比特币那些你可能存在的疑惑

课程组成员：擒龙、吴六木、小玛、Mingo、今日无限、中笨聪、一木先生、静心、OWEN、蓝海、蔚蓝、文辉

- **什么是比特币？**

比特币是数字货币的一种，用于在比特币网络上面进行流通和激励维护系统正常运行的，代替实物货币的一种代币。

- **什么是比特币网络？**

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？**

比特币的发展史有很多发明人成果的迭代。中本聪 2008 发表的学术论文，引入了比特币，比特币的发展史有很多发明人成果的迭代。但中本聪的身世至今为止仍然是个谜。可能是一个人或者一个组织的代号。

- **比特币网络是不是被人控制？**

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？**

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。使用“send”功能，该功能允许与 ECDC（或智能合约）进行直接交易和交换

- **如何获得比特币？**

在比特币系统当中获取比特币的方式有三种，两个身份。矿工身份：提供算力参与比特币系统的运行支撑。获得比特币方式（1）处理交易获取的手续费；（2）进行挖矿，党获得记账权力的时候，系统给的奖励。（比手续费高得多）。用户身份：在交易所或者私下买入以及支付比特币。

- **用比特币如何进行支付？**

只需要有相应的客户端（或者钱包），将对方的交易地址在交易当中填好，填上转账金额和手续费，注意一定要写上手续费。这样就可以实现跨域转账，方便易操作。

- **比特币的优缺点是什么？**

优点：支付自由、极低的费用、降低商家的风险、安全和控制、透明和中立；

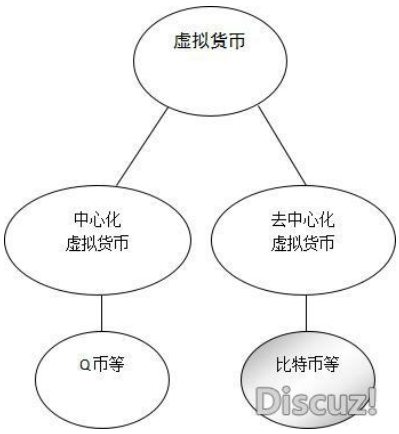
缺点：接受程度有待提高，国家控制严格、波动性高、处于发展阶段。

- **为什么人们相信比特币？**

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。

- **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。

- **比特币合法吗？**

各国的政策不同，对待比特币的看法也不同。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。

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。

● 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。

- **比特币和传销币、庞氏骗局一样吗，回事泡沫吗？**

首先，先了解清楚什么是庞氏骗局。庞氏骗局是非法式的层压式推销，是一种诈骗性的投资运作，也就是“拆东墙补西墙”、“空手套白狼”。这种骗术是查尔斯·旁兹 “发明”的。其运作模式就是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。庞氏骗局最重要的特点就是，先来者主要依靠后来者的加入才能赚到钱，最后的投资者就是击鼓传花的“接盘侠”。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。

对于比特币，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。从来没有人承诺比特币一定会有收益，而且随着数年的价格波动，早投入也不一定获得收益，晚投入也不一定亏损判断一个东西是否有价值，主要是根据一个东西没有提高效率。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。比特币在跨境全球转移资产、购买实物等方面是增加交易，创造财富的。

庞氏骗局、传销也好，最开始只产生了需求，有需求就会有价格，但是没有提高效率，最终的实际需求也是为 0，所以最终的结果也是归 0。所以比特币和传销是截然不同的东西。

- **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。早期参与者同样也承担着相应多的风险。

- **比特币的总量有限不会有局限性吗？开采完了 BTC 是不是完蛋了？**

比特币挖矿挖的实质是获得记账权，就相当于大家一起工作来记录工作情况，按一定概率由人来记，但是不能让你白劳动，系统会给予一部分钱（BTC）作为奖励回馈，有回报大家都想做这件事，那就竞争，系统为了保证公平，按大家的算力 占系统总算力的概率来让大家去竞争挖矿权。

比特币的总量是 2100 万个，准确的说是 20999999.97690000 个，比 2100 万少一点，预计 2140 年能开采完。格林威治时间 2012 年 11 月 28 日 15:24:38，编号第 210000 个区块产生。从这个区块起的”阶段 2”，每个区块包含的新比特币数量减半为 25 个，这是历史上第一次减半。今后每产生 210000 个区块，比特币数量都会依次减半。直到第 33 次减半时，每个块产生 0.0021 个新比特币直接减为 0 个。

