

大家好，今天来为大家分享比特币打印价格查询网站的一些知识点，和比特币打印价格查询网站官网的问题解析，大家要是都明白，那么可以忽略，如果不太清楚的话可以看看本篇文章，相信很大概率可以解决您的问题，接下来我们就一起来看看吧！

本文目录

1. [09年网上买的比特币，怎样才能找回？](#)
2. [比特币和庞氏骗局的本质区别在哪里？](#)
3. [我就想知道让各大高校瘫痪的比特币病毒到底是什么鬼？](#)
4. [紧急求助！如何预防比特币病毒？](#)

09年网上买的比特币，怎样才能找回？

09年？几月？网上买的？什么网站？一看这些就知道楼主完全不了解比特币，也根本不了解比特币的特性，提出这样的问题也就是好奇而已。比特币是08年11月提出，09年1月正式推出，早期的比特币只能通过电脑显卡运算获得，后来也叫挖矿，也可以通过当时的论坛进行最初的交易，直到2010年3月才在国外诞生第一家交易所Bitcoinmarket.com而且根本不接受人民币交易，后来又陆续出了门头沟、BTC-E这样的头部交易所，但是也同样不直接接受人民币。国人想要进去交易必须得通过很复杂的手段才行，而且有金额限制，每年不超过5万美金，直到2011年国内才诞生第一家比特币交易所btcc比特币中国。还有你提问在网上找回，这就有很大矛盾，09年出来后，所有的采矿、赠与获得的比特币都是通过比特币全节点钱包完成，也就是说当时的比特币全都是保存在钱包里，也没有任何平台和网站可以保存，如果你没有钱包那你是如何购买的呢？

比特币和庞氏骗局的本质区别在哪里？

比特币并非庞氏骗局

欧洲中央银行曾对比特币进行仔细认真的研究以后，于2012年发表分析报告判断：目前未有任何迹象表明比特币是庞氏骗局。

要说清楚这个问题，我们首先要了解下什么是庞氏骗局：

这哥们叫查尔斯·庞兹（Charles Ponzi）庞氏骗局就是以他的名字命名的

他是一位生活在19、20世纪的意大利裔投机商，1903年移民到美国，1919年他开始策划一个阴谋，骗子向一个事实上子虚乌有的企业投资，许诺投资者将在三个月

内得到40%的利润回报，然后，狡猾的庞兹把新投资者的钱作为快速盈利付给最初投资的人，以诱使更多的人上当。由于前期投资的人回报丰厚，庞兹成功地在七个月内吸引了三万名投资者，这场阴谋持续了一年之久，才让被利益冲昏头脑的人们清醒过来，后人称之为“庞氏骗局”。

说的简单点，用两个成语概括就是“拆东墙补西墙”，“空手套白狼”。他的最大特别就是用高回报率去骗取投资者的钱，然后用后边投资者的钱去还许诺给前面投资者的利润。

这样只要骗子能一直收纳新的投资，他就可以拿出钱去付他承诺的高利润，游戏就可以继续下去。一但没有新的人加入，资金链就会断裂，骗子就没有办法偿还高额的利息和本金。（实际上总有这么一天）只能选择携款跑路了。

庞氏骗局的本质就是一场骗局

再说说比特币

中本聪于2008年发表了一篇名为《比特币：一种点对点式的电子现金系统》，之后于2009年为了验证他的理论便造出了比特币。

中本聪虽然目前还不知道他到底是何方神圣，但这个人对经济学，网络技术，密码学和编程都有很深的造诣。

比特币是有数量上限的（2100万个）这样就可以避免货币超发带来得通货膨胀。从目前看来任何国家都有超发货币的冲动（你手里有印钞机又缺钱的时候你会怎么选？）

比特币使用私匙作为数字签名交易，不需要通过银行，清算中心，证券商等第三方机构，从而避免了手续费、繁琐的流程、以及受监管的问题

中本聪又创造性的引入了区块链的概念，用矿机来记账。把各种需要数据中心记录的信息分布到各个矿机中。用分布式监管代替集中监管。以解决比特币的安全性问题

事实证明到目前没有一个组织和个人能破掉比特币的“金钟罩”

比特币本质是一种理想化，中心化的电子货币，它本身没有任何人去操作

至于比特币最近的暴涨，原因我们暂时不多做讨论。本质上也只是比特币兑换美元

的汇率的波动而已。

比特币从创建之初到现在没有任何人承诺过高回报，并通过这个高回报去引诱投资者，这就是比特币和庞氏骗局的本质区别。

比特币到系统从创建之初就是自动运行的，人们不需要也无法修改它的系统体系以及规则。就连中本聪本人也无法。

当然有很多人说，中本聪在初期收集了很多比特币（据称他持有一百万个比特币）。然后抬高比特币价格，坐收渔利。但比特币帐号的匿名性特点，其实这样的说法也只是坊间传闻。无据可查。

