



我被通知在“挖矿”?! 莫慌, 按照指引来操作



信息网络工程研究中心

2022.5.10

什么是虚拟货币“挖矿”？

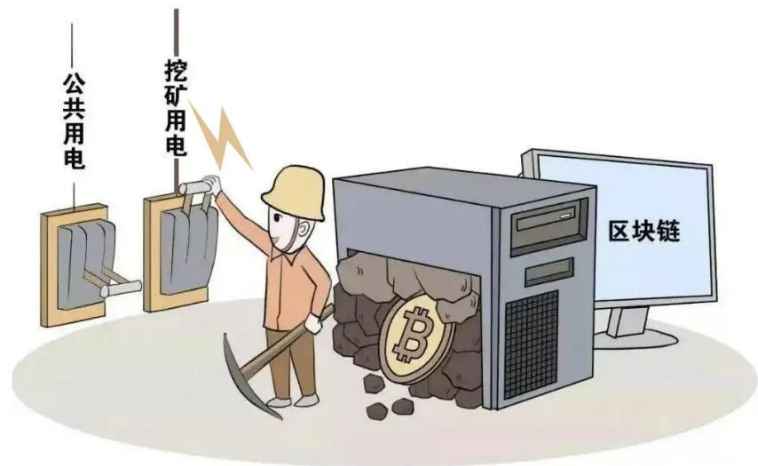


- **虚拟货币**是特定的虚拟商品，不是货币当局发行，不具有法偿性和强制性等货币属性，并不是真正意义上的货币，不具有与货币等同的法律地位，不能且不应作为货币在市场上流通使用，公民投资和交易虚拟货币不受法律保护。
- **虚拟货币“挖矿”**是指通过计算机参与算法计算来获得虚拟货币的过程（俗称“挖矿”），最重要成本是“矿机”提高算力的显卡、GPU等配置和运行所需的电费。



“挖矿”行为的危害

- “挖矿”行为能源消耗和碳排放量大，与国家的“碳中和”目标相悖，同时其本身对国民经济贡献度低，对产业发展、科技进步等贡献度低。
- 虚拟货币完全是一个炒作出来的商品，在使用电脑对其计算的时候，会浪费大量的电力，而在这个过程中没有产出任何有用的物质，只是搞出了一串数字而已，并且这串数字还很有可能被用来犯罪。



虚拟货币“挖矿”违法吗？

- 2021年9月3日 《国家发展改革委等部门关于整治虚拟货币“挖矿”活动的通知》发改运行〔2021〕1283号
- 虚拟货币“挖矿”活动能源消耗和碳排放量大，对国民经济贡献度低，对产业发展、科技进步等带动作用有限。整治虚拟货币“挖矿”活动对促进我国产业结构优化、推动节能减排、如期实现碳达峰、碳中和目标具有重要意义。
- **整治意义：金融风险，产业结构优化，节能减排**
- **总体要求：严密监测、严防风险、严禁增量、妥处存量**
- **治理手段：停止优惠政策，限制供电**
- **对象：政府部门、企事业单位**



中华人民共和国国家发展和改革委员会
National Development and Reform Commission

热门搜索：油价 产业结构调整

请输入关键字

首页

机构设置

新闻动态

政务公开

政务服务

首页 > 机构设置 > 机关司局 > 政研室 > 重要工作

国家发展改革委等部门关于整治虚拟货币“挖矿”活动的通知

发布时间：2021/09/30

来源：政研室

打印



微博



微信

为有效防范处置虚拟货币“挖矿”活动盲目无序发展带来的风险隐患，深入推进节能减排，助力如期实现碳达峰、碳中和目标，现就整治虚拟货币“挖矿”活动有关事项通知如下：

一、充分认识整治虚拟货币“挖矿”活动的重要意义

虚拟货币“挖矿”活动指通过专用“矿机”计算生产虚拟货币的过程，能源消耗和碳排放量大，对国民经济贡献度低，对产业发展、科技进步等带动作用有限，加之虚拟货币生产、交易环节衍生的风险越发突出，其盲目无序发展对推动经济社会高质量发展和节能减排带来不利影响。整治虚拟货币“挖矿”活动对促进我国产业结构优化、推动节能减排、如期实现碳达峰、碳中和目标具有重要意义。各地区、各部门和有关企业要高度重视，充分认识整治虚拟货币“挖矿”活动的必要性和重要性，切实把整治虚拟货币“挖矿”活动作为促进经济社会高质量发展环节，采取有效措施，全面整治虚拟货币“挖矿”活动，确保取得实效。