比特币开采完了是不是比特币系统完蛋了？那是不可能的，维持系统的激励机制包括两部分：挖矿费用+交易手续费，当比特币被挖取完了，这里提供两种个人见解思路：

（1）调整手续费比例，以继续保持激励机制的维护；

（2）开发分叉币，增强系统币的流通量，各种数字货币在交易所上都有固定的价值，也相当远人民币不同的面值，间接增加发行量。

- **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。

- **什么是比特币节点和区块链节点？**

（1）比特币节点

比特币是一种点对点的电子现金系统，更直接地说，是节点对节点。每笔交易由发起方向周围的节点进行广播，节点收到之后再广播给自己周围的节点，最终扩散至全网。**每一个比特币钱包都是一个节点，其中拥有完整区块链账本的节点叫做全节点。**2017 年 10 月，比特币全网约有 9300 个全节点，负责比特币转账交易的广播和验证。转账交易发生后，由所有节点共同广播至全网，挖矿的节点验证该交易正确后会记录至区块链账本。美国、德国、法国拥有的比特币全节点数最多，中国的全节点数量约占全球 5%（数据来源于：bitnodes.21.co）。由于运行比特币节点不提供任何奖励，且不需要全节点也可以进行比特币转账，所以比特币的全节点数只占节点数的一小部分。

（2）区块链节点

在最初的区块链网络设计中，不存在任何中心化的特殊节点和层级结构，每个节点完全对等，承担着**网络路由、验证交易信息、传播交易信息、发现新节点等工作。**但是实际上物理设备是存在明显性能差距的，以比特币网络为例，可作为节点的设备有个人计算机、服务器、专为比特币挖矿设计的矿机，以及移动端，它们提供的算力相差了几个数量级，并且存储空间也不同。目前市面上可见的移动端存储空间最大不过 100 GB 左右，而存有全部数据的区块链数据总量已经超过 60 GB，想要将移动端作为全节点无疑是不现实的。于是有了全节点和轻型节点，全节点是传统意义上的区块链节点，包含有完整的区块链数据，支持全部区块链节点的功能。全节点通常是高性能的计算设备，比特币刚面世时依靠 CPU 来提供算力，后来使用 GPU，发展到现在是专门设计将 SHA256 算法固化到硬件的矿机，算力成几何增长趋势。轻型节点是依靠全节点存在的节点，不用为区块链网络提供算力，只保存区块链的区块头，由于区块头包含了 Merkle 根，可以对交易进行验证。轻型节点多为移动端，如智能手机、平板电脑、移动计算机等。

- **什么是交易和交易单？**

① 交易：Tx，发生的一笔转账，eg：A 付给 B 2BTC。交易包括两部分：买卖交易和本地数据库上链存储。

② 交易单：记录交易的数据。

交易组成：

1) prevTxHash：前一 Tx 的 Hash 值；

2) index：前一 Tx 的输出值；

3) scriptSig：前一支付者的签字 ECDSA(the elliptic curve digital signature algorithm)；

4) value：面值；

5) scriptPubKey：收款者的地址，A 的 Bitcoin 地址=RIPEMD-160(SHA256(PubkeyA))；

6) txHash：此 Tx 的 Hash 值。

- **为什么一个区块当中存储的交易总数固定？**

（1） 最简单的交易单（一个输入、一个输出），存储大小：166bytes；

（2） 处理速度：10tps。tps(transactions per second)

- **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。

- **交易手续费是什么？**

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。

- **转账是不设置手续费，会发生什么情况？**

转账的时候不设置手续费的话，或者说手续费达不到该转账平台的最低要求标准的时候，该交易会无效的。而且如果设置的比特币交易费用过低的时候，交易也会被很晚处理。矿工处理交易的标准是：手续费和交易单存在的时间。所以特别是对于紧急交易的时候，好事多设置点交易费用。

