

今天给各位分享黑客为什么只收比特币的知识，其中也会对黑客为什么只收比特币呢进行解释，如果能碰巧解决你现在面临的问题，别忘了关注本站，现在开始吧！

本文目录

1. [为什么电脑病毒现在勒索都勒索比特币了？什么是比特币？](#)
2. [比特币能被黑客破坏吗？](#)
3. [比特币为什么要用这么多显卡？](#)
4. ["勒索病毒"为什么只要比特币？](#)

为什么电脑病毒现在勒索都勒索比特币了？什么是比特币？

5月12日晚间，一次黑客的行动，使全球近100个国家的微软系统计算机同时遭到名为WannaCry（想哭吗）或WannaDecryptor（想解锁吗）的电脑病毒袭击，至少4.5万台机器受到感染，造成数十亿网名的恐慌。在我国部分高校网络系统沦为重灾区，中石油加油站网络支付系统也受到影响。

设计此次病毒的黑客要求，用户在被感染后的三天内缴纳相当于300美元的比特币，逾期不缴，“赎金”翻倍。如果超过七天，仍不缴纳“赎金”，那么，攻击者就不客气了，直接把电脑上的数据和资料全部删除。

但是短时间付不起300美元怎么办？没关系，黑客还设了为期六个月的“人性化”特别还款通道。当然，如果你英语过关的话，可以发电子邮件和他们客服联系，人家说不定还会免除你的受害哦，台湾地区已有先例。

那么，问题来了，黑客为什么要比特币？比特币又是什么？

比特币（BitCoin）的概念最初由中本聪在2009年提出，根据中本聪的思路设计发布的开源软件以及建构其上的P2P网络。比特币是一种P2P形式的数字货币。点对点的传输意味着一个去中心化的支付系统。

与大多数货币不同，比特币不依靠特定货币机构发行，它依据特定算法，通过大量的计算产生，比特币经济使用整个P2P网络中众多节点构成的分布式数据库来确认并记录所有的交易行为，并使用密码学的设计来确保货币流通各个环节安全性。P2P的去中心化特性与算法本身可以确保无法通过大量制造比特币来人为操控币值。基于密码学的设计可以使比特币只能被真实的拥有者转移或支付。这同样确保了货币所有权与流通交易的匿名性。比特币与其他虚拟货币最大的不同，是其总数量非常有限，具有极强的稀缺性。该货币系统曾在4年内只有不超过1050万个，之后的总数量将被永久限制在2100万个。

不依靠特定机构发行的比特币，是一种基于区块链技术的“数字货币”。为什么在这次病毒袭击中，它会被犯罪组织所看中，成为黑客指定的“赎金”呢？这或许是因为其具有便捷、匿名的性质，可以实现快速的全球转账。

相比起其他方式，利用比特币汇款要更加“隐秘”。

正常的跨国汇款会经过层层外汇管制机构审查，交易记录会被包括银行在内的多方记录在案，甚至交易超过一定额度后，为防止洗钱等违规行为，还需向有关部门上报。

但如果用比特币交易就简单多了，只要输入数字地址，点几下鼠标，等待确认交易后，就可以完成交易。

同时，比特币价格在近期大幅上涨，也是其被黑客看中的原因。4月20日起，国内外市场的比特币价格强势突破。截至5月9日，中国的比特币价格突破9740元，创国内比特币历史新高。5月10日，比特币美元交易平台BITFINEX比特币上涨5.4%，最高价格达1779美元，折人民币12287.9元；日本比特币交易平台BITFLYER最高价达221.4万日元，折合人民币13004元；韩国比特币交易平台BITHUMB最高价2318000韩元，折合人民币14082元。目前，海外比特币交易平台均高出国内2600元以上。

加上这些因素，黑客们不喜欢才怪了！

比特币能被黑客破坏吗？

安全研究人员表示，黑客现在伪装加密货币挖掘恶意软件，并将其作为合法的Windows安装包传递出去。研究人员表示，这种恶意软件，通常被称为Coinminer，使用了一系列混淆方法，使其攻击特别难以检测。