二、总体要求

(一) 指导思想。以习近平新时代中国特色社会主义思想；五中全会精神，深入贯彻习近平生态文明思想，坚定不移贯彻“绿水青山就是金山银山”的总体思路，充分发挥各地区、各部门合力，加强虚拟货币“挖矿”项目，加快存量项目有序退出，促进产业结构优化和助力碳达峰、碳中和目标。

(二) 基本原则。

坚持分级负责。建立中央统筹、省负总责、市县落实的工作；省级政府对本区域范围的整治工作负总责，并压实市县各级政府按照中央部署和省级政府实施方案要求，细化落实举措，确保取得实效。

坚持分类处理。区分虚拟货币“挖矿”增量和存量项目，严禁新增虚拟货币“挖矿”项目，在保证平稳过渡的前提下，结合各地实际情况，加快有序退出存量项目。

坚持依法依规。运用法治思维和法治方式全面推进虚拟货币“挖矿”活动整治，严肃查处整治各地违规虚拟货币“挖矿”活动。



信息网络工程研究中心(信息化办公室)

Information and Network Engineering and Research Center (Office of Information Technology)

虚拟货币“挖矿”违法吗？



2022年6月11日 星期三

无障碍模式



中华人民共和国国家发展和改革委员会
National Development and Reform Commission

热门搜索：油价 产业结构调整

请输入关键字

首页

机构设置

新闻动态

政务公开

政务服务

首页 > 政务公开 > 政策 > 发展改革委令

中华人民共和国国家发展和改革委员会令

第49号

《国家发展改革委关于修改〈产业结构调整指导目录（2019年本）〉的决定》已经2021年12月27日第20次委会议审议通过，现予公布，自发布之日起施行。

主任：何立峰

2021年12月30日

附件：

《国家发展改革委关于修改产业结构调整指导目录（2019年本）的决定》.pdf

国家发展改革委关于修改 《产业结构调整指导目录（2019年本）》的决定

在《产业结构调整指导目录（2019年本）》淘汰类“一、落后生产工艺装备”“（十八）其他”中增加第7项，内容为“虚拟货币‘挖矿’活动”。



信息网络工程研究中心(信息化办公室)

Information and Network Engineering and Research Center (Office of Information Technology)

虚拟货币“挖矿”违法吗？

广东省发展和改革委员会“虚拟货币‘挖矿’行为违法性质知识科普”

案例一：

省内严查严处国有“挖矿”活动，多人被处分

案例二：

利用办公电脑“挖矿”，受党内警告处分

案例三：

虚拟货币“挖矿”相关协议，不受法律保护

虚拟货币“挖矿”行为违法性质知识科普

原创 广东省发展改革委 广东省发展和改革委员会 2022-03-22 21:02

点击  “广东省发展和改革委员会”关注我们

一、什么是虚拟货币？什么是虚拟货币？

虚拟货币以数字化形式存在于网络世界中，不具有与货币等属性，也不具有与货币等同的效用，投资和交易虚拟货币的行为也不受法律保护。虚拟货币“挖矿”活动指通过专用“矿机”计算，对国民经济贡献度低，对产业发展、和交易环节衍生的风险越发突出，其盲目无序带来不利影响。



二、“挖矿”的危害



信息网络工程研究中心(信息化办公室)

Information and Network Engineering and Research Center (Office of Information Technology)

拒绝主动“挖矿”，防范被动“挖矿”



- **主动“挖矿”**——顾名思义，以任何形式主动参与“挖矿”活动的行为；
- **被动“挖矿”**——多数是由于上网终端感染“挖矿”病毒，导致被动参与“挖矿”活动。
- 在学校范围内，任何“挖矿”行为都会造成公共资源的消耗和浪费，主动“挖矿”、被动“挖矿”都是违规行为。全校学生、教职工应提高网络安全意识、规范上网行为，对个人上网终端、办公科研主机落实安全防范措施，防范上网终端感染病毒而产生被动“挖矿”行为。学校网络中心将不断跟进“挖矿”病毒发展事态，为全校师生提供安全防范指引，全校齐心协力抵御“挖矿”病毒。



如何排查“挖矿”病毒？

- 在巨大利益趋势下，黑客通过各种可能手段传播“挖矿”病毒。
- **一不小心就中招**
- 上网用户以下行为都可能感染病毒：
 - 1、点击QQ、微信、邮件中的不明文件（钓鱼文件）；
 - 2、下载运行盗版软件（软件捆绑）；
 - 3、访问被植入挖矿脚本的网页（浏览器挖矿）；
 - 4、使用内网穿透软件、远程账号弱密码、主机漏洞不修复（漏洞传播）；
 - 5、pip、npm、gem等软件包安装命令输错字符串（恶意开源软件包）；
 - 6、随意使用U盘（U盘病毒）。
- “挖矿”病毒严重消耗主机的运行能力和电力，同时还将伺机向校内其他设备蔓延，甚至造成主机被非法控制。



