目录

- 投机活动和价格的波动会成为比特币的一个问题吗？
- 如果有人将现有的比特币全部买下将会怎样？
- 如果有人创造了一个更好的数字货币将会怎样？

- 交易
- 为什么我必须等待 10 分钟？
- 交易手续费是多少？
- 如果我的电脑关机时接收到比特币会怎样？
- "同步"是什么意思？为什么同步要花很长时间？

- 挖矿
- 什么是比特币挖矿？
- 比特币的挖矿的原理是什么？
- 挖矿不是一种能源浪费吗？
- 如何通过挖矿帮助保护比特币的安全？
- 开始挖矿前，我需要些什么？

- 安全性
- 比特币安全吗？
- 比特币在过去被黑客攻击过吗？
- 用户是否可以联合起来攻击比特币？
- 量子计算是对比特币的威胁吗？

- 帮助
- 我想了解更多。我在哪里可以得到帮助？

概览

什么是比特币？

比特币是一个共识网络，促成了一个全新的支付系统和一种完全数字化的货币。它是第一个去中心化的对等支付网络，由其用户自己掌控而无须中央管理机构或中间人。从用户的角度来看，比特币很像互联网的现金。比特币也可以看作是目前最杰出的三式簿记系统。

谁创造了比特币？

比特币是第一个实现了“隐秘货币”概念的货币。1998 年，Wei Dai 在 cypherpunks 邮件列表中首次阐述了“隐秘货币”的概念，即：一个采用密码学原理控制货币的发行和交易、而不是依赖于中央管理机构的全新的货币形态。2009 年，中本聪（Satoshi Nakamoto 化名）在 cryptography 邮件列表中发表了第一个比特币规范及其概念证明。2010 年年底，中本聪离开该项目，关于

他的身份没有透露太多。此后，众多开发人员致力于比特币的项目，比特币社区迅速成长起来。

中本聪的匿名身份经常会引起毫无根据的忧虑，其中很多是与比特币开放源代码特性的误解有关。比特币的协议和软件都是公开发布的，世界各地的任何开发人员都可以查看其代码，或者开发他们自己修改过的比特币软件版本。就像目前的开发人员，中本聪的影响仅仅局限于那些他做出的被其他人采纳的改动，因此，中本聪并没有控制比特币。那么，在今天，关于比特币的发明者的身份问题可能和纸张发明者的身份问题一样。

谁在控制比特币网络？

没有谁拥有比特币网络，就像没有人拥有电子邮件背后的技术一样。比特币由世界各地所有的比特币用户控制。开发者可以改善软件，但他们不能强行改变比特币协议的规则，因为所有的用户都可以自由选择他们想用的软件。为了相互之间保持兼容性，所有用户也需要选择遵循相同规则的软件。只有所有用户达成完全一致的共识，比特币才能正常地工作。因此，所有的用户和开发者对接受和保护这一共识很有动力。

比特币是如何运作的？

从用户的角度来看，比特币就是一个手机应用或电脑程序，可以提供一个个人比特币钱包，用户可以用它支付和接收比特币。这就是比特币对于大多数用户的运作原理。

在幕后，整个比特币网络共享一个称作“块链”的公共总帐。这份总帐包含了每一笔处理过的交易，使得用户的电脑可以核实每一笔交易的有效性。每一笔交易的真实性由发送地址对应的电子签名保护，这使得用户能够完全掌控从他们自己的比特币地址转出的比特币。另外，任何人都可以利用专门硬件的计算能力来处理交易并为此获得比特币奖励。这一服务经常被称作“挖矿”。你可以查阅专用页面 和 原始论文来了解更多有关比特币的信息。

真的有人使用比特币吗？

是的，越来越多的企业和个人在使用比特币。这既包括像饭店，公寓和律师事务所那样的传统企业，也包括像 Namecheap，WordPress，Reddit 和 Flattr 这样的流行在线服务。虽然比特币仍然是一个相对较新的现象，但它发展迅速。2013 年 8 月底，流通中的比特币总值超过了 15 亿美元，每天都有价值数百万美元的比特币在进行兑换。