- **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？**

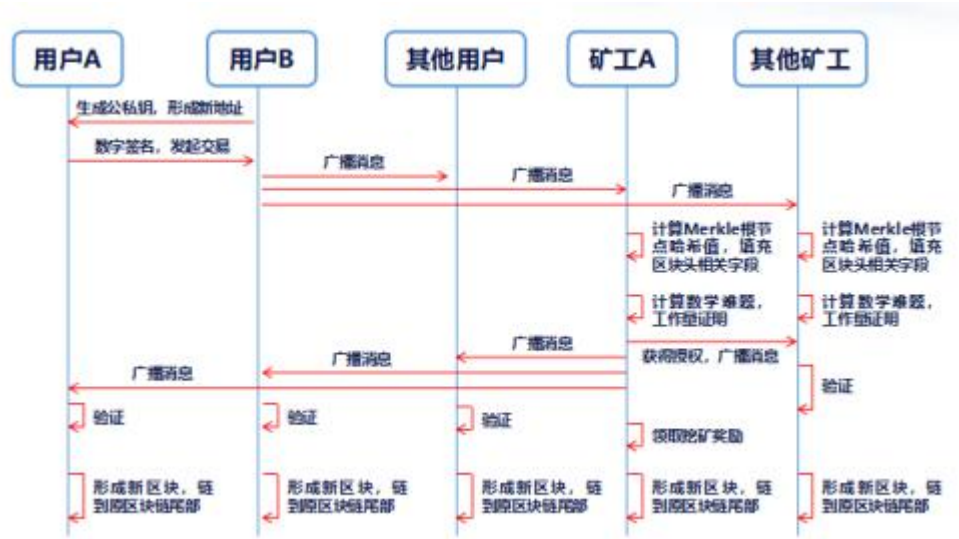
只有像 Bitcoin Core 这样的完全节点型客户端才需要较长的同步时间。从技术上来说，同步是一个下载并核实网络上所有以往比特币交易的过程。某些比特币客户端需要知道所有以往的交易才能计算你比特币钱包的可用余额并完成新的交易。这一步骤非常消耗资源，需

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。

- 什么是比特币挖矿？

中本聪提出了 chain of block，区块链名词不是他最先这样称呼的。区块链相当于盖楼，上一个区块的 hash，若之间发生一个比特的变化就会发生“雪崩效应”。用户先发起交易，用私钥加密，然后节点对其进行验证合法性。若合法，则打包到块里面。一个块什么时候可以开始争夺记账权。可以有两个参数进行决定：**时间间隔和交易的数量。有时候等了半天交易量很少可以采用时间间隔来确定一个块，有时候交易量太大了可以采用交易量来确定为一个块。**只要服务器运行协议，这个服务器对应的就相当于一个节点，然后矿工（**愿意贡献算力**）上面的节点进行争夺记账权，节点可以随时加入和退出。**只有矿工挖到了块并且广播出去，经过确认验证之后，才算挖到块，给予奖励，之后的块在这个块的基础上进行继续挖。**只不过在争夺记账权的时候系统会动态设置难度（**比如要求哈希结果 256 位当中前 20 位为 0，动态增加难度可以让前 21 位为 0**），广播并通过共识机制达成共识。比特币效率慢的原因是每次记账都要达成共识，比较繁琐，消耗了大量的电力等能源，所以有些人认为这是一种浪费。也导致对于 POW 机制，想要发生 51%的是多么困难的事情。有人会说可以使用银河超算，其实那样的算力还不及现在算力的 1%。比特币现在的分配机制中挖矿奖励在逐渐减少，但是手续费在增加（虽然目前手续费不是那么夸张）。以后当没有新的币产生时，就会依赖于手续费。

- 比特币的挖矿的原理是什么？



① 节点监听全网交易，通过验证的交易进入节点的内存池，并更新交易数据的 Merkle Hash 值。

② 更新时间戳。

③ 尝试不同的随机数（Nonce），进行 hash 计算。

④ 重复该过程至找到合理的 hash。

⑤ 打包区块：先装入区块 meta 信息，然后是交易数据。

⑥ 对外部广播新的区块。

⑦ 其他节点验证通过后，链接至区块链，主链高度加一，然后切换至新区块后面挖矿。

随机数什么时候满足？

SHA256（SHA256（版本号+前一区块哈希值+Merkle 根哈希+时间戳+难度值+随机数））≤ 目标值

- **挖矿不是一种能源浪费吗？**

这是维护一套系统的必要，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。现在银行的金库，安保，柜台租金，银行从业人员薪资，交易系统，不需要支出吗？维护一套现金系统运转从来都不是免费的。

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。

- **挖到区块之后为什么需要 6 个块的验证？**

① **双花**：双重支付，一笔钱花了两次

② **6 个块的验证**：目的是解决双花问题

（1）具体证明过程：

- p：诚实节点找到下一块的概率；
- q：攻击者找到下一块的概率；
- z：诚实者建立的链和攻击者建立的链长度之差，诚实节点找到下一块时加 1，攻击者找到下一块时减 1；
- z=-1：攻击者超过诚实者，成功地重复支付；
- qz：攻击者从落后于 z 块起，追上诚实者的概率。

$$z_{i+1}=\begin{cases} z_i+1, & \text{以概率}p; \\ z_i-1, & \text{以概率}q. \end{cases}$$

$$q_z=\begin{cases} 1, & \text{如果}z<0\text{或}q>p; \\ (q/p)^z, & \text{如果}z\geq 0\text{或}q\leq p. \end{cases}$$

