本文将基于46个交易所的工作证明(PoW)对9种主流加密货币进行分析。我们从三个维度测试了交易所的确认时间，分别是：块、分、美元值。

加密货币交易所是黑客的主要目标。加密货币价值的巨大流量可以满足他们发动双花攻击并从中获利的企图。就在最近，一些交易所受到了比特币黄金攻击的影响。

虽然交易所无法防止51%计算能力攻击(双花攻击)，但可以调整充值所需的最小块确认次数，以降低此类风险。交易所可以增加支持资产的大宗确认时间，可以增加黑客反向交易的成本。

Block联系了一些交易所，以了解他们在设置充值确认时间时在用户便利性和安全性之间的权衡。然而，大多数交易所不愿提供更多有关大宗交易确认的信息。出于安全原因&quot只有一次交流让我们对这种过程有了一些了解。

根据一家大型亚洲交易所的反应，大多数顶流交易所为了确定一项资产的大宗确认号，会考虑很多因素。，包括&quot相关令牌的算法、网络和生态系统的历史、网络的当前操作&quot诸如此类。然而，该交易所也指出，该平台必须平衡便利性和安全性。他们说，

从我们的角度来看，最重要的是保证交易所和用户的安全。但我们也希望给用户带来快速便捷的体验，所以我们在努力实现两者的平衡。

问交易所多久调整一次块确认时间，交易所告诉我们。技术小组一直在监控货架上资产的网络状态，但是&quot如果没有必要，我们不愿意调整。"

Let&#039；s选取九项资产的确认时间进行分析。在此之前，让&#039；让我们解释一下下图中提到的概念：

确认：这是指在交易所充值后，资产到达账户(并投入使用)所需的批量确认次数。需要注意的是，部分交易所对充值/取款设置了不同的确认号。在本文中，我们只分析充值确认号码。

分钟：指交易所充值后资产到账(并投入使用)所需的时间(以分钟为单位)。这可以通过将区块链的平均块间隔时间乘以所需的块确认次数来获得。。比如取出一块比特币的平均时间是10分钟，在比特币基地上确认收到比特币充值需要3块，所以用户在比特币基地上充值后需要等待30分钟(即3次确认*10分钟)。

$:这是指区块奖励的美元值，可以帮助我们估算黑客试图对交易所发起双花攻击时必须承担的成本。这是通过将每个块中奖励的代币乘以在书写时对应于该货币的美

元值，然后将其乘以交易所要求的块确认的数量来获得的。。比如目前比特币一个区块的奖励是12.5BTC，按照4986美元/BTC的价格计算，区块奖励大约是62300美元。如果黑客计划在比特币基地双倍消费他们的比特币余额，

，那么费用大概是18.7万美元(也就是6.23万美元*3次确认)。为了简化计算，我们不&#039；本文不考虑交易成本，只考虑块报酬。

比特币（BTC）

下表显示了每个交易所比特币充值所需的最低确认次数。

抽样的46家交易所全部接受比特币。

这些交易所需的比特币块确认次数平均为2.4次(20.4分钟)。，中位数是2(20分钟)。[XY002][XY001]其中4家交易所接受比特币充值的方式是最保守的，即6次确认(60分钟)。也就是说，用户在这些交易所充值比特币后，需要等待一个小时才能到账。

而如果黑客发起攻击，逆转交易需要花费37.4万美元。[XY002][XY001]近三分之一的交易所将确认号设置为1。

以太坊（ETH）

下表是每次兑换ETH和以太坊代币充值所需的最小确认号。

抽样的交易所中有93%接受ETH。

这些事务所需的以太网块确认的平均数为18(3.9分钟)，中位数为12(3分钟)。

充值方式最保守的有两个交易所。、独立储备和流动性。这两个交易所需要50次确认，这意味着用户需要等待大约11分钟才能给账户充值，而黑客需要大约1.1万美元才能逆转交易。

充值所需确认次数最低的是Bitfinex，5次确认(1分钟)

