# 51%算力攻击

## 什么是51%算力攻击

比特币白皮书中，有过这样的表述：诚实节点控制算力的总和，大于有合作关系的攻击者算力的总和，该系统就是安全的。

换句说，当系统中有合作关系的恶意节点所控制的算力，超过诚实节点所控制的算力，系统就是有被攻击的风险。

这种由恶意节点控制超过50%算力所发起的攻击，称为51%算力攻击。

那是不是所有的加密货币系统都有可能遭遇51%算力攻击的风险呢?

其实并不是的，只有基于 PoW（工作量证明）共识机制的加密货币，才存在51%算力攻击，比如比特币、比特现金和目前阶段的以太坊等。

**一、如何发动51%攻击?**

假定发动51%攻击的人是一个理性的人，攻击的目的为了利益，而不是为了其他，因而攻击者在发动攻击前有两个条件：

1、掌握了比特币全网的51%算力
2、手里持有大量比特币

攻击者发动攻击

1、把比特币转到交易所或某个机构或个人，卖出所有比特币，并且收到钱、把钱提现到银行帐号(提现目的是为确保收益，也可不用提现)。这个时间越短越好，能大大节省攻击时间。

2、用51%算力从还没向交易所转币的区块开始重新生成区块

比如：向交易所转币的区块为第30万个区块，攻击者就在第29万9999个区块开始重新生成区块。

3、因为攻击者有51%算力，而且假设他能在攻击过程中保证一直51%算力，所以他的攻击一定成功，也就是说他生成的攻击块链一定能追上原块链。

4、当攻击块链的长度超过原块链2个区块，所有的客户端将丢弃原块链，接受攻击块链。至此，51%攻击成功。

**二、造成后果**

原块链上29万9999个区块之后交易全部作废，有以下影响：

A 29万9999个区块之后没有交易的客户的币数量没有任何影响。
B 29万9999个区块之后转出比特币的人会发现：币回来了。
C 29万9999个区块之后接收到比特币的人会发现：币消失了。
D 最重要的后果是：人们对比特币网络的信心降到冰点，比特币的币值将受到重创。

**三、51%攻击方法说明如下**

1、这是一种能够获得最大利益的51%攻击方法，因为我们假定攻击者是理性的、为获得利益而攻击，而非一心置比特币于死地而不求任何回报的疯子。

2、无需51%算力就可以发动51%攻击，比如45%算力，有成功可能性，但非确定性成功。有这么一个场景：原块链长度30万，攻击者具备45%算力，从29万9999个区块开始计算，运气好的话，攻击块链延长到30万零2个，而原块链还是30万长度，攻击就成功了。这种攻击影响的区块数量少，如果币数量小，则被发现的可能性很小。目前大家担心的是这种情况。本人认为，虽然连续产出3个区块的可能性

不大，但不是没有出现过，ghash.io就出现过连续产出5-6个区块的情况。因而这种非51%攻击的可能性完全存在，比特币世界要时刻监控、密切注意。

3、有人说多等几个确认就能避免51%攻击。这话有严重问题。如果是非51%算力的攻击，多等几个确认是有效的，数量特别大的比特币转帐应该等几天。但是如果是51%算力攻击，就应该知道，如果攻击者能一直保持51%算力，他可以从比特币最近检查点之后的区块开始重新计算，攻击块链能追上原块链，成功只是时间问题。如果攻击花费了1年时间，也要等1年的确认吗，因而这种认识不全面。

