如何理解比特币的扩容和分叉，什么是硬分叉和软分叉！

比特币每个块的大小是1M，可容纳1000多个交易信息。如果你在最后一个比特币区块浏览器上观看，你会发现每个区块现在大约有100个M大约，已经达到了块容量的上限。如果比特币网络的转账越来越多，许多交易将不会包装和确认交易后的第一个块，可能需要等待几个块或更长时间。

比特币在历史上经历过几次“粉尘攻击”。所谓“粉尘攻击”，也就是说，有人创造了大量的小转账，使得网络中有大量的交易需要确认，导致正常的比特币转账无法确认，确认时间延迟，影响网络的正常运行。

在“粉尘攻击”在事件中，许多交易者等待了两天或更长时间才得到确认。“粉尘攻击”非常极端的例子，但是看现在的比特币网络，正常转账量已经远远超出了它们能够承受的最大容量。每个区块的大小现在都是1M，因此，扩大现有比特币容量，突破现有1M这个过程叫扩容。

自2014年以来，比特币社区一直被提上议事日程。我们知道比特币网络是一个分散的网络，世界上没有一个集中的机构来运作，一切都取决于社区协商达成协议。不同的团队对扩张有不同的想法，所以推广效率相对较低。

2015年底，比特币Core开发团队和矿工在香港举行了圆桌会议，当时在香港达成了共识，但很快就流产了。2017年，纽约比特币社区重新协商，采用隔离见证加2M扩张的方式再次达成共识，我们称之为纽约共识。共识当天，全球21个国家56家知名区块链初创名区块链初创公司的共同签署和全网83%左右计算能力的支持。因此，比特币系统从2017年上半年开始升级和部署。

事实上，比特币扩容的方案有很多，历史上也经历了许多迭代。一般来说，有两种方式：一种是不接触比特币本身的区块，使用闪电网络结算比特币，将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区块的大小。这里要解释什么是闪电网络，例如：几个朋友一起玩牌，不是每一轮结算，而是最后结算。A欠B10元，B欠C20元，最后C给A10元，B给C10元就可以了。闪电网将首先记录大量的小转账，最后结算，这样比特币网络就不会被大量的小转账交易所占据。然而，该技术成熟，闪电网络需要在隔离见证的基础上应用，尚未大规模应用，因此网民关注比特币块本身的扩展。

比特币块本身的扩容是一种相对成熟的技术方法。有以下三个主要的扩容方案：BI

P141、 UASF和Segwit2x。

BIP141是比特币Core团队提出的隔离见证方案。隔离见证是为了让区块承载更多的交易量而设计的。我们知道区块上的信息分为交易信息和见证信息，交易信息是区块上记录的转账；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时直接将这两个信息放在区块中，因此一个区块可以携带的交易信息不多。如果将见证信息从区块中取出，区块只记录交易信息，也可以从这个角度扩展区块可以携带的交易信息。

BIP141是目前公认的隔离见证激活方案。激活条件是在2017年11月15日任何困难周期约两周内。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激活方案。UASF或Segwit2x实现这种帮助BIP141激活隔离见证。

UASF字面意思是用户激活软分叉。UASF用的是一个叫做BIP2017年8月1日，比特币BIP148软件会拒绝不包含Bit1信号块，也就是说，如果大多数矿工操作该软件，他们将拒绝一些没有操作该软件的矿工挖掘的块。因此，这些矿工将拥有最长的链，并在最长的链上激活它们BIP隔离见证141。最终运行BIP链条上会看到95%以上的节点包含Bit1信号触发隔离见证。该计划已经实施，但我们现在看到了新的区块链资产—比特币现金。比特币现金的块大小可能上升到8M，可容纳的交易量约为原比特币原链的8倍。

Segwit2x有一些比特币公司和80%计算能力的矿工Consensus会议签署的纽约共识协议通过BIP91来激活隔离见证。BIP91的做法是在连续两天内支持80%的计算能力BIP所有91信号BIP91节点将拒绝所有不包括在内的节点BIP141准备信号块。因此，这些矿工将拥有最长链，并在最长链上激活隔离见证。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增加至2M。也有可能导致新的分叉。

什么是硬分叉，什么是软分叉呢?

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块，块将分为两个独立的链，矿工需要选择两个区块链中的一个进行采矿。

当比特币协议比特币协议规则发生变化时，旧节点不会意识到规则是不同的。他们将遵循变更后的规则，并接受新节点创建的块。因此，软分叉不会产生两个区块链，而是在原始链的基础上共存新旧。类似于软件升级，您保存了一个word在2003使用2003文档word2011年打开原来的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，最大的风险是“重放攻击”。什么是“重放攻击”，这件事可以追溯到2016年7月以太坊硬分叉过程中发生的事情。当时，教育平台和用户基本上是第一次遇到这样的事情，所以他们缺乏经验和准备，所以他们损失了很多。例如，比特币分为一种或多种比特币，我们称之为比特币1，比特币2，比特币3，用户账户同时存在三种相应数量的比特币，每个链地址和私钥算法，交易格式完全相同，导致一个链交易在另一个链可能完全合法，所以用户在一个链上，可以在另一个链上，也可以确认，这是“重放攻击”。简单地说，当你转移比特币1时，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和比特币3可能永远不会回来。

对于用户来说，防止比特币攻击也很简单。方法一:尘埃落定前不要转账比特币。分叉落定后，比特币可以转移到两个不同的钱包和地址，直到两种资产完全分离，然后转移到比特币，这可能需要很多时间和程序。方法2，把你的比特币放在一个可靠的钱包或交易平台上，这些技术平台将帮助你处理分叉过程中可能遇到的各种问题，因为他们自己的操作需要。如果你把你的比特币存在于一个只支持分叉的比特币钱包中，你可能会面临一些新资产将无法获得的损失。

如果您对区块链数字货币交易平台价格比较感兴趣，希望找到可靠的正式区块链数字货币交易平台，那么您可以更深入地咨询我们的货币牛官方客户服务，同时可以申请免费加入我们的货币牛官方社区，集团货币圈区块链经验丰富的专业玩家和行业名人，可以帮助您回答问题，共同进步，货币圈掘金。