比特币现金（BCH）

下表为各交易所比特币现金(BCH)充值所需的最低确认次数。

91%被抽样的交易所接受比特币现金(BCH)。

这些交易要求的BCH大宗交易确认的平均次数为7.2次(72分钟)，中位数为4.5次(45分钟)。

Coincheck&#039；的充值方式是最保守的，需要30次确认。换句话说，用户给账户充值大约需要300分钟，而黑客反向交易大约需要63000美元。[XY002][XY001]四家交易所的确认数量最少。

，用于1次确认(10分钟)。

BSV

下表为各交易所BSV充值所需的最低确认数。

41%的抽样交易所接受BSV。

这些交易所要求的BSV大宗交易确认的平均次数为18.5次(185分钟)，中位数为10次(100分钟)。

在这些交易所中，Bibox&#039的充值方式是最保守的，需要80次确认。

。换句话说，用户需要等待大约800分钟才能给账户充值，而黑客需要大约11万美元才能撤销交易。

充值需要的最低确认次数是Bitforex，1次确认(10分钟)

莱特币（LTC）

。

85%的抽样交易所接受LTC

这些交易所要求的LTC大宗交易确认的平均次数为4.6次(11.5分钟)，中位数为4次(10分钟)。

最保守的充值方式有四个交易所，需要12次确认。也就是说，用户给账户充值大约需要30分钟，而黑客反向交易大约需要4900美元。

七家交易所的充值确认次数最少。

，33%的交易所抽样确认(10分钟)

门罗币（XMR）

接受XMR

。

这些交易所要求的XMR块确认的平均次数为10.5次(21分钟)，中位数为4次(16分钟)。

其中液体的充值方式最为保守，需要50次确认。换句话说

用户给账户充值大约需要100分钟，而黑客反向交易大约需要3000美元。

6家交易所充值所需确认次数最低，3次确认(6分钟)

达世币（DASH）

。

65%的抽样交易所接受破折号

这些交易所要求的破折号阻止确认的平均次数为12次(30分钟)，中位数为7.5次(18.7分钟)。

最保守的充值方式有三个兑换，需要50次确认。也就是说，用户给账户充值大约需要125分钟，而黑客反向交易大约需要6700美元。

充值需要确认次数最少的有四个交易所。

，59%的交换被抽样确认(2.5分钟)

以太坊经典（ETC）

被接受等等

。

这些交易所要求的ETC块确认的平均数量为2150(466分钟)，中位数为100(21.7分钟)。

其中，北海巨妖&#039；s充值方式最保守，需要43200次确认。。换句话说，用户给账户充值大约需要9360分钟，而黑客反向交易大约需要62.1万美元。

CoinEx充值需要的确认次数最少，12次确认(3分钟)。

。2019年以太坊经典经历了一轮51%的攻击。

ZCASH

抽样的交易所有63%接受ZCASH

。

这些交易所要求的ZCASH大宗交易确认的平均次数为15.5次(39分钟)，中位数为12次(30分钟)。

其中，STEX&#039；s充值方式最保守，需要110次确认。换句话说

用户给账户充值大约需要275分钟，而黑客反向交易大约需要32000美元。

CoinEx充值需要的确认次数最少，为1次确认(2.5分钟)。

交易所之间的比较

块比较样本中九项资产所需的块确认的标准偏差。与标准差巨大的经典以太坊相比

，每次交易所比特币充值所需的确认次数差别不大。

就是说交易所已经就比特币的大宗确认数量达成了普遍共识。但是对于以太坊经典来说，每次兑换的区块确认数量差别很大。需要注意的是，支持每种资产的交易所数量也会影响其标准差。

另外，比较了各种交易所的大宗确认所需的时间(分钟)(删除了ETC，因为ETC与其他货币的差异太大，难以正常解读图表)。虽然比特币网络的安全性相比其他资产是最高的，但是从充值等待时间来看，换货给用户造成的成本有时候太高了。

下表说明了资产确认所需的美元成本(参考2020年3月16日的数据)。

本文为区块付费内容。