根据拇指原理 z=6 时稳定。（拇指原理：由经验得出）

（2）q 的大小的影响

由全概率公式得差分方程：$q_z = pq_{z+1} + qq_{z-1}$

初始条件：$q_0 = 1, q_a = 0$

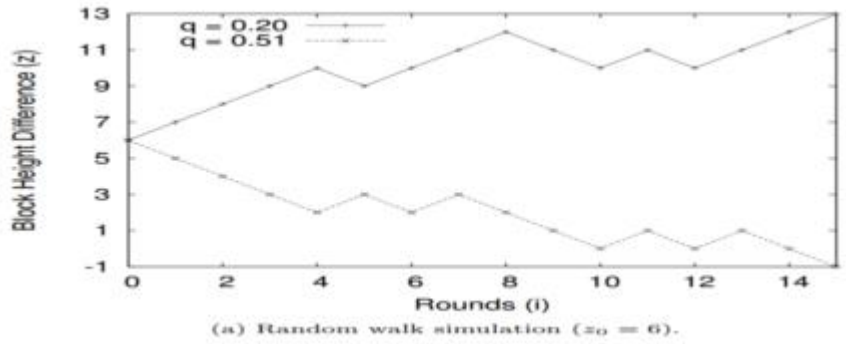
其中 a 是诚实者超过攻击者最大的步数

$$q_z = \frac{(q/p)^a - (q/p)^z}{(q/p)^a - 1}$$

$a \to \infty$ 得：$q_z = \begin{cases} 1, & \text{如果} z < 0 \text{或} q > p \\ (q/p)^z, & \text{如果} z \geq 0 \text{或} q \leq p \end{cases}$

所以可以发现，q 越大，块的步数越大，导致攻击成功的可能性越大。

（3）q=0.2 和 q=0.51 的对比



(a) Random walk simulation ($z_0 = 6$).

可发现当 q=0.51 的时候，在 14 块的时候可以完全追上诚实节点。

- **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。最主要的是他的共识机制是 POW 共识机制，需要达到全网 51%的总算里才可以进行攻击，这个成本很高，很难达到。但是不代表没有可能行，比如说现在几个大的矿池之间能否联合攻击呢？

- **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。

由于比特币系统还在初期阶段，在 2010 年 8 月 15 日的那天，在比特币系统中，比特币被错误验证的漏洞发现和利用，导致产生了 1,840 亿比特币。

- **量子计算是什么？对比特币的威胁吗？**

量子计算是对传统计算的革命，当前已经从实验室初步走向商业化应用。量子计算与传统计算的最大区别在于：

① 传统计算机采用二进制比特，即“0”和“1”；

② **量子计算采用量子比特（qubit）作为最小的运算单元。**

而量子比特可同时存在两种可能的状态，这种新状态被称作“叠加态”。因此，对量子比特的操作可以让许多计算工作并行进行。**目前计算机领域所谓的并行计算只是从效果上来看形成问题的并行解决，实际从 CPU 的运行来看，CPU 依旧是一次只能处理一个计算。**量子计算将会是真正意义上的并行计算，计算速度大大提升，对 1000 位的大数进行因数分解只需要几秒，而传统的计算机则需要 1025 年。目前量子计算已经从实验室初步走向商业化应用。量子计算已成为 IBM、微软和谷歌等信息产业巨头竞相逐鹿的战场。由于量子位在普通环境下难以制备，并且多量子位之间的协调控制较难，因此目前的量子计算机量子位数较少，导致量子计算机只能处理特定的问题，通用性差。此外量子计算机的制造维护成本特别高。量子计算机的成熟和大规模应用还需要突破很多技术瓶颈。

威胁导致的改变：

① **挖矿竞争的格局会改变。**拥有量子计算能力的挖矿速度较传统的二次加速，即利用 Grover 算法暴力搜索 hash 码。但区块链不一定基于 pow 的机制，因此该影响在未来未必存在。

② **基于大数分解的密钥方案将被 shor 算法破解，让区块链失去保密性。**解决的方案是引入其它用量子算法无法破解的密钥机制。

- **量子计算机出来，是不是区块链不能玩了？**

① 目前量子计算机距离成熟至少还有 5 年以上的时间，大概率 10 年以上.