就算中本聪持有大量比特币是事实，也不能证明这就是庞氏骗局

第一，中本聪发明比特币的时候，他肯定也不会想到比特币会有目前这样高的价值。

第二：所有比特币的生产和去处，都有帐可查的。所以他拥有的比特币也不是他自己造出来的，只有可能是他在初期挖矿得来的。

第三在金融世界里早期投入获得暴利的事情到处都是。股票的原始股，就是一种很典型的例子。股票市场可并不是一种庞氏骗局哦。

所以在目前看来，比特币只是一种高风险的系统。大家要注意他的风险。但它和庞氏骗局还没有半毛钱关系。

我就想知道让各大高校瘫痪的比特币病毒到底是什么鬼？

这个病毒叫做“WanaCrypt0r2.0”（WanaCry直译过来，应该叫“想哭”），主要针对微软的Windows操作系统。

如果你不小心通过点开可疑邮件、未经扫描的附件等方式中招，那么等待你的将是：电脑所有文件会被加密锁定，制作病毒的黑客还会通过修改桌面壁纸和弹窗的方式，温馨提示被感染的机主（病毒提示内容甚至可因地区不同，而翻译成当地不同语言）。需要在指定时间内，支付价值300美元的比特币才能纾困，超时翻倍，拒绝的话，电脑中的文件可能会被彻底清空。

WannaCry病毒攻击的漏洞，是通过微软的Windows操作系统中的网络端口（如445、135、137、138、139端口等）以及网络共享等途径实现感染和攻击。这也解

释了为什么中国成为此次病毒攻击的主要受害地区——在中国，教育网因为没有关闭445端口而成为感染重灾区。

对普通用户来说，如果你及时升级，事情没有那么可怕，升级地址：

<https://technet.microsoft.com/zh-cn/library/security/ms17-010.aspx>

根据提示升级操作系统补丁就行了。

该病毒与美国国家安全局的黑客工具有关，或者最起码本次袭击借鉴了被泄露的NSA（美国国家安全局，好莱坞大片里经常见到）工具。去年起，一个自称为影子黑客（ShadowBrokers）的组织在网上公布了NSA针对Windows文件与打印机共享系统漏洞的黑客编程代码，但NSA从没有正面承认过。

紧急求助！如何预防比特币病毒？

以支付比特币换取解密为特征的计算机病毒来势汹汹，世界多国计算机均已中毒，其中英国和中国尤为严重。昨天今天被该病毒的消息刷屏了，该病毒危害性不少，特别是面临毕业季，很多学生的论文存在丢失的巨大风险。

首先说如何预防，我的建议是，作为个人计算机用户，首先要关闭445端口，下载微软补丁完成修复，推荐下载360提供的NSA武器库免疫工具，完成该病毒的防护，下载地址连接<http://dl.360safe.com/nsa/nsatool.exe>

此次病毒于5月12日晚在我国校园网开始蔓延。据360分析分析，该病毒是由NSA泄漏的“永恒之蓝”黑客武器传播的。“永恒之蓝”可远程攻击Windows的445端口，该端口方便用户在局域网中轻松访问各种共享文件夹或共享打印机。

用户计算机如果之前安装的2017年3月的微软补丁，则不会中招。之前由于国内曾多次出现利用445端口传播的蠕虫病毒，中国电信等运营商对个人用户封掉了445端口，但教育网并无此限制，存在大量暴露着445端口的机器，因此成为不法分子使用NSA黑客武器攻击的重灾区。

根据360公司周鸿祎的说法，目前“永恒之蓝”传播的勒索病毒以ONION和WNC RY两个家族为主，受害机器的磁盘文件会被篡改为相应的后缀，图片、文档、视频、压缩包等各类资料都无法正常打开，只有支付赎金才能解密恢复。这两类勒索病毒，勒索金额分别是5个比特币和300美元，折合人民币分别为5万多元和2000多元。

。

根据360针对校园网勒索病毒事件的监测数据显示，国内首先出现的是ONION病毒，平均每小时攻击约200次，夜间高峰期达到每小时1000多次；WNCRY勒索病毒则是5月12日下午新出现的全球性攻击，并在中国的校园网迅速扩散，夜间高峰期每小时攻击约4000次。

其实，针对NSA黑客武器利用的Windows系统漏洞，微软早在2017年3月已发布补丁修复。360公司也已推出NSA武器库免疫工具，能够一键检测修复NSA黑客武器攻击的漏洞，对WindowsXP、2003等已经停止更新的系统，免疫工具可以关闭漏洞利用的端口，防止电脑被NSA黑客武器植入勒索病毒等恶意程序。

文章分享结束，比特币打印价格查询网站和比特币打印价格查询网站官网的答案你都知道了吗？欢迎再次光临本站哦！