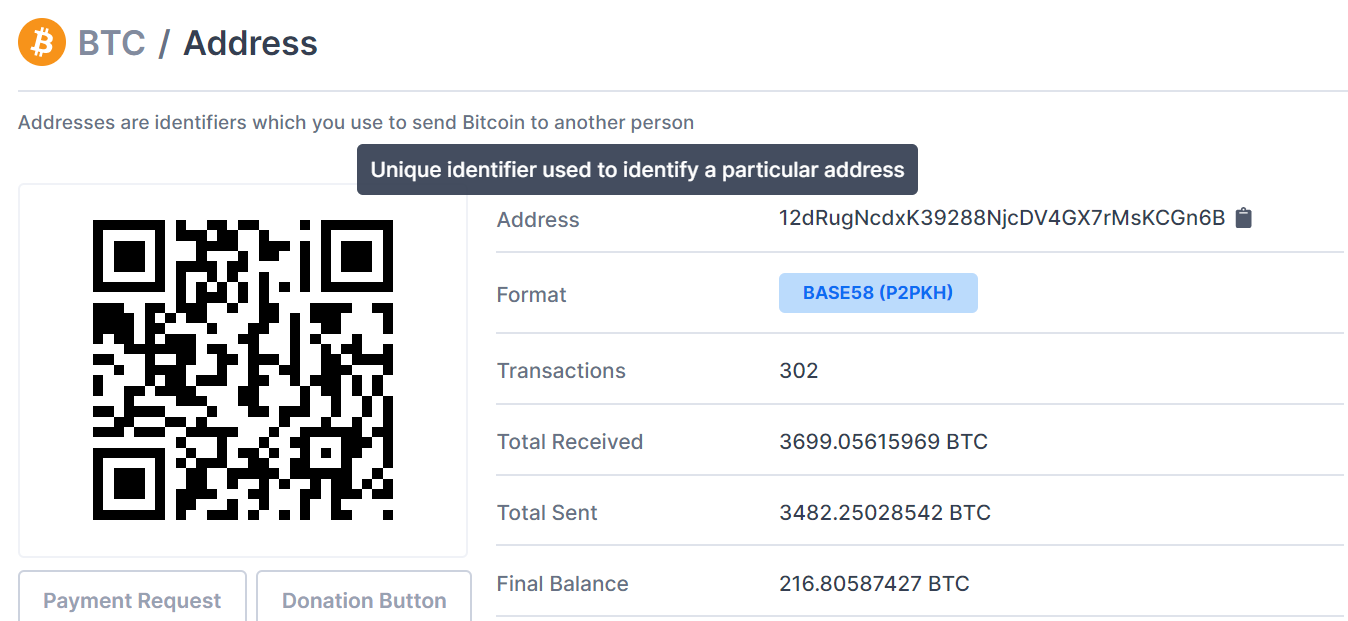
**一、概述**

挖矿现在已经被广为熟知，很多服务器在遭受入侵后，多数会被植入挖矿木马。2019年上半年的挖矿木马报告显示，日均新增6万个木马样本，挖矿木马已成为病毒木马黑产中的中坚力量。那为何挖矿木马会如此受到大家的青睐呢，是何利益一直驱使着大量黑客触犯法律铤而走险去入侵他人服务器植入挖矿木马。

