OTC = 法币交易 C2C = customer to customer 个人与个人之间的电子商务

OTC = Over the counter 场外交易

交易对 挂单 吃单

火币、币安、OKex = BHO

ICO = Initial Coin Offering 首次币发行 别名；首次公开募币

密钥 = secret key

密文 = Cipher Text

密文是加了密的文字，明文是加密之前的文字。密文是以明文进行加密后的报文。

网络安全、用户验证、入侵检测、密码技术有情

=====================================================================

51%攻击

A矿工挖出新区块后，会将这个消息广播到全网，但广播的过程存在时滞。有时，B矿工也挖出了区块，在没有及时收到广播的情况下，将自己的消息广播给了其他矿工。

收到A矿工广播的人会将后续区块链接到A挖出的区块后面，还有些矿工则将新区块链接到了B挖出的区块后面。

这时，比特币网络出现了两条分支。

针对这种情况，全网有一套公认的“取舍机制”：只认可一条链，哪条分支后面跟的区块最多，哪条分支就会被保留，另一条分支上的区块就全部作废了。

51%攻击正是利用了这套机制，可以反复使用同一笔比特币。

他先用比特币交易，按照记账原理，这条信息被链接到了区块链最新的一个区块上。接着，他在记录了这笔交易的区块的前一个区块后面迅速添加新区块，只要他添加区块的速度比原来那条链添加区块的速度快，就能成功将这条分支变成最长链。

由于比特币网络永远只认可最长链，所以原先的那条链被撤销了。记录了他的交易信息的区块也作废了，他之前转出的比特币又回到了他的手中。

你应该也发现了，这种攻击可以成功的前提就是攻击者打造分支的速度要足够快。根据概率学计算，当有人拥有全网51%算力时，他发起的攻击肯定能够成功。

========================================================================

离线钱包，又称离线电子钱包，是指一种离线支付使用的电子钱包。

交易费可当作是为了包含（挖矿）一笔交易到下一个区块中的一种鼓励，也可当作是对于欺诈交易和任何种类的系统滥用，在每一笔交易上通这征收一笔小成本的税而造成的一种妨碍。交易费被挖出这个区块的矿工得到，并用记录在这个交易的区块链中。

Basic 标准版

Advanced 专业版

DDOS = distributed denial of service 停止服务

CDN = Content Delivery Network 内容分发网络，通过在网络各处的加速节点服务器来为网站抵挡恶意流量，把正常流量进行转发。

网络账本

底层技术

区块中