这一发现来自安全公司趋势科技（TrendMicro），它表示，恶意软件作为WindowsInstallerMSI文件到达受害者的计算机上，这是值得注意的，因为WindowsInstaller是用于安装软件的合法应用程序。使用真正的Windows组件使其看起来不那么可疑，并可能允许它绕过某些安全过滤器。

黑客的诡计并不止于此。研究人员指出，一旦安装，恶意软件目录包含充当诱饵的各种文件。除此之外，安装程序还附带了一个脚本，可以杀掉在受害者电脑上运行的任何反恶意软件进程，以及受害者自己的加密货币挖掘模块。

研究人员还观察到，恶意软件具有内置的自毁机制，使检测和分析更加困难，它会

删除其安装目录下的每个文件，并删除系统中的任何安装痕迹。虽然趋势科技还无法将攻击链接定位到特定国家/地区，但它注意到安装程序使用了西里尔语。平心而论，西里尔语似乎在加密货币罪犯中非常受欢迎。

比特币为什么要用这么多显卡？

近几个月来，包括比特币在内的各种虚拟货币大行其道，尤其是这个比特币更是如此，其单价甚至超过了10000元人民币，价格可以说跟乘着火箭差不多。导致的结果就是AMD的显卡被矿工们抢光，市场上的400系与500系显卡也基本被一扫而光。

从比特币的本质说起，比特币的本质其实就是一堆复杂算法所生成的特解。特解是指方程组所能得到无限个（其实比特币是有限个）解中的一组。而每一个特解都能解开方程并且是唯一的。

为什么要用显卡挖矿？而不用cpu？

相比较于CPU的复杂运算，显卡使用的GPU进行的是通用计算。因此可以堆叠成百上千个流处理器，每一个流处理器就像是小小的CPU，虽然其运行复杂程序的能力远远没有CPU来的给力，但是架不住流处理器多，因此实际性能尤其是单精度浮点性能要比CPU强的多。挖包括比特币之内的动作大家可以认为是利用显卡在做不断地通用计算，并且这个计算复杂度比较低而且相当重复，显卡使用的流处理器正好适合这样的算法。就像是不断地解方程组，显卡是2000位中学生，而CPU则是8名数学博士。虽然数学博士的数学知识远远超过中学生，但是像解虚拟货币这样的中等方程组的速度8名数学博士肯定不如2000名中学生来的快。因此显卡越多，运算数量也大大增加。

"勒索病毒"为什么只要比特币？

文：张家明/海外财富网

自由主义一直是比特币的精神内核，无政府主义者是比特币早期拥趸，在他们眼中，天生反骨的比特币是“乌托邦世界”的经济基石，它从诞生之日起就是美联储的梦魇，未来会成为世界货币，重构全球金融体序，再造一个新世界。

今天的比特币已经破10000美元，总市值高达1600亿美元，此物一出天下反，已经不再是个口号。

什么是比特币？

比特币 (BitCoin) 的概念最初由中本聪在2009年提出，根据中本聪的思路设计发布的开源软件以及建构其上的P2P网络。比特币是一种P2P形式的数字货币。点对点的传输意味着一个去中心化的支付系统。

很多人仍然不明白什么是比特币，更不明白比特币为什么不受公权力打压，我们从“小岛经济学”上再来谈谈比特币为什么天生是个“反骨仔”。

在一个小岛上生活着一群善良的人民，他们以贝壳作为信用中介交换食物，日子过得幸福而美好。1000年过去了，岛上出现一彪形大汉，要求大家认可他家树上的叶子为唯一信用中介，试图反抗的人都被扔到海里喂鱼，善良的人民很快被驯服，慢慢以大汉家里的叶子作为等价交换物，岛民必须用物品换取叶子，再用叶子去交换其它物品。

日子一天天过去了，每个人手里的叶子越来越多，但买到的东西却越来越少，除了大汉自己，大部分人日子过得越来越紧巴。

有一天，一个聪明人发明一种新的记账方式，你只要将自己的明细提交到账本里，得到岛上6个人的认可，那么系统就认为这个账目是对的，所有的交易都在账目上用数字表示，如果这个人想去买东西，只需要在上面划账，就可以拿走商品。因为账目是公开的，每个人都可以对账单检查，除非随机6个人里面有4个人串通好。如果选择了这种方式，小岛上根本就不需要叶子。