如何获得比特币？

- 作为商品或服务的支付方式。
- 在一个比特币交易所购买比特币。
- 和你附近的人兑换比特币。
- 通过具有竞争力的挖矿赚取比特币。

  尽管可能有人愿意让对方以信用卡或 PayPal 支付的方式购买自己的比特币，大部分的交易平台是不接受来自这些支付方式的资金的。这是为了防止某些情况下有人用 PayPal 购买比特币，然后在交易到一半的时候撤销。这通常被称作退单。

  ### 用比特币支付有多难？

  相比借记卡或信用卡购物，比特币付款更加容易，无需一个商家账户就可以接收比特币付款。在你的电脑或智能手机上的钱包应用程序中，输入收款人的比特币地址和付款金额，按发送键即可完成付款。为了更方便地输入收款人地址，很多钱包可以通过二维码扫描或者 NFC 技术触碰两部手机获得地址。

比特币的优势是什么？

- ***支付自由*** - 无论何时何地都可以即时支付和接收任何数额的资金。无银行假日，无国界，无强加限制。比特币允许其用户完全控制他们的资金。
- ***极低的费用*** - 目前对比特币支付的处理不收取手续费或者仅收取极少的手续费。用户可以把手续费包含在交易中来获得处理优先权，更快收到由网络发来的交易确认。另外，也有商家处理器协助商家处理交易，每天将比特币兑换成法定货币并直接将资金存入商家的银行账户。因为这些服务都基于比特币，所以它们可以提供远低于 PayPal 或信用卡网络的手续费。
- ***降低商家的风险*** - 比特币交易是安全，不可撤销的，并且不包含顾客的敏感或个人信息。这避免了由于欺诈或欺诈性退单给商家造成的损失，而且也没有必要遵守 PCI 标准。在信用卡无法使用或欺诈率高得令人无法接受的地方，商家也可以很容易地扩展新的市场。最终结果是更低的费用，更大的市场，和更少的行政成本。
- ***安全和控制*** - 比特币的用户完全控制自己的交易；商家不可能强制收取那些在其它支付方式中可能发生的不该有或不易发现的费用。用比特币付款可以无须在交易中绑定个人信息，这提供了对身份盗用的极大的防范。比特币的用户还可以通过备份和加密保护自己的资金。

- ***透明和中立*** - 关于比特币资金供给本身的所有信息都存储在块链中，任何人都可以实时检验和使用。没有个人或组织能控制或操纵比特币协议，因为它是密码保护的。这使得比特币核心被相信是完全中立，透明以及可预测的。

比特币的缺点是什么？

- ***接受程度*** - 仍然有很多人不知道比特币。每天有更多的企业接受比特币，因为他们希望从中受益，但这个列表依然很小，为了从网络效应中获益，仍然需要有更多的企业支持比特币。
- ***波动性*** - 流通中的比特币总价值和使用比特币的企业数量与他们可能的规模相比仍然非常小。因此，相对较小的事件，交易或业务活动都可以显著地影响其价格。从理论上讲，随着比特币的市场和技术的成熟，这种波动将会减少。这个世界以前从未出现过任何一个新兴货币，所以想象它将如何进展真的非常困难 (同时也令人兴奋)。
- ***处于发展阶段*** - 比特币软件依然处于 beta 版本，许多未完成的功能处于积极研发阶段。新的工具，特性和服务正在研发中以使比特币更为安全，为更多大众所使用。其中有一些功能目前还不是每个用户都能使用。大部分比特币业务都是新兴的，尚不提供保险。总体来说，比特币尚处于成熟的过程当中。

为什么人们相信比特币？

关于比特币的大部分信任来自于一个事实：它根本不需要任何信任。比特币是完全开源和去中心化的，这意味着任何人在任何时间都可以查看整个源代码。所以世界上的任何一个开发人员都可以精确验证比特币的工作原理。任何人都可以实时地一目了然地查询现存的所有的比特币交易和已发行的比特币。所有的付款不依赖于第三方，整个系统由大量专家审查过的密码学算法保护，比如那些用于网上银行的算法。没有组织或个人可以控制比特币，而且即使并非所有的用户都值得信任，比特币网络仍然是安全的。