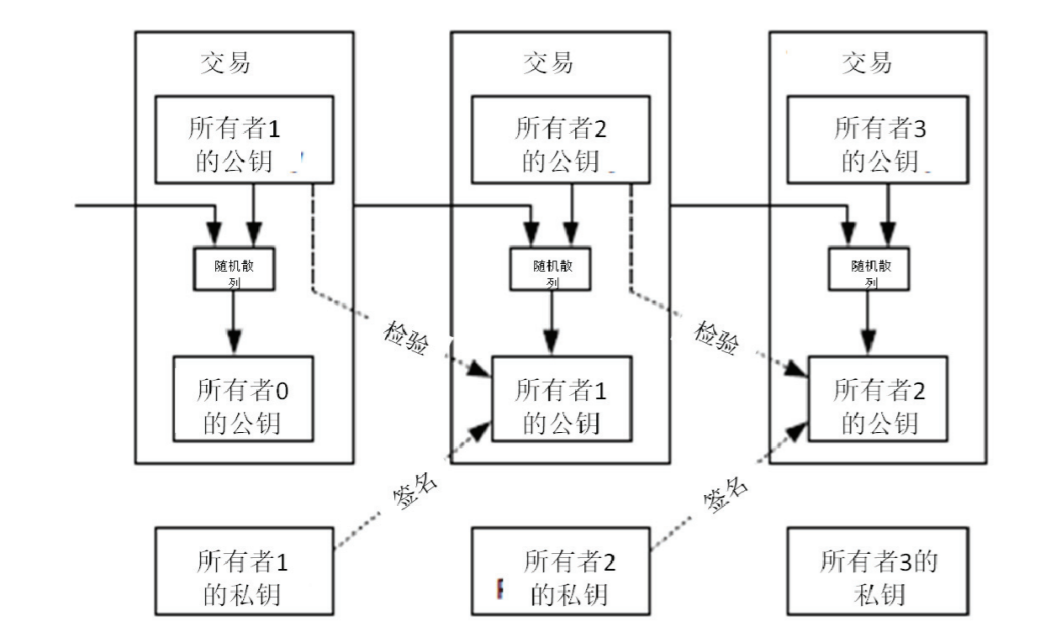
**二、挖矿的收益**

当下互联网的贸易，几乎都需要借助金融机构作为可信赖的第三方来处理电子支付信息，此类交易方式受限于“基于信用的模式”，无法实现完全不可逆的交易。比特币之父中本聪提出了电子支付系统，基于密码学原理，使得任何达成一致的双方，直接进行支付而不需要第三方中介参与。所谓的比特币实际就是一串数字签名，每一位所有者通过对前一次交易和下一位拥有者的公钥（Public key）签署的一个随机散列的数字签名。

比特币就是一串字符串，所谓的比特币交易也是一个地址转移到另外一个地址，并且比特币的交易记录也是公开的，每个地址拥有多少比特币都是公开的，可以通过https://blockchain.info/ 地址进行查询，只需要通过BTC地址就可查询到相关账户的比特币信息。