说到这里，很多朋友应该已经明白，这个账本就是比特币，而叶子就是传统意义上的法币（每年都在增长），大汉则像政府。虽然很多人已经习惯了暴力信用，认为叶子天生有权威，而账本只是一串虚幻的数字，但从整个人类发展历史来看，其实账本才真正回归货币本质。不管你承不承认，比特币从出生的那一天起，它就是想来取代法币的。而传统的法币体系，是整个民族国家赖以生存的底层建筑。

目前，与大多数货币不同，比特币不依靠特定货币机构发行，它依据特定算法，通过大量的计算产生，比特币经济使用整个P2P网络中众多节点构成的分布式数据库来确认并记录所有的交易行为，并使用密码学的设计来确保货币流通各个环节安全性。P2P的去中心化特性与算法本身可以确保无法通过大量制造比特币来人为操控币值。基于密码学的设计可以使比特币只能被真实的拥有者转移或支付。这同样确保了货币所有权与流通交易的匿名性。比特币与其他虚拟货币最大的不同，是其总数量非常有限，具有极强的稀缺性。该货币系统曾在4年内只有不超过1050万个，之后的总数量将被永久限制在2100万个。

比特币可以用来兑现，可以兑换成大多数国家的货币。使用者可以用比特币购买一些虚拟物品，比如网络游戏当中的衣服、帽子、装备等，只要有人接受，也可以使

用比特币购买现实生活当中的物品。

比特币的诞生：

2008年爆发全球金融危机，当时有人用“中本聪”的化名发表了一篇论文，描述了比特币的模式。和法定货币相比，比特币没有一个集中的发行方，而是由网络节点的计算生成，谁都有可能参与制造比特币，而且可以全世界流通，可以在任意一台接入互联网的电脑上买卖，不管身处何方，任何人都可以挖掘、购买、出售或收取比特币，并且在交易过程中外人无法辨认用户身份信息。2009年，不受央行和任何金融机构控制的比特币诞生。或许这正是对2008年金融危机的一种绝望报复。政府已经没有办法控制自己了，货币滥发成了一种“财政鸦片”？或许比特币创立者中本聪（Satoshi）打包第一份开源代码时说了一句话：这是英国财政大臣达林考虑第二次出手纾解银行危机的时刻（这句话是泰晤士报当天的头版文章标题）。中本聪引用这个标题，正是对旧有的脆弱银行系统的冷嘲。

比特币的构成：

比特币是一种“电子货币”，由计算机生成的一串串复杂代码组成，新比特币通过预设的程序制造，随着比特币总量的增加，新币制造的速度减慢，直到2140年达到2100万个的总量上限，被挖出的比特币总量已经超过1200万个。

比特币最大的支撑是什么，是数学。一开始支持比特币的人，是信仰数学的人。它像一个猜谜游戏：在比特币节点里任何人都可以争取记账权，谁先解决一道数学题谁就先记账。这种数学题有个特点——解起来很难，验证很容易。这是比特币应用中使用的哈希算法（RIMPED160算法），它是比特币安全体系的“安全之链”以及椭圆曲线方程。（具体参考《人类最美的54个公式》）

比特币归根结底属于数学，它天生理性且中立。虽然自由主义者认为比特币承载了“此物一出天下反”的理想，但实际上比特币仍然只是数学在互联网世界的一种延伸，无论赋予它多少荣耀与光环，它仍然只是一个工具，与TCP/IP协议、支付宝、P2P一样，最大的意义就是为人民服务，如果不能改善个人的生活，BTC最终会沦为科技先验者的实证游戏。

新鲜实用的海外投资理财资讯，尽在海外财富网HaiwaiMoney.com

想要获取更多关于全球经济的信息，请关注海外财富网微信公众号（haiwaicaifuziXun）

黑客为什么只收比特币和黑客为什么只收比特币呢的问题分享结束啦，以上的文章

解决了您的问题吗？欢迎您下次再来哦！