我能用比特币赚钱吗？

你永远不应期望通过比特币或任何新兴技术致富。对于任何听起来好得令人难以置信，或违背基本经济规律的东西保持警惕始终是很重要的。

比特币是一个不断增长的创新领域，这里有商机，同时也有风险。即使到目前为止，比特币以飞快的速度在发展，但谁也不能保证它将继续增长。任何有关比特币的时间和资源的投入都需要创业精神。用比特币赚钱的方法有很多种，如挖矿，投机或经营新业务。所有这些方法竞争都很激烈，并且没有利润保证。每个人应该对任何此类项目中所涉及的成本和风险自己做出适当的评估。

比特币是完全虚拟和非物质的吗？

比特币和人们每天使用的信用卡和网上银行网络一样是虚拟的。比特币和其它任何形式的货币一样可以用来在网上或者实体商店支付。比特币也可以兑换成实体货币比如 Casascius 币，但是手机支付通常更加方便。比特币余额存储在一个大型分布式网络中，任何人都无法恶意修改。换句话说，比特币用户对他们的资金拥有唯一的控制权，比特币不会因为其虚拟性而消失。

比特币是匿名的吗？

和其他任何货币一样，比特币的设计允许其用户在一个可接受的隐私程度支付和接收付款。但是比特币不是匿名的，所以无法提供和现金一样的隐私程度。使用比特币会留下许多公共记录。有多种机制可以用来保护用户的隐私，还有更多正在开发中。然而，在大部分比特币用户正确使用这些功能前还有功夫要投入。

一些人担忧比特币的私下交易可被用于非法目的。值得一提的是，比特币无疑将受制于已经在现有的金融体系内发挥作用的类似规定。比特币不会比现金更具有匿名性，而且也不太可能防碍犯罪调查的进行。此外，比特币的设计也是为了防止大范围的金融犯罪。

比特币丢失时会发生什么？

当一个用户丢失了他的钱包，其后果是其中的资金退出流通。丢失的比特币和其它比特币一样依然存在于块链中。但是丢失的比特币将永远处于休眠状态，因为任何人都无法找到可以再次使用这些比特币的私钥。根据供求法则，当可用的比特币变少时，剩余的比特币会有更高的需求量，其价值就会升高作为补偿。

比特币能否扩大规模成为一个主要的支付网络？

比特币网络已经能够每秒钟处理比目前的处理量大很多的交易数量。但是它还没有完全成熟到可以将规模扩展至主要信用卡网络的程度。提高目前这一上限的工作正在进行中，未来的需求也非常清楚。从一开始，比特币网络的每一个方面都在不断成熟，优化和专门化，这一过程在今后几年内仍将持续。随着流量的增加，更多比特币用户可能会使用轻量级的客户端，而完全网络节点则可能成为更为专门化的服务。更多详情请查阅维基页面 可扩展性 。

合法

比特币合法吗？

据我们所知，比特币在大部分行政辖区并没有被立法机构界定为非法货币。但是，一些行政辖区(如阿根廷和俄罗斯)严格限制或禁止国外货币。其他行政辖区(如泰国)可能限制颁发许可给某些实体，如比特币交易平台。

来自不同行政管辖区的监管机构正在采取措施，就如何将这项新技术与正规的，受监管的金融体系结合在一起，为个人和企业提供一些规则。例如，美国财政部的金融犯罪执法网络(FinCEN)，就如何描述涉及虚拟货币的某些活动，发布了非约束性的指导。

比特币对非法活动有用吗？

比特币是货币，而货币的使用一直以来都有合法和非法的目的。在被金融犯罪利用的程度上，现金，信用卡和目前的银行系统是远远胜过比特币的。比特币能够带来支付系统的重大革新，这些革新所带来的裨益被认为是远远超过其潜在弊端的。