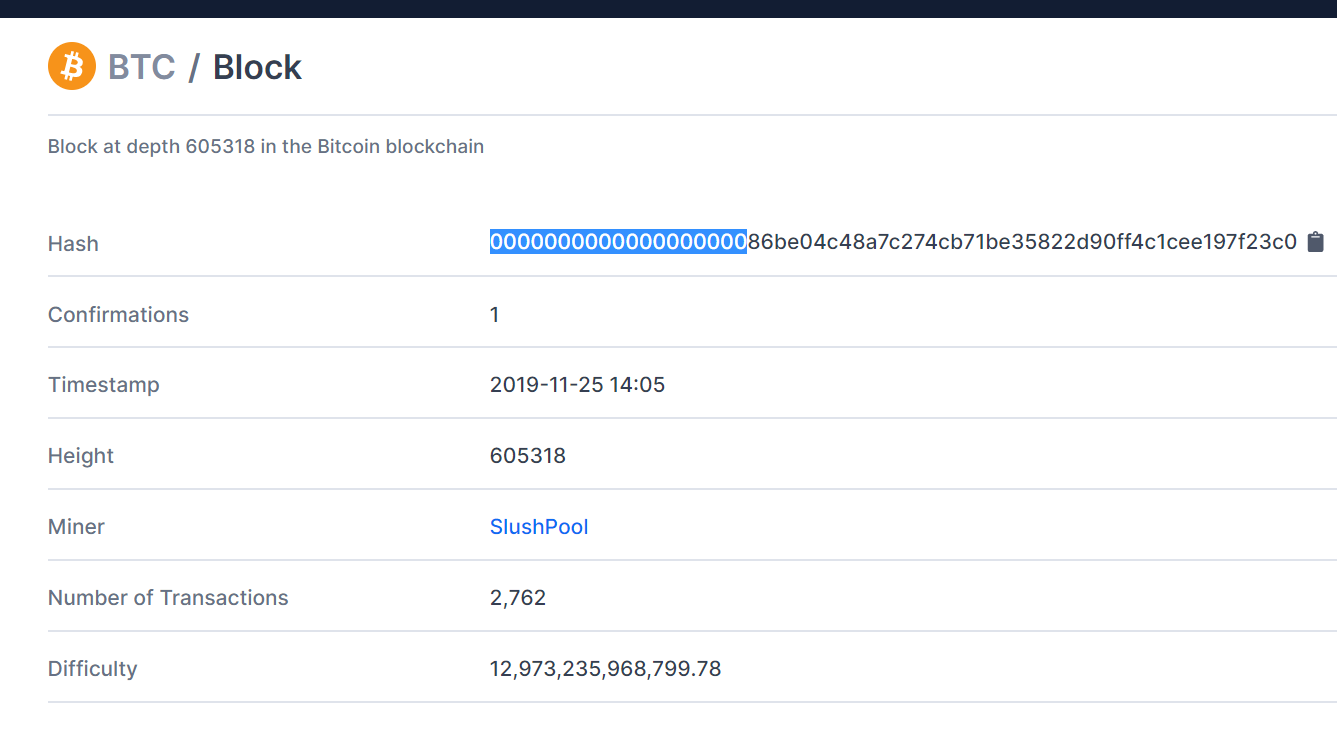


当两个账户进行交易时，付款方需要提供上一笔交易hash、本次交易双方地址、支付方公钥、支付方私钥生成的数字签名，整个交易过程如下：



在确认交易的真实性后，交易数据需要写入区块中，此时整个交易才算结束。写入区块的过程就是矿工所做的工作。根据比特币协议，一个区块大小大约是1MB，而每一笔交易大约是500字节左右，一个区块大约可以存储2000多条记录，矿工们负责将这些交易打包成一个区块，并且计算这个区块的hash值，也就是记账工作。中本聪最初设计是大约每10分钟产生一个区块，为了增加计算难度，引入了工作量证明（Proof-of-Work）。在区块中补增随机数（Nonce），这个随机数要使得该给定区块的随机散列值出现了所需的那么多个 0。我们通过反复尝试来找到这个随机数，直到找到为止，这样我们就构建了一个工作量证明机制。

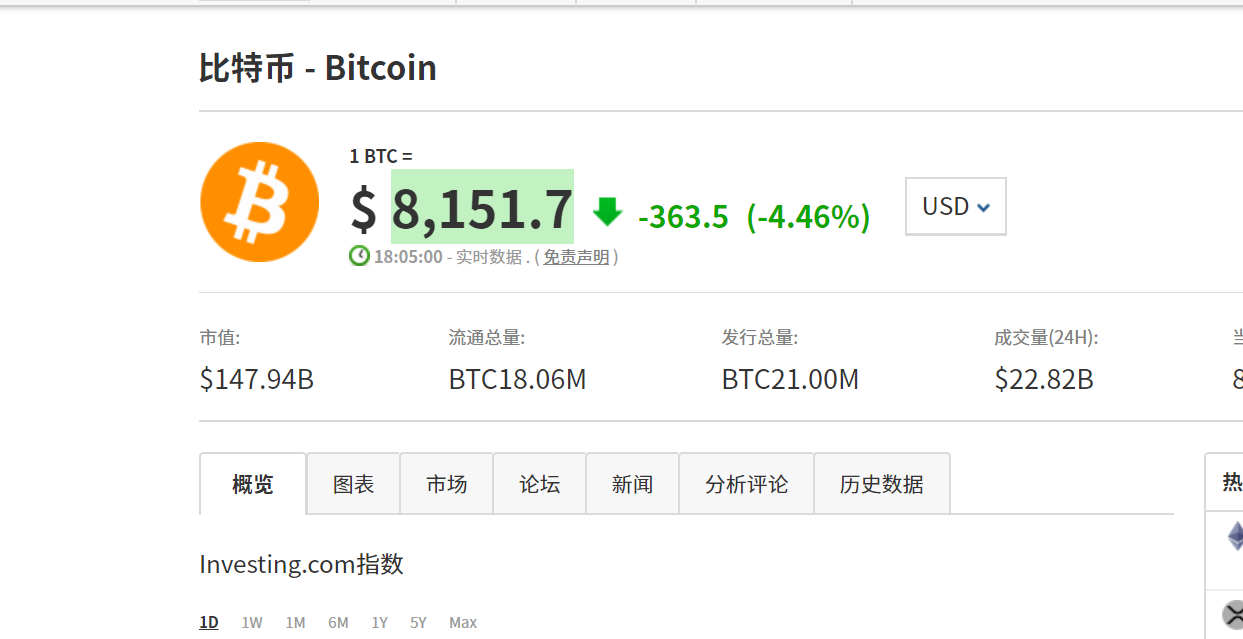
挖矿的过程实际就是在计算一道数学题，计算sha256（sha256（上一个Hash值，交易记录集，随机数）），通过不停的变换随机数，在经过海量计算后找到满足目标的hash数值。Hash的值由数字、大小写字母组成，每一位有62（10个数字、26个大写、26个小写）种可能性，那么第一位出现0的概率大约为62分之一，如果前两位为0则需要尝试62的平方次，如下区块前19位为0，则相当于尝试了62的19次方次计算，应该是已经上亿亿级别的运算了。