如何排查“挖矿”病毒？



- 感染“挖矿”病毒的症状
- 1、主机运行卡顿，重启后依然卡顿
- 2、没打开软件，但CPU使用率几乎到达100%
- 3、主机温度偏高，风扇噪声大
- 4、杀毒软件发出“挖矿”病毒恶意软件告警
- 如果主机出现以上一种或者多种情况，这台主机可能已经感染了“挖矿”病毒。



如何排查“挖矿”病毒？



- **Windows系统排查和清理方法**
- 对于安装Windows操作系统的主机，建议开启Microsoft Defender 或者安装360、火绒等杀毒软件进行全盘查杀。
- 部分“挖矿”病毒隐藏比较深，杀毒软件不一定能查出，或者在进程表中也看不到。建议在关掉所有运行软件后，通过netstat -ano命令查看所有通信的PID，对链接可疑外部地址的进程文件进行重点查杀（方法参考附件1）。
- 一旦发现感染“挖矿”病毒，为避免查杀病毒不完全，建议直接进行电脑全盘格式化、重装系统。



如何排查“挖矿”病毒？



- **Linux系统排查和清理方法**
- Linux系统可安装ClamAV等杀毒软件进行病毒查杀，使用GScan、chkrootkit、rkhunter等工具进行入侵检查。
- 或者按以下方法进行手动排查：
 - 1、排查是否存在CPU或内存使用率异常高的进程，排查启动项、计划任务等，使用netstat命令查看是否存在不正常的网络连接，top命令检查可疑进程，pkill命令杀死异常进程；
 - 2、如果进程还存在，说明有定时任务或开机启动进程，使用/var/spool/cron/root、/etc/crontab 和/etc/rc.local检查。
 - 3、查找异常登录记录
- 通过grep、last和lastb等命令查找登录记录，确定系统的账户密码是否被泄露或爆破。
- 一旦发现感染“挖矿”病毒，为避免查杀病毒不完全，建议直接进行电脑全盘格式化、重装系统。



如何排查“挖矿”病毒？

- 浏览器“挖矿”清理方法
- 恶意网站在网页植入挖矿木马，用户访问了植入的网页后，浏览器会解析脚本进行挖矿。如果不小心点击了可疑网页，应注意浏览网页时CPU使用率，计算机CPU使用率飙升且大部分CPU使用来自于浏览器，那么网页中可能被植入了挖矿脚本。清理浏览器类型“挖矿”，先关闭浏览器，再打开任务管理器，找到并强制关闭仍在继续运行的浏览器进程。



如何排查“挖矿”病毒？

- 手机“挖矿”清理方法
- 手机挖矿病毒伪装为以正常应用，或利用浏览器网页进行挖矿。手机无端出现卡顿、发热、死机，可能是恶意应用在挖矿，建议安装手机杀毒软件进行查杀。
-



如何防范“挖矿”病毒



- **使用正版操作系统和软件，进行正确的安全配置**
- 1、使用正版操作系统和软件，从官方网站下载安装包，及时更新操作系统、软件版本和补丁，设置系统自动更新功能，时刻保持系统更新状态；
- 2、开启防火墙功能，安装杀毒软件，开启实时防护和自动更新，定期全盘深度查杀；
- 3、使用学校DNS服务器（自动获取IP时默认使用学校DNS服务器，无需再手动配置）；
- 4、手动关闭系统默认开启的但是并不使用的服务，建议检查并关闭系统的默认文件共享服务、网站服务等；
- 5、服务器限制可互联的IP范围，默认屏蔽任何不受信地址的连接请求；不需联网主机，离线运行；不需访问互联网的主机，申请封禁访问互联网。



如何防范“挖矿”病毒



- 保持良好的上网习惯
- 1、不要连接不明WIFI;
- 2、不要随意打开来自聊天工具或电子邮件附件中的不明文件;
;
- 3、使用主流安全的浏览器，建议开启防挖矿功能;
- 4、不要浏览色情内容或浏览器提示危险的网站;
- 5、不要安装任何内网穿透软件、翻墙软件;
- 6、不要随意安装外挂软件。



如何防范“挖矿”病毒



- **安全管理账号**

- 1、不要共享使用账号，也不要将自己的账号转借他人；
- 2、避免使用弱口令、默认密码、出厂密码以及允许未授权访问，避免多个应用或设备使用相同口令；口令不少于10个字符，至少包含大小写字母、特殊字符和数字；
- 3、多用户服务器，为每个用户建立单独账号；做好用户操作权限限制，禁止直接登录root，仅系统管理员可以切换到root账号；设置系统口令管理策略，强制使用强密码、设置密码有效期、设置连续输错密码锁定账号。