比特币的设计是提高货币安全性的巨大进步，也是针对许多金融犯罪形式的重要保护机制。例如，比特币完全不可能被仿造。用户完全掌控他们的支付交易，不会像信用卡诈骗那样收到未核实的费用。比特币交易是不可撤销的，避免了诈骗性退单。通过非常强大且有用的机制，比如备份，加密和多重签名，比特币可以保护资金免于盗取和遗失。

一些人担忧比特币对于罪犯可能更具吸引力，因为它可以用来进行私下的和不可撤销的付款。然而，这些功能早已存在于完善的被广泛应用的现金和电汇中。比特币的使用无疑将受制于已经在现有金融体系内发挥作用的类似规定，而且它也不太可能防碍犯罪调查的进行。一般来说，当一些重要突破没有被熟知之前，存在争议是很常见的。其中，互联网就是一个很好的例子可以说明这种情况。

比特币能被监管吗？

比特币协议本身是不能修改的，除非几乎全部的用户一起协作来选择要使用哪个软件。在全球比特币网络规则中试图赋予一个区域管理机构特殊权利是不切实际的。任何一个富有的组织可以选择投资挖矿硬件来控制整个网络中一半的计算能力，从而实现对最近交易的冻结和撤销。然而，他们无法保证能一直拥有这种能力，因为这一投资需要和全世界其他矿工的总和持平。

然而，用监管任何其它货币类似的方式监管比特币的使用是可能的。和美元一样，比特币可以用于各种用途，其中一些可以被视为合法的，或者并不是符合每个行政管辖区的法律。在这一点上，比特币无异于任何其他的工具或资源，会受制于每个国家不同的规定。在限制性的规定下，比特币的使用也会变得很艰难，这种情况下，很难确定将有多大比例的用户会继续使用该技术。选择禁止比特币的政府将会阻碍国内企业和市场的发展，将创新转移到其他国家。像

往常一样，监管机构所面临的挑战是在不损害新兴市场和企业的发展的同时，制定出有效的解决方案。

比特币和税收有何关系？

比特币不是法定货币，在任何行政管辖区都没有法定货币的地位，但无论使用的是什么介质，往往都要承担纳税义务。在许多不同的行政管辖区，对于由比特币产生的收入、销售所得、工资、资本收益、或一些其他形式的纳税义务都有各种各样的法律法规。

关于比特币和消费者保护

比特币使人们可以用他们自己的方式自由交易。每个用户都可以像使用现金一样付款和收款，同时也能参与更为复杂的合约。多重签名允许比特币网络只有在某个既定群体中同意为交易签名的成员达到一定数量时才接受该交易。这为将来发展创新的纠纷仲裁服务打下了基础。这一服务可以在双发无法达成一致的情况下允许对资金没有控制权的第三方来批准或者拒绝一笔交易。和现金以及其它支付方式不同的是，比特币总是会留有一份公开证据证明交易确实发生过，这可以被用来对存在欺诈行为的企业进行追索。

同样值得注意的是，商家通常依靠其公众口碑来维持经营并付工资给其员工，然而当他们反过来跟新顾客打交道时却无法得到这样信息。比特币的运作方式可以让个人和企业都免于欺诈性退单的危害，同时当顾客不愿意信任某个商家时可以让其选择要求更多的保护。

经济

比特币是怎样产生的？

新的比特币通过“挖矿”产生，“挖矿”是一个具有竞争力和去中心化的过程。这一过程包括个人为比特币网络服务，并因此得到回报。比特币的矿工使用专用的硬件处理交易和保护比特币网络，并在交易时收集新的比特币。

比特币协议的设计方式是以固定的速率发行新的比特币。这使得比特币的挖矿成为一个竞争极为激烈的行业。当越来越多的矿工加入比特币网络，赚取利润变得越来越难，矿工必须寻求效率以削减生产成本。任何中央管理机构或开发者都无权控制或操纵该系统以提高他们的利润。任何行为如不符合该系统要求遵循的规则，都将被全世界任何一个比特币节点所拒绝。

比特币以一个可预测的逐步下降的速率发行。新产生的比特币数量会逐年减半，直到比特币的总数达到 2100 万个。到那时，比特币矿工也许只能通过大量的小额交易费用来支持。

