如何理解比特币的膨胀和分叉，什么是硬分叉和软分叉！

每块比特币的大小为1M，可容纳1000多条交易信息。如果你在最后一个比特币区块浏览器上看的话，你会发现大概有100M&#039；s，这已经达到了块容量的上限。如果比特币网络上的转账越来越多，很多交易都不会在交易后的第一块打包确认，可能需要几块甚至更多。

比特币在历史上经历过几次“粉尘攻击”。所谓的&quot灰尘攻击&quot，也就是说有人制造了大量小额转账，使得网络中大量交易需要确认，导致无法确认正常的比特币转账，延误了确认时间，影响了网络的正常运行。

在&quot灰尘攻击&quot许多交易员等待了两天或更长时间才得到确认。一个非常极端的例子&quot灰尘攻击&quot，但是纵观现在的比特币网络，正常的转账金额已经远远超过了他们的最大容量。每个区块的大小现在是1M，从而扩大了现有的比特币容量。突破现有1M的过程叫做扩容。

从2014年开始，比特币社区被提上日程。我们知道比特币网络是一个去中心化的网络，世界上没有一个中心化的组织来运作。一切都要靠社会各界协商达成一致。。不同团队对扩张的想法不一样，所以推广效率比较低。

2015年底，比特币核心开发团队和矿工在香港召开圆桌会议。当时在香港达成共识，但很快流产。2017年纽约比特币社区通过隔离见证和2M扩张的方式重新谈判并再次达成共识，我们称之为纽约共识。共识达成当天，全球21个国家的56家知名区块链创业公司联合签名，并得到全网约83%计算能力的支持。因此比特币系统从2017年上半年开始升级部署。

其实比特币扩容的方案有很多，历史上也有过多次迭代。一般来说有两种方式：一种是使用闪电网络结算比特币，不接触比特币本身的区块。把大量交易放在比特币本身的网络之外；另一种是直接扩大比特币块的大小。这里解释一下闪电网是什么，比如几个朋友一起打牌，不是每轮结算，而是最后结算。甲欠元，乙欠C20元，最后丙给元。b给C10元就行。闪电会先记录大量的小额转账再进行结算，这样比特币网络就不会被大量的小额转账交易占用。但技术成熟，需要在隔离见证的基础上应用雷电网，还没有大规模应用。所以网友关注的是比特币区块本身的扩容。

比特币区块扩容本身就是一种比较成熟的技术方法。主要有三种扩展方案：BIP141、UASF和Segwit2x。

BIP141是比特币核心团队提出的隔离见证方案。隔离见证旨在使块承载更多事务。我们知道，区块上的信息分为交易信息和见证信息。，交易信息是块上记录的转账；见证信息是验证交易信息可靠性的节点和时间。中本聪在设计比特币的时候直接把这两条信息放在了区块里，所以一个区块可以承载的交易信息很少。如果从块中取出见证信息，块只记录交易信息，也可以从这个角度扩展块可以承载的交易信息。

BIP141目前被认为是一种隔离见证激活方案。激活条件是2017年11月15日任何困难时期的两周左右。。如果95%的计算能力发出准备就绪的信号，隔离见证将被激活。但是这种情况很难实现，所以有人提出了其他的激活方案。UASF或Segwit2x实现了这种隔离见证来帮助BIP141激活。

UASF字面意思是用户激活软叉。UASF使用一种叫做BIP的软件。2017年8月1日，比特币BIP148软件将拒绝包含一个Bit1信号块，即如果大部分矿工操作该软件，他们会拒绝一些没有操作该软件的矿工挖掘出的石块。因此，这些矿工将具有最长的链，并在最长的链上激活他们的BIP隔离见证141。最后，BIP链中超过95%的节点将被视为包含触发隔离见证的Bit1信号。。该计划已经实施，但现在我们看到了一种新的区块链资产——比特币现金。比特币现金的块大小可能会上升到8M，可以容纳的交易量是原来比特币链条的8倍左右。

Segwit2x有一些比特币公司和矿工有80%的计算能力。共识会议上签署的纽约共识协议通过BIP91激活隔离见证。。BIP91的做法是连续两天支持80%的计算能力。所有91个信号BIP91节点将拒绝所有被排除的节点BIP141以准备信号块。因此，这些矿工将拥有最长的链，并激活最长链上的隔离见证。。在2017年底或2018年初激活隔离见证后，Segwit2x块上的大小上限将通过硬分叉从1M增加到2M。这也可能导致新的分歧。

什么是硬分叉，什么是软分叉？

硬分叉是指当比特币协议发生变化时，如果旧节点拒绝接受新节点创建的区块，那么该区块将被分成两个独立的链，矿工需要在两个区块链中选择一个进行挖掘。

当比特币协议规则发生变化时，老节点赢了&#039；我没有意识到规则是不同的。它们将遵循更改后的规则，并接受新节点创建的块。因此，软分叉不会产生两个区块链，而是在原有链条的基础上新旧并存。类似于软件升级你在2003年保存了一个word，在2011年用2003文档word打开了原来的Word文本2003，这就是向前兼容。

对于普通人来说，如果比特币真的分叉，最大的风险就是&quot重放攻击&quot。

。什么是&quot重放攻击&quot？这个事件可以追溯到2016年7月以太坊硬分叉时发生的事情。当时教育平台和用户基本都是第一次遇到这种事情，缺乏经验和准备，所以损失很大。例如比特币分为一个或多个比特币，我们称之为比特币1、比特币2、比特币3。用户中有三个对应的比特币&#039；的账户。每条链都有相同的地址和私钥算法，交易格式也完全一样，这就使得一条链在另一条链上交易完全合法成为可能。因此，用户在一个链上，可以在另一个链上，或者可以确认这是一个&quot重放攻击&quot。简单来说，当你转移比特币1的时候，你的比特币2和比特币3也可能同时被转移。如果你转移的地址不是你自己的那么那些比特币2和3可能就再也回不来了。

对于用户来说，防范比特币攻击也非常简单。方法一：不要&#039；在尘埃落定之前不要转移比特币。分叉结算后，比特币可以转到两个不同的钱包和地址。直到两种资产完全分离，再转移到比特币，可能需要大量的时间和程序。方法二，把你的比特币放在可靠的钱包或者交易平台上。这些技术平台会帮助你处理因为自身运营需要，在分叉过程中可能遇到的各种问题。。如果你把你的比特币放在一个只支持分叉的比特币钱包里，你可能会面临一些无法获得新资产的损失。

如果你对区块链数字货币交易平台的价格感兴趣，希望找一个可靠的区块链官方数字货币交易平台。那么你可以更深入的咨询我们币牛官方客服，同时可以免费申请加入我们币牛官方社区。团币圈区块链经验丰富的职业玩家和行业名人可以帮你答疑解惑，共同进步。