② 量子计算机成熟之后，对以密码学为基础的各种领域都会带来巨大的冲击，区块链只是其中很小的一块。

③ 对比特币的冲击会特别大，因为是基于 POW 的模式。

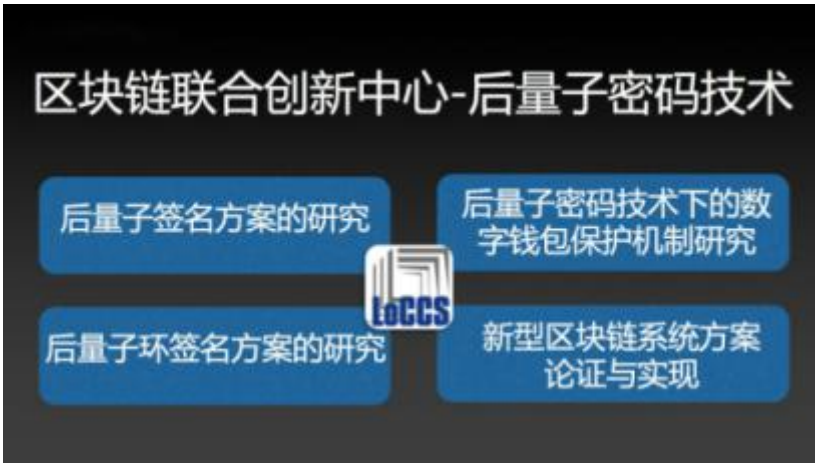
④ 区块链的技术，会随着量子计算机的发展，而继续发展。不用过于担心量子计算机直接把区块链干掉了。

⑤ 区块链最有价值的地方还是价值传递和改造生产关系，这一定会对整个商业社会造成巨大的影响。

- **后量子密码学的研究有哪些？**

设计“新型抗量子公钥密码”的队伍现在必须和那些研发量子计算机的队伍赛跑。

要知道，阔悦科技与上海交大还在对区块链联合创新中心的后量子密码技术在后量子签名方案、后量子密码技术下的数字钱包保护机制、后量子环签名方案，以及新型区块链系统方案论证与实现等四个方面进行研究。



Evgeny Kiktenko 团队的论文分别提出了两种解决方法。第一种是在加密过程中在哈希算法加持量子签名（post-quantum digital signature schemes），不过具体细节没有透露。第二种，在信息对比过程中，采用一种叫做量子秘钥分布（Quantum Key Distribution）的方式来验证每位参与者的身份。

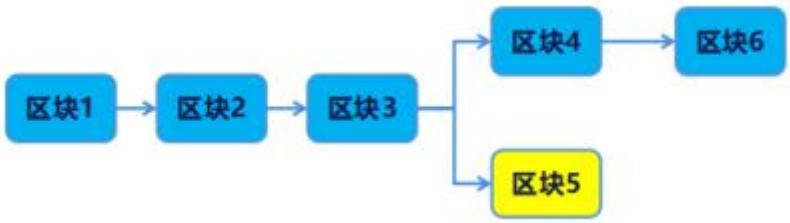
- BTC 的分叉币是什么？怎么分叉的？

比特金（BCH），于 2017 年 8 月 1 日硬分叉产生，比特币的首个分叉币，也是比特币当今频繁分叉的导火线，BCH 支持 8M 大区快，区块大不需要 Segwit，BCH 挖矿算法和矿机与 BTC 一样，但 BCH 挖矿难度调整机制 EDA 不稳定，导致挖矿难度在某时段会暴增 3 倍，所以

BCH 预计在 2018 年 11 月 3 日进行硬分叉升级，加入 DAA 挖矿难度调整机制。到现在为止 BTC 的分叉币越来越多，包括：BCH、BTG、B2X、BCD、SBTC、BCHC 等，根本不会管 BTC 是否愿意。

- **什么是硬分叉和软分叉?**

区块链的分叉问题是指某一节点若收到多个针对同一前续区块的后续临时区块，则该节点会在本地区块链上建立分支，多个临时区块对应多个分支。僵局的打破要等到下一个工作量证明被发现。