比特币为什么有价值？

比特币具有价值是因为它作为货币形式的一种是有用的。比特币具有货币的数学特性(持久性，可携带性，可互换性，稀缺性，可分割性和易识别性)而非依赖于物理特性(比如黄金和白银)或中央权力机构的信任(比如法定货币)。简而言之，比特币是由数学支持的。有了这些特性，一种货币形式要具有价值所需要的就是信任和使用。对比特币而言，这可以从它日益增长的用户，商家和初创企业基数上得到体现。同所有货币一样，比特币的价值直接来自于愿意接受它作为支付方式的人们，这也是唯一的来源。

比特币的价格由什么决定？

比特币的价格由供需决定。当对比特币的需求增加，比特币价格就上涨；需求减少，价格就下跌。目前只有很少的比特币在流通，新的比特币以一个可预见的逐步下降的速率发行，这表示需求必须遵循这一通胀水平才能保持价格的稳定。和它可能会成为的市场规模相比，比特币目前仍然是一个相对较小的市场，无需大量资金就能促使市场价格上下波动，因此，比特币的价格仍然很不稳定。比特币价格，2013 - 2015：

比特币会变得不值钱吗？

会。历史上有很多不成功而不再使用的货币，比如魏玛共和国时期的 德国马克以及更近的 津巴布韦元。虽然以前的货币失败通常是由于在比特币上不可能发生的超通货膨胀，但是总会有潜在的技术失误，竞争货币和政治问题等。基本的经验就是，没有一种货币可以被认为是绝对安全，不会出现失败或困难时期的。比特币自诞生起几年中被证明是可靠的，而且比特币继续成长的潜力很大。但是，没有人能够预测比特币的未来会怎样。

比特币是泡沫吗？

价格的快速上涨并不会构成泡沫。人为的高估将会导致一个突然向下的修正，才会构成泡沫。基于成千上万的市场参与者个体行为的选择导致比特币价格的波动是市场决定价格的结果。从情感上说，价格变动的原因包括：对比特币失去信心，不是基于比特币经济的基本面的价格和价值之间的巨大差异，越来越多的刺激投机性需求的新闻报道，对不确定性的恐惧，以及过时的非理性的繁荣和贪婪。

比特币是庞氏骗局吗？

庞氏骗局是一种诈骗性的投资运作，它是利用投资者自己的钱作为回报支付给投资者，或者利用新投资人的钱支付给老投资者，而非通过公司本身经营所赚

的钱作为回报。当没有足够的新投资人加入便导致庞氏骗局瓦解，最后的投资人便会蒙受损失。

比特币是一个无中央管理机构的自由软件项目，因此，没有人能够对投资回报做虚假的陈述。就像其他主要货币，如黄金、美元、欧元、日元等，比特币不能保证购买力并且汇率是自由浮动的。由此导致的波动性使得比特币持有者无法预测获利或损失。事实是，由于其有用的和有竞争力的特性，比特币正在为成千上万的用户和企业所使用。

比特币不会使早期使用者受益更多吗？

一些早期使用者拥有大量的比特币，因为他们在一个未经证实的技术上冒着风险投入了时间和资源，而当时该技术几乎还无人使用，也更难保证其安全性。在比特币变得有价值之前，许多早期的使用者经常消费大量的比特币，或者仅仅只买了少量的比特币，因此并没有获得巨大的收益。谁也不能保证比特币的价格将上涨或下跌。这非常像投资给一个早期的初创公司，可能会随着其实用性和普及获得价值，也也可能一直没有突破。比特币尚处于起步阶段，它的设计者眼光长远；很难想象它如何能够更少地偏向早期的使用者，今天的用户可能会是明天的早期使用者，也可能不是。

比特币的总量有限不会有局限性吗？

Bitcoin 的独特之处在于只有总量为 2100 万的比特币会被生成。但是这根本不会成为一种局限，因为交易中可以将比特币划分成更小的次级单位，比如 bit - 一比特币等于 1,000,000 bit。一个比特币可以拆分到小数点后 8 位（0.000 000 01），如果将来平均单笔交易规模减小到一定程度时，甚至可以拆分到更小的单位。