找到满足的hash值后，将记录添加到区块链中，也就意味着挖矿成功了，会获取整个区块的收益。由于需要较强的算力，所以现在很多矿工都加入矿池，通过贡献自己的算力共同挖矿，在获取收益后根据各自的贡献进行分享。这也就能解释多数被植入挖矿木马的机器，都会出现cpu使用骤增、耗电量增多现象，在挖矿木马进行分析时会发现矿池相关信息。

比特币协议规定，挖到新区块的矿工将获得奖励，一开始（2008年）是50个比特币，然后每4年减半，目前（2019年）是12.5个比特币。由于比特币可以分割到小数点后八位，那么到了2140年，矿工将得不到任何奖励，比特币的数量也将停止增加，大约为2100万个。这时，矿工的收益就完全依靠交易手续费了。

最新比特币价格约8000美金，折合人民币5万多，价格还是相当客观的，这也就是为什么大家对挖矿仍然热情不减。



**三、挖矿木马的传播方式**

现在很多的挖矿木马已经不在像之前那样傻傻的，通过top、netstat等命令可以直接看到恶意程序，现在会使用一些隐藏手段去隐藏挖矿进程来存活更久。其感染方式也是变的多种多样。

* 漏洞利用

Windows系统漏洞、服务器组件插件漏洞、中间件漏洞以及web漏洞；redis、ssh、3389、mssql、IPC$等各种弱口令漏洞。利用系统漏洞或弱口令快速获取相关服务器权限，植入挖矿木马。

* NSA武器的使用

“方程式黑客组织”使用的部分网络武器被公开，其中包括可以远程攻破全球约70% Windows系统的漏洞利用工具。包括永恒之蓝、永恒冠军、永恒浪漫、永恒协作、翡翠纤维、古怪地鼠、爱斯基摩卷、文雅学者、日食之翼和尊重审查。黑客NSA武器进行批量漏洞扫描攻击，获取更多肉鸡，植入挖矿木马贡献算力。

* 无文件挖矿

通过在Powershell中嵌入PE文件加载的形式，达到执行“无文件”形式挖矿攻击。新的挖矿木马执行方式没有文件落地，直接在Powershell.exe进程中运行，这种注入“白进程”执行的方式可能造成难以检测和清除恶意代码。

* 利用网页挂马

网站在其网页内嵌了挖矿 JavaScript 脚本，用户一旦进入此类网站，JS 脚本就会自动执行，自动下载若干个病毒。部分系统存在flash高危安漏洞，也被攻击者利用，使电脑自动运行挖矿代码。

* 暴力挖矿病毒

[360](http://www.360.cn/newslist/zxzx/WinstarNssmMinerlxsrljblwk.html) 发现了可以迅速传播的挖矿劫持程序WinstarNssmMiner。这个恶意程序的特别之处在于，卸载它会让受害者的计算机崩溃。WinstarNssmMiner首先启动svchost.exe进程并向其植入代码，然后将该进程的属性设置为CriticalProcess。由于计算机将其视为关键进程，因此一旦强制结束该进程，计算机就会蓝屏。

* 黑吃黑

因为比特币地址很长，为了方便使用很多人会选择保存在本地，很多挖矿木马会带有劫持剪贴板功能，当监视到受害主机出现比特币交易时，会将收款钱包替换为自己的钱包地址，从而盗取受害者资产。

最后蹭网也可能会被成为他人矿工，之前星巴克的公共wifi就被爆出被黑客利用来进行挖矿，黑客主要通过入侵 WIFI 提供商，在 WIFI 连接页面被植入挖矿代码，导致用户在连接 WIFI 时执行挖矿程序。

**四、防范建议**

1、 规范上网行为，不要下载来历不明的软件、工具；

2、 及时安装系统补丁，修复应用系统应用漏洞、中间件漏洞、组件、插件等相关漏洞。

3、加强密码策略，增加密码复杂度定期进行密码修改，开启相关登录失败处理策略，防止攻击者暴力破解。

学习参考：<https://www.anquanke.com/post/id/181873>