凌晨2:16分，BCH在第556767个块高度发生硬分叉，分叉大战落下帷幕，分成了BCH ABC和BCH SV两个阵营。

在此次此次硬分叉中，BCH ABC和BCH SV双方都没有进行“重放保护”。也就是说，此次分叉后，理论上，重放攻击将有可能导致任何一方发生共识崩塌和算力归零。

何谓“重放攻击”

传统计算机术语中，重放攻击(Replay Attacks)又称重播攻击、回放攻击，是指攻击者发送一个目的主机已接收过的数据包，来达到欺骗系统的目的。重放攻击在任何网络通讯过程中都可能发生，是计算机世界黑客常用的攻击方式之一。主要用于身份认证过程。

而在区块链领域，重放攻击(Replay Attacks)通常出现在区块链硬分叉的时候，指的是“一条链上的交易在另一条链上也往往是合法的”。

有一个例子可以简单的说明什么是区块链中的“重放攻击”：

小A向某个不能有效识别付款（这里指不能判断是哪一笔付款）的啤酒厂买啤酒，
当他把用支付宝成功付款的付款信息出示给销售员后， 销售员把啤酒给他。
然后小A又再把上次的付款信息出示给另一个销售员， 销售员又给他一份啤酒。
只要小A不断重复出示他的付款信息，就可以源源不断骗得啤酒，
这对于啤酒厂来说就是被重放攻击了，损失了无数啤酒。

就本次BCH硬分叉来说，BCH由一条链变成了两条链，在这两条链都得到支持并持续运营的情况下，另外一条分叉出来的链又产生了BSV这一资产，也就是BCH ABC和BCH SV都存在。由于没有重放保护，分叉完了之后如果不去管它，任其自然生长，这时候就会出现这样的情况：你在SV链上交易时，由于相同的地址、算法和交易格式，拿到ABC链上去重新广播，就有可能会被ABC链承认有效，从而进行相同的交易操作。攻击者一旦利用这个漏洞，不断在交易所进行充提操作（BCH SV），就能获取额外的BCH ABC。

这就意味着，没有重放保护的BCH用户资产已经被暴露于风险之中，更严重的，还将导致共识崩塌和算力归零。

“重放攻击”源起：以太坊硬分叉

2016年7月20日晚，以太坊在第192万个区块高度发生了硬分叉，产生了两条链，分别称为ETH chain和ETH Classic chain，上面的代币分别称为ETH和ETC。

这两条链上的地址和私钥算法相同，交易格式也完全相同，导致在其中一条链上的交易在另一条链上很可能是完全合法的。所以你在其中一条链上发起的交易，放到另一条链上去重新广播，可能也会得到确认。

由于事先没有做好预案，很多人利用这个漏洞，不断在交易所进行ETH充提操作，获取额外的ETC。 “重放攻击”得以在区块链世界被重新定义。

受重放攻击的影响，对用户来说，以太坊目前的问题是存在的。因为ETH和ETC都有很好的经济量，而用户如果无法解决掉自己的操作被重放的可能，他想卖其中一个资产的同时保留另一个资产，要么自行进行分离，要么就只能在交易所的协助下才能实现了。

应对：先分离 再交易

既然BCH在没有重放保护的前提下已经发生分叉，被重放无法避免，那么，为了避免受损失，交易所和用户都有必要在进行新的交易之前，对所持有的BCH ABC/BCH SV进行分离。

让我们回看一下BCH升级后的两个版本：bitcoin abc 0.18.2和bitcoin sv 0.1。

Abc0.18.2协议版本主要修改是增加了两个操作码OPcode， OP_CHECKDATASIG（CDS）和OP_CHECKDATASIGVERIFY（DSV）；将区块里的交易排序规则从拓扑排序（TTOR）改成了规范排序（CTOR）。

SV0.1协议版本主要修改是恢复了比特币早期的四个操作码OPCode，OP_MUL，OP_LSHIFT，OP_RSHIFT，OP_INVERT；删除每个脚本201个操作码的限制；提高区块大小上限到128MB。

由于两个版本都更新了操作码，对于已经持有BCH的用户来说，使用新的 OP code进行交易操作，应先进行分离再操作账户更为稳妥。

分离最简单有效的办法，就是在分裂点后100个区块，从矿池购买一丁点coinbase交易的UTXO，发到你的BCH钱包里，然后将所有余额一次性转入一个新地址。只需要在一条链上这么做一次，就可以彻底分离出来了。

分离两种资产后，新OPCode你就可以使用了，不会出现因被重放而导致新OPCode在BCH链上有安全隐患的情况。

在此安比（SECBIT）实验室提醒广大BCH持有者和支持ABC/BSV的交易所，在分离你/你的用户的BSV之前，为避免重放造成损失，在交易中谨慎使用新的OPCode。