4、攻击块链可以隐藏地计算，直到比原块链多两个块链后才放出，按照目前的比特币网络协议，可以马上取代原块链，因而整个攻击可以不为人所知，直至最后一时刻。

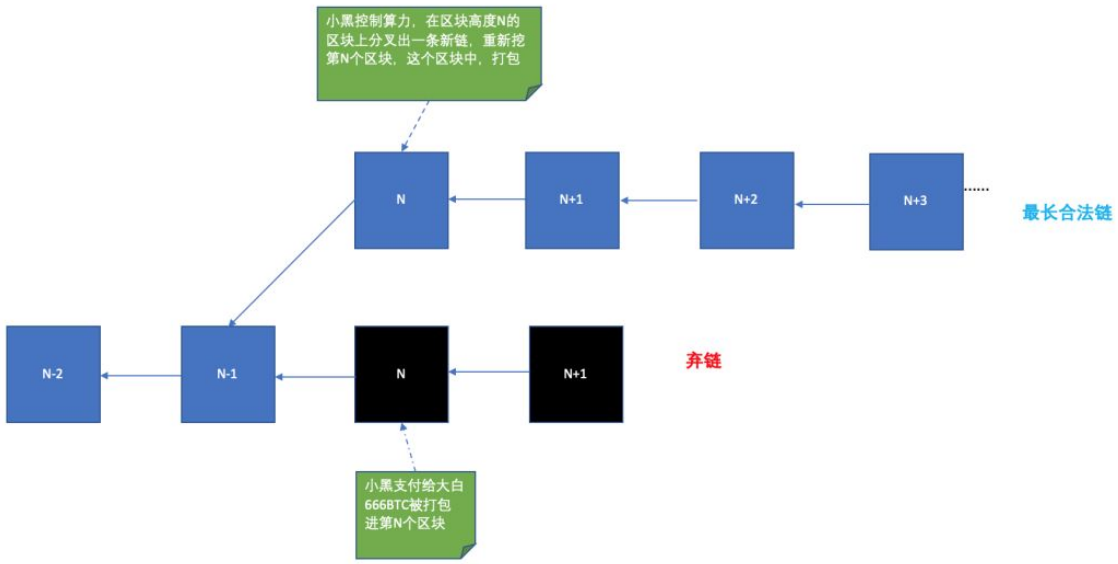
## 可以干什么事

1、双花（Double Spending）。

双花的意思是一份"钱"花了两次甚至多次。51%算力攻击是如何做到双花的呢?

假设小黑有 666 BTC，他把这些 Token 支付的大白同时，也把这些 Token 发到自己的另一钱包地址上。

换一句话说，小黑的一份钱，同时转给两个人。最终，发给大白那笔交易先被得到了确认，并打包在区块高度为 N 的区块内。




这时，控制了超过50%算力的小黑，发起51%算力攻击。他通过重新组装第 N 个区块，将发给自己那笔交易打包进区块里，并持续在这条链上延展区块。

由于算力的优势，这条量将成为最长合法链。这样小黑666BTC双花成功，大白钱包里的 666 BTC"不翼而飞"了。

2、压制某些地址发送/接受比特币

除此之外，51%的算力攻击还能做什么呢？它还可以压制某个地址发送/接收比特币。

小黑和大白吵架了，小黑仰仗自己掌控了51%算力，他在知道大白比特币地址情况下，可以让与大白相关的交易一直无法确认。

比如大白为了向中本聪表达自己的敬意，想往"创世地址"发送 1 枚比特币。掌控超过半数算力的小黑，不会打包这条交易，不仅如此小黑还能做到让其他矿工也不会打包这条交易。

小黑是怎么做到的呢?

如果其他矿工挖出的新区块打包了这笔交易，小黑会选择不在这个区块之后继续挖矿，他会选择在上一个区块之后，重新构建新区块，并把大白这笔交易拒绝在外，仰仗自己算力优势，小黑分叉出的这条链，将成为最长合法链。

在这种情况下，其他矿工也就只好不打包与大白有关的交易，否则挖出的区块也会被小黑给孤立，得到出块奖励也将被作废。

PS：即使控制超过50%的算力，也不能转移其他人的 Token，因为这个操作是需要私钥进行签名，如果想伪造签名来"偷币"，这种行为是诚实的矿工所不能容忍的，这将颠覆系统共识。

**我们不担心51%区块链攻击有以下几点：**

区块链的维护者们，为了共同的利益，不会允许某个机构或个人的算例突破到51%。

拥有51%算力的拥有者，不会愿意做这种搬起石头砸自己脚的事情。

追求完美的工程师们，为了避免这种理论上的可能性，思考出了其他共识协议来解决该问题，比如PoF等。

比如，PoW共识协议在比特币系统中稳定运行了将近十几年时间，从来没有因为51%算力攻击出现问题，因为51%算力攻击仅仅是理论上可行。