比特币不会陷入螺旋式的通货紧缩吗？

螺旋式通缩理论这么阐述，如果预计价格要下跌，为了从较低的价格中获利，人们将选择今后再购买。由此导致的需求减少反过来将使商家试图通过降低他们的价格刺激需求，从而使问题更糟，并导致经济萧条。

尽管该理论普遍地被中央银行家们用于解释通货膨胀，但它似乎并不总是有效，经济学家之间对该理论也有争议。消费类电子产品市场就是一个例子，商品价格不断下跌，但并没有导致萧条。同样地，比特币的价值不断在上升，同时比特币经济的规模也随之大幅增长。因为比特币的经济规模和货币价值都是从 2009 年由零开始，所以比特币是螺旋式通缩理论的一个反例，说明有时候该理论必然是错的。

尽管如此，比特币并没有设计成为一个通货紧缩的货币。更准确的说法是，比特币在其早期有通胀的趋势，在其后期变得稳定。只有当人们粗心地丢了钱包又没有备份时才会导致流通中的比特币数量减少。有了稳定的货币基础和稳定的经济，货币的价值应保持不变。

投机活动和价格的波动会成为比特币的一个问题吗？

这是一个鸡生蛋、蛋生鸡的问题。为了稳定比特币的价格，需要越来越多的企业和用户发展大规模的经济。为了发展大规模的经济，企业和用户将寻求价格的稳定性。

幸运的是，波动性不会影响比特币作为 A 到 B 点对点支付系统的主要优点。企业可以即时将比特币兑换成当地货币，使其既能得益于比特币的优势，又不会受到比特币价格波动影响。由于比特币提供了许多有用的独特功能和属性，很多用户选择了使用比特币。有了这样的解决方案和动因，随着将来比特币成熟和发展到一定程度，实现其价格的有限波动是完全可能的。

如果有人将现有的比特币全部买下将会怎样？

发行至今的比特币只有一小部分在交易市场上出售。比特币市场竞争激烈，意味着一个比特币的价格会根据供求关系上下浮动。另外，在未来几十年中新的比特币还会持续发行。所以即使是最决断的买家也不可能将现有的比特币全部买下。但是这种情况并不意味着这个市场对价格操纵是免疫的。要使比特币的市场价格上下变动并不需要投入非常大量的资金，因此到目前为止比特币依然属于一种波动性较大的资产。

如果有人创造了一个更好的数字货币将会怎样？

这有可能发生。但就目前来说，比特币仍是迄今为止最流行的去中心化虚拟货币，不过谁也不能保证它永远处于这一地位。现在已经有一些受到比特币启发的替代货币出现。然而一个较为合理的假设是，新型货币需要有重大的改进才可能在目前既定的市场上替代比特币，当然这些依然是不可预知的。在不改变协议基本组成的前提下，比特币或许也会采用一些竞争货币的改进措施。

交易

为什么我必须等待 10 分钟？

比特币几乎是即时接收付款的。然而，在网络开始将你的交易加入一个区块来确认该交易以及你可以使用接收到的比特币之前，有一个平均 10 分钟的延迟。确认的意思是在网络上达成了一个共识，即你收到的比特币没有用来支付给别人因此被认定是你的财产。一旦你的交易被包含进一个区块，则之后的所有区块都会包含它，这将极大地巩固这个共识并减小交易撤销的风险。每一个用户

都可以自行判断交易被确认的时间点，但通常来说，收到 6 个确认就如同在信用卡交易后等待 6 个月那样安全。

交易手续费是多少？

大多数交易都可以不花手续费，但我们鼓励用户自愿支付一笔小额费用来加快交易确认以及酬谢矿工。当需要手续费时，通常不会超过几分钱的价值。您的比特币客户端通常会在需要时估算出适当的费用。

