特地是12月中旬以来，比特币的价钱在突破2万美元新高后末尾狂泻，最大跌幅将近40%，很多比特币用户末尾怀疑比特币系统的牢靠性。本文尝试对一些常被提及的攻击手段中止剖析，议论一下比特币终究能不能被杀死。

一、151%攻击

攻击原理：攻击者破费巨额资金置办或租用少量的矿机，超过总算力的51%，形成51%攻击，从而可以窜改区块数据，制造双花，招致人们对比特币的怀疑破灭。

剖析：首先，目前比特币网络的总算力已达天文数字，要形成51%攻击，需求数百亿美元的资金，而且不能改动历史买卖，除了可以双花外没有其他的利益，因此，除国度机器外，没有团体或机构有这个财力和动力去做这事。而国度机器要动用这么庞大的资金不可以没有任何征兆，会惹起猛烈的国际反应，要做这样的决策不是一件易事。

其次，发起51%攻击不是一挥而就的，需求相当长的进程，而比特币网络的算力散布是公开实时可见的，在抵达51%之前就会被社区发觉，历史上曾经发生过——2014年Ghash.io矿池的算力曾屡次短期抵达过51%，惹起了社区的警觉，收回了正告，矿工们自觉地撤离了该矿池，使算力快速公开降到平安水平。

第三，假定攻击者专断专行，继续扩展算力，其他矿工们可以采取团体屏蔽该矿池IP的方式将其孤立，构利息质上的硬分叉，然后经过普遍地宣扬，由最终用户选择抛弃攻击者的区块链，使得攻击者的算力毫无用途。

第四，比特币的开拓者还有一个“终极核武器”，那就是矫正共识算法。只需改动共识算法中几行关键代码，就能够让一切的矿机报废，回到CPU/GPU挖矿的时期，攻击者和所有矿工一同同归于尽，而比特币网络照旧能够一般运转。

总之，51%攻击不只代价庞大，也是实际上不能抵达手腕的。

二、断网攻击

攻击原理：目前比特币的买卖报文是没有加密的，扫尾的4个字节总是0xF9BEB4D9，很冗杂被选择进去。经过对比特币报文中止剖析，依据其特征在主干网上将其屏蔽，从而使比特币节点无法收发买卖，破坏局部甚至整个比特币网络。

剖析：首先，该攻击手段在一国境内是可行的。但该国的比特币节点可以采用VPN

大约在Tor网络上运转比特币钱包软件，这样一切的报文都是经过加密的，不再具有上述特征，也就无法屏蔽。

其次，比特币软件开拓者可以矫正软件，直接采用经过混杂、加密的报文停止网络交互，固然功用会受到肯定影响，但上述屏蔽手段自然就无法失效了。

第三，即使局部国度能够在技术上屏蔽一切比特币买卖，但只需还有别的国度没有实施屏蔽，比特币网络就能一般运转，杀死比特币的手腕就无法达成。被屏蔽国度的买卖者可以经过其他手腕与比特币网络停止交互，如微信、电子邮件、卫星等，仍然可以进行交易，只是麻烦了许多而已。

三、难度攻击

攻击原理：经过对大少数的矿池节点进行DDoS攻击，使其无法参与记账，形成全网算力大幅下降，而挖矿的难度是不会跟着下调的，从而招致整个记账延迟，汇进来的款项迟迟不能被确认抵达收款人手里。

分析：有两种对策：一是矿池改换IP地址脱离攻击，只需有相当一局部矿池脱离攻击范围，整个比特币网络依然可以一般运转；二是修正比特币的难度调整算法，变短难度调整周期，就像比特币现金所做的那样，胜利地防止了难度攻击。

四、病毒攻击

攻击原理：向钱包软件中注入病毒，偷盗比特币。

分析：这种攻击是可行的，但只能针对团体进行，不能影响到整个比特币网络。梦想上针对比特币钱包的病毒和木马少见多怪，也频频发生偷盗事情，但并没有影响到人们比照特币的决计，防病毒软件公司也在不时地更新防范措施。

五、量子攻击

攻击原理：随着量子计算机技术的逐渐干练，未来可以运用算力弱小的量子计算机破解比特币的加密算法，从而破坏整个比特币零碎，招致比特币变得一文不值。

分析：首先，比特币采用了少量的加密算法来保证零碎的平安性，这些算法都是国际通用的算法，在各行各业取得普遍的运用。等量子计算机展开到可以破解这些算法时，遭到威胁的不只仅是比特币，而是整团体类社会。

其次，往常学术界曾经有了很多抗量子攻击的加密算法，只是思索到功用效果未被

业界采用，而比特币在设计上曾经思索到未来可以改换加密算法，一种实验性地采用了抗量子加密算法的新型数字货币Hcash也行将推出。

六、交易所攻击

攻击原理：攻击或封锁交易所，断开法币与比特币交易的通道，破坏市场决计。

分析：这一手段在中国用过了，但比特币的价钱却一飞冲天，充沛说明了其有效性。比特币不是一国的数字货币，只需国际市场还具有，就无法破坏。况且即使封锁了交易所，人们还可以进行场外交易，或在去中心化交易所交易。

七、硬分叉攻击

攻击原理：不时改动比特币钱包软件的参数或算法，招致少量的硬分叉，手段是聚集比特币用户群，降低比特币的网络效应。当每一个分叉的用户群都变得很小时，就很冗杂杀死比特币了。

分析：2017年8月比特币现金第一次硬分叉，曾让比特币用户极为担忧，但实际上对比特币并没有形成不良影响，之后频频出现少量的硬分叉币，带来的却是比特币价钱和交易量的双双下跌。出乎意料的结果，充沛证明了硬分叉攻击的不可行。

那么，怎样才干真正杀死比特币呢？

笔者想象了两种情形：

一是一切的比特币开拓团队都墨守成规，墨守成规，不再吸纳最新的科技效果完美自己，从而出现新的数字货币各方面技术手段片面跨越比特币，被社会普遍接受，进而取代比特币。这是比特币的失利，但也是虚拟数字货币的成功。

二是比特币协议或钱包软件出现严酷的破绽，招致整个比特币系统的平安性不能取得保证，出现大面积的资金被盗、被贱卖且短期内不可控，社会对比特币的决计完整丧失。

由此可见，由于比特币的完整去中心化特性，从外部进行攻击是不能够杀死比特币的，只需比特币自己才干杀死本人。