如何防范“挖矿”病毒



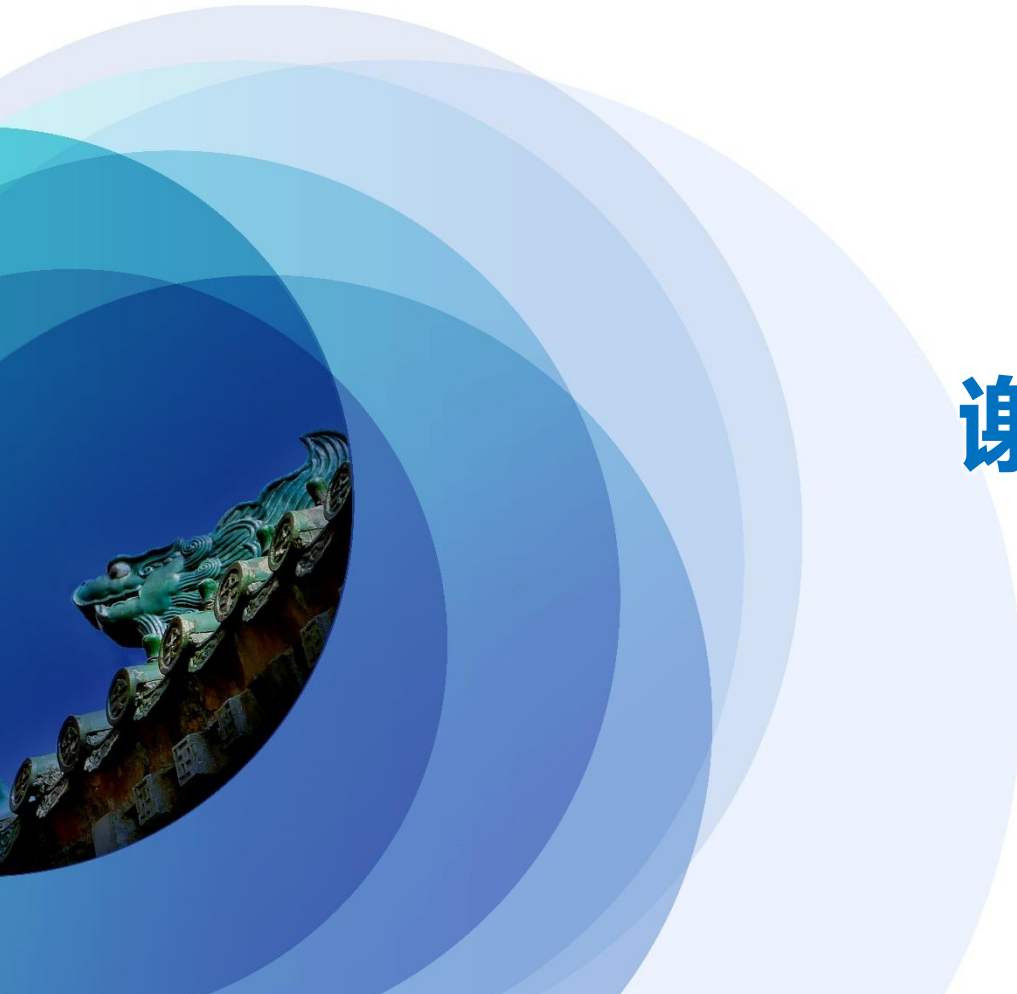
- **做好主机日常维护**
- 1、U盘不要随处插，每次使用前先扫描一遍；
- 2、个人主机不用时关机或断网，不要在不使用的情况下长时间联网待机；
- 3、服务器长时间不使用，应及时停机；
- 4、科研服务器应指定管理员，定期对系统运行情况、系统日志（特别是主机登陆成功和失败日志）、异常账号、病毒查杀情况进行巡查，及时清理不用的账号；
- 5、开启系统日志记录功能，且日志记录设置足够容量（如Windows设置事件日志1G）或记录时长（Linux系统设置180天）；
- 6、如需远程登录Linux的SSH服务，使用密码登录时应杜绝弱口令，推荐使用免密码的Public Key方式登录；Windows 远程桌面使用动态口令（可安装multiOTP Credential Provider）。



如何防范“挖矿”病毒

- 谨慎使用科研开发安装软件包
- 用pip、npm、gem等软件包安装命令输错字符串可能导致安装伪装的挖矿软件包，输入安装命令时严格检查字符串。





谢谢!