交易手续费能对过多交易导致的网络超载起到保护作用。具体的收费方案还在发展中并将随着时间的推移而改变。因为手续费用与交易金额无关，所以它可能有时候看上去非常低（0.0005BTC 相对于一笔 1000BTC 的转账 ），有时候高的离谱（0.004BTC 相对于一笔 0.02BTC 的支付）。手续费的高低是由交易数据的大小和交易次数等因素决定的。比如说，如果你接收了一大批小额的款项，那么其支付的费用就会高些。这种支付就好比用一分钱硬币来付餐厅帐单。小额比特币的快速消费可能也会产生手续费。如果你的活动符合常规交易的特征，则手续费应该会很低。

如果我的电脑关机时接收到比特币会怎样？

这没有关系。比特币会在你下次打开钱包程序的时候出现在你的帐户里。事实上比特币并不是由你电脑上的软件来接收，它们是被添加到一个由网络中所有设备共享的公共总帐户中。如果你在你的客户端没有运行的时候收到比特币，当事后再打开客户端的时候，它会下载区块并更新任何尚未记下的交易，而那些比特币最终会出现在钱包中，就像是实时收到的一样。只有在你想花比特币的时候才需要用到你的钱包。

"同步"是什么意思？为什么同步要花很长时间？

只有像 Bitcoin Core 这样的完全节点型客户端才需要较长的同步时间。从技术上来说，同步是一个下载并核实网络上所有以往比特币交易的过程。某些比特币客户端需要知道所有以往的交易才能计算你比特币钱包的可用余额并完成新的交易。这一步骤非常消耗资源，需要有足够的带宽以及能存放整个块链的空间。为了保持比特币的安全性，需要有足够的用户使用完全节点型客户端，因为他们起着确认和中继交易的作用。

挖矿

什么是比特币挖矿？

挖矿是消耗计算资源来处理交易，确保网络安全以及保持网络中每个人的信息同步的过程。它可以理解为是比特币的数据中心，区别在于其完全去中心化的设计，矿工在世界各国进行操作，没有人可以对网络具有控制权。这个过程因

为同淘金类似而被称为“挖矿”，因为它也是一种用于发行新比特币的临时机制。然而，与淘金不同的是，比特币挖矿对那些确保安全支付网络运行的服务提供奖励。在最后一个比特币发行之后，挖矿仍然是必须的。

比特币的挖矿的原理是什么？

任何人均可以在专门的硬件上运行软件而成为比特币矿工。挖矿软件通过 P2P 网络监听交易广播，执行恰当的任务以处理并确认这些交易。比特币矿工完成这些工作能赚取用户支付的用于加速交易处理的交易手续费以及按固定公式增发的比特币。

新的交易需要被包含在一个具有数学工作量证明的区块中才能被确认。这种证明很难生成因为它只能通过每秒尝试数十亿次的计算来产生。矿工们需要在他们的区块被接受并拿到奖励前运行这些计算。随着更多的人开始挖矿，寻找有效区块的难度就会由网络自动增加以确保找到区块的平均时间保持在 10 分钟。因此，挖矿的竞争非常激烈，没有一个个体矿工能够控制块链里所包含的内容。工作量证明还被设计成必须依赖以往的区块，这样便强制了块链的时间顺序。这种设计使得撤销以往的交易变得极其困难，因为需要重新计算所有后续区块的工作量证明。当两个区块同时被找到，矿工会处理接收到的第一个区块，一旦找到下一个区块便将其转至最长的块链。这样就确保采矿过程维持一个基于处理能力的全局一致性。

比特币矿工既不能通过作弊增加自己的报酬，也不能处理那些破坏比特币网络的欺诈交易，因为所有的比特币节点都会拒绝含有违反比特币协议规则的无效数据的区块。因此，即使不是所有比特币矿工都可以信任，比特币网络仍然是安全的。

挖矿不是一种能源浪费吗？

为了保护和运行一个支付系统而消耗能源并不是一种浪费。和其它任何支付服务一样，使用比特币会产生处理成本。运行目前流行的金融系统必需的服务，比如银行，信用卡和运钞车，也消耗大量能源，虽然它们消耗的能源总量不像比特币那样是透明，也不易度量。