会默认选择高度最高的分叉链作为主链，每一个区块代表高度为 1。分叉包括，硬分叉和软分叉两种。

① **硬分叉：**指比特币区块格式或交易格式（这就是广泛流传的“共识”）发生改变时，未升级的节点拒绝验证已经升级的节点生产出的区块，不过已经升级的节点可以验证未升级节点生产出的区块，然后大家各自延续自己认为正确的链，所以分成两条链。

② **软分叉：**指比特币交易的数据结构（这就是被广泛流传的“共识”）发生改变时，未升级的节点可以验证已经升级的节点生产出的区块，而且已经升级的节点也可以验证未升级的节点生产出的区块。

- **图灵完备指什么？BTC 系统具备吗？**

在可计算性理论里，如果一系列操作数据的规则（如指令集、编程语言、细胞自动机）可以用来模拟单带图灵机，那么它是图灵完备的。这个词源于引入图灵机概念的数学家艾伦·图灵。作为计算机的理论模型，图灵机是英国数学家 Alan Turing 于 1963 年提出的、为了研究可计算问题而构思的抽象计算模型，可以看作等价于任何有限逻辑数学过程的终极逻辑机器。

简单来说，图灵机由控制器、可无限延伸的纸带及在带子上左右移动的读写头组成；运行过程中，读写头从当前纸带上读取信息，并通过内部固定程序输出回纸带，同时转换自己内部状态在纸带上移动。这个概念简单的机器，理论上可执行任何直观可算函数。

如果一门编程语言、一个指令集可实现图灵机模型里面全部的功能，或者说能够满足任意数据按照一定顺序计算出结果；我们就可称其具有图灵完备性。而上一问提到的以太坊就是一个图灵完备的区块链系统，其虚拟机可运行智能合约，理论上能够解决所有的可计算问题，从而尽最大限度满足各种现实应用场景的开发。

图灵完备的通用性，保证的是计算的可行性，不保证计算的效率及代码的可理解性、可维护性；所以它不一定能满足某些领域的特定需求。当需求之间存在冲突时，语言开发者须进行取舍并作出优化设计，从而降低解决问题的复杂度。虽然图灵机会受到储存能力的物理限制，但图灵完全性却通常指“具有无限存储能力的通用物理机器或编程语言”。

- **什么是双花？bitcoin 中如何解决双花问题？传统货币中存在吗？**

双花就是一笔钱化两次，双花分为两种：在这笔钱使用之前之前双花和在这笔前使用之后双花（这个是需要满足 51%算力才可以进行）；

BTC 系统如何解决双花问题？首先看看这笔交易的来源是否来自 UTXO（为话费交易列表），然后看看提交的交易有没有有效签名，如果同一个 UTXO 构造了两笔交易，那么矿工会处理时间早的那笔，另外一笔交易被视为无效。当这两笔相矛盾的交易中的一笔被写入区块链，并且深度达到 6 后（6 个确认后），可以认为这笔交易获得了最终的确认。等待 6 个确认的情况下，比特币是几乎绝对不可能被双花的。一个确认都不等待，则有相当的可能被双花攻击。通常，3 个确认已经相当安全。

注意：同一个 UTXO 构造了两笔交易，一般矿工可以优先选择交易费用高的那笔，因为自己赚的多，当交易费用一样的时候，一般矿工选择先看见的那笔交易。

一般存在验证延迟的系统，按道理来说都会存在双花问题。就看如何避免了。

- **比特币点对点交换是一个地址的比特币交换给另一个地址的比特币？**

比特币都在你的钱包里面，一个钱包可以产生多个私钥，每个私钥对应一个地址，所谓交换相当于买卖商品 A 花钱买 B 的商品，A 从自己的钱包当中生成发送地址，把比特币发给 B 的地址（接受地址）当中，到 B 的钱包当中。但是这个过程当中的花费包括两部分。第一部分是你买东西的钱，第二部分是你完成这笔交易需要花费的钱，都是由买家 A 提供的，钱到哪里去了？买东西的钱给了卖家 B，交易费用给了处理这笔交易的矿工节点。

- **比特币和黄金有什么相似处吗？**

比特币和黄金有很多相似的地方。

（1）稀缺性：他们都是舒徐稀缺品，价格昂贵；

（2）总量有限：比特币总量是 2100 万个，黄金在地球上的资源也是有限的；

（3）需要挖矿开采：比特币是矿工挖矿，黄金是采矿人员开采；

（4）均具备流通性：都在市场上流通，并且被认可；

（5）货币特性：具备数字货币的几个属性和流通属性；

课程组多外合作联系人：紫瑶若水

参加课程组协作联系人：蔚蓝