比特币挖矿原理的设计使其可以通过使用专门的硬件随着时间推移优化挖矿过程，从而消耗较少的能源。而挖矿的运行成本依然与需求成正比。当比特币挖矿竞争变得过于激烈且收益减少时，一些矿工会选择停止活动。此外，所有挖矿消耗的能源最终都转化为热能，而利润最多的矿工正是那些可以很好利用热能的人。一个最优的高效挖矿网络不会消耗任何额外能源。尽管这是一种理想情况，挖矿的经济原则就是个体矿工都朝着这一理想状况而努力。

如何通过挖矿帮助保护比特币的安全？

挖矿创造了一种等同于彩票的竞争机制，向块链连续添加新的交易区块对任何人来说都是非常困难的。这一机制可以防止任何个体获得能够冻结某些交易的能力，从而确保了网络的中立性。这一机制也可以防止任何个体替换一部分块链来降低他们自己的花费，否则这种做法可以被用来欺诈其他用户。挖矿机制使得撤销一个以往的交易变得极其困难，因为这需要重写该交易之后的所有区块。

开始挖矿前，我需要些什么？

在比特币的早期，任何人都可以利用他们计算机的中央处理器寻找新的区块。随着越来越多的人开始挖矿，寻找新区块的难度大幅提高，以至于目前唯一有成本效益的方法就是使用专门的硬件。你可以访问 BitcoinMining.com 获得更多信息。

安全性

比特币安全吗？

比特币技术，包括协议和密码学，有着强大的安全性记录，并且比特币网络也许是世界上最大的分布式计算工程。比特币最常见的薄弱环节是用户失误。存储私钥的比特币钱包文件可能会意外地被删除，丢失或盗取。这跟用电子形式存储的实体现金非常相似。幸运的是，用户可以利用可靠的安全性策略来保护他们的资金，也可以使用提供良好安全性等级以及偷盗或遗失保险服务的供应商。

比特币在过去被黑客攻击过吗？

比特币使用的协议和密码学规则在问世多年后仍行之有效，这是个好的现象，说明这个概念的设计非常好。但是，在各种软件的执行过程中，也发现了安全漏洞并予以修正。和其它形式的软件一样，比特币软件的安全性取决于发现并修正问题的速度。类似的问题发现越多，比特币就越趋于成熟。

对于在不同的交易平台和业务中发生的窃取和安全漏洞，经常会存在误解。虽然这些是不幸的事件，但是它们并不代表比特币被黑客攻击，也不代表比特币内部存在缺陷，正如银行抢劫并不会危害到货币本身一样。但是准确地说确实需要一整套良好的策略和直观的安全性解决方案来使用户更好地保护他们的资金，降低盗取和遗失的一般风险。在过去几年中，这样的安全功能快速发展，例如钱包加密，离线钱包和多重签名交易。

用户是否可以联合起来攻击比特币？

轻易改变比特币协议是不可能的。任何不符合协议的比特币客户端都无法强制其他用户遵守它自己的规则。就目前的规则来说，在同一个块链上双重消费是不可能的，没有合法签名的比特币消费也一样。因此，凭空产生大量比特币，使用其他用户的资金，腐败整个网络以及类似的情况都是不可能发生的。

但是，多数的矿工可能会任意地选择去冻结或撤销最近的交易，多数的用户也可能为了对协议做出一些修改而施加压力。因为比特币只有在所有用户都完全达成共识时才能正常运作，所以修改协议是非常困难的，需要压倒性的多数用户去采用这些改动以至于剩下的用户除了跟随没有其他选择。一般来说，很难想象一个比特币用户为什么会选择采用任何可能会危害到他资金的协议改动。

量子计算是对比特币的威胁吗？

是的，包括传统银行系统在内的大部分依赖于密码学的系统都是这样。但是量子计算机还不存在，也许短期内也不会出现。当量子计算确实即将成为比特币威胁的时候，可以利用后量子算法来更新比特币协议。基于这一更新的重要性，有理由相信开发人员会将其反复审核，最终为所有比特币用户接受。