# 概要

存在一个广为人知的说法，即基于权益证明（POS）机制的数字货币相比于基于工作量证明（POW）机制的数字货币更加不容易受到51%攻击。在这篇文章中，

我们证明了这是错误的，实际上，如果攻击者的动机足够大（这是常识），他将会攻击成功而无需成本。

# 简介

比特币在2013年越来越受欢迎，尽管它在2008年就已经出现了。它通常由外行人描述为电子货币，但是这个定义在计算机科学界通常为革命性的协议。该协议的核心，

比特币可以提供财产权的保障，在一个去中心化点对点的网络中，记账单位以有限的速度来生产。存在购买和交易比特币的市场。在这篇文章写下的时候，大概1230万个

比特币正在流通，一枚比特币大约价值850美元。不管我们从理论上将它归类为货币还是资产，经济学家应该对这种新的“不明金融物体”感兴趣。在这篇文章中，我们研究

比特币技术的一个特殊方向，在数字货币社区里存在争议，我们借鉴了经济学中的一些工具。

为了达到这一目的，我们需要描述一下比特币的工作原理。当一个个体发送比特币至另一个个体时，该信息会在比特币网络上进行广播。但是，因为技术目的我们不会在

此讨论。该转账，被当作一个区块和其他转账一起被处理，需要被添加进区块链用来确认和固定。区块链是一个公共帐本，包含了历史上所有的比特币转账记录。而确认

和固定区块链的工作是通过矿工来完成的。实际上，这个挖掘过程包括解决一个数学问题，RST矿工通过这种技术手段完成了基于工作量的证明（POW），可以将一系列的

转账添加到区块链上。因为它需要计算力的资源，成功的矿工会得到比特币作为奖励。为了控制货币基础，挖矿被设置成了更加复杂的模式。因为每个矿工解决问题的可能

性依赖于他的算力，挖矿的难度由系统中所有算力的总和来决定。总结一下，对于POW机制的加密货币，包括比特币，矿工是通过竞争解决数学问题来确认和固定转账。第一个解决问题的矿工得到奖励。该问题的复杂是刻意制造的，用来控制货币基础。这个处理过程被一些人认为是天才之举，但是被另外一些人批评没有效率因为白白损失了资源。是这样的，比特币的矿工们需要进行算力的军备竞赛，到最后，很多硬件、工程和能源会被用来解决人造的极端困难的问题。

因为需要对系统的信任来让大家接受，比特币是开源的。所以，许多替代数字货币可以没有成本地制造出来。每一个都宣称解决了比特币的缺陷。很自然地，一些数字货

币试图针对比特币POW机制的无效率。大多数数字货币都是基于另一个挖矿流程，被称为基于权益证明（POS）机制。为了方便和不那么生硬，我们下面就称之为POS，

将转账添加进区块链的预期回报不是基于矿工的算力，而是基于矿工们目前拥有的数字货币数量。Peercoin和Nxtcoin是两个使用POS机制的替代货币（前者部分，

后者完全）。

让我们现在来解释一下所有数字货币的弱点。简单地说，不管是POW还是POS，如果一个单独的矿工可以创造大量的区块，那么任何数字货币都不可信。在POW数字货币中，

这种情况被称为“51%攻击”，这会导致该货币的价值遭受重创，即单个矿工拥有了超过了50%全网络的算力。在POS数字货币中，当有某个矿工持有超过50%的货币时，

同样的攻击会也出现。在数字货币社区内有这么一个说法，POS相比于POW更不容易受到51%攻击，因为对于恶意节点而言购买50%的数字货币会比购买50%的算力更加昂贵

（直接和机会成本）。在这片文章中，我们会证明这种说法是错误的，并且对于恶意节点来说，购买50%的POS数字货币几乎无需成本。

# 模型

让我们假设存在N+1个节点，N>2。每一个节点都有一个序号{0,…,N}。在经济体中存在两个商品，数字货币（CC）和法币。没有货币流动性限制。每一个节点被分配一个

单位的CC。CC货币系统的利率用r来表示，单位为个/次。该利率代表了使用CC作为交换工具所产生的单位。对于所有的节点而言，时间消耗为β。CC失去所有的价值当某

个节点获得（（N+1）/2）个CC单位。节点0对于杀死CC有着特殊的兴趣。所以，它会得到U，如果某个节点获得了（（N+1）/2）个CC单位。

CC可以在市场上进行交易。我们特别关注这种情况，即某个节点（特指节点0）可能愿意持有超过半数的CC数量。所以，我们不能使用传统的供给—需求模型来认定节点们

都是原子个体。我们需要进一步来描述这个市场。在每一步里，节点0无差别地和其他拥有CC单位的节点i进行配对。节点0使用“交易或走人”的模式来向节点i提出购买CC

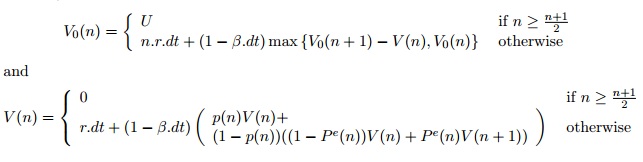
的要求。节点i接受或不接受该报价。成交与否建立在0的报价和i是否接受。每两次配对之间的时间差为dt，任意长短。我们将任意个一个节点i>0的对CC法币价值的

预期定义为V（n），n代表节点0所拥有的CC数量。V0（n）是节点0对于CC法币价值的预期，其中n是他自己拥有的CC数量。

很明显，步骤“0报价，i接受或不接受”有一个简单的输出：要么0给出了一个极低的价格被接受，或者提出了一个价格被拒绝。在第一种情况下，i的CC单位以

（1-βdt）V（n）成交。

一旦这一步被计算出来，我们可以精确地写出V和V0的动态分析：



在这里p（n）=1/（N-n）代表了任何拥有CC的节点和节点0配对的概率，。Pe（n）为任何非节点0的节点愿意让节点0购买CC的期望。

让我们来解决比（N+1）/2更小的最大的整数n的问题，n=（N+1）/2。这里有两个可能性的方程。第一个是Pe（n）=0，V（n）=r/β和V0（n）=nr/β。

这个子博弈方程当且仅当U≤r（n+1）/β的时候成立。第二个方程是Pe（n）=1，当dt趋于0的时候，V（n）趋于0，V0（n）趋向于U。这个子博弈方式当且

仅当U>r（n+1）/β的时候成立。让我来解决该博弈之前的一步。再一次，存在两个和上面一样的方程。第一个方程是对于所有的Pe（n），V（n）=r/β而V0（n）=nr/β。

该子博弈方程当且仅当U≤r（n+1）/β的时候成立。第二个方程是Pe（n）=1，当dt趋于0的时候，V（n）趋于0，V0（n）趋向于U。

这个子博弈方式当且仅当U>r（n+1）/β的时候成立。同样的逻辑可以一直推算出所有的步数。

然后，我们的博弈中有两个方程。在第一个方程中，当U>r（N+1）/β的时候，节点0买到了一半以上的货币会直接杀死了CC。因为这样的预期每一个节点都会存在，

所有节点会开始抛售他们的CC，因为他们知道没有价值了。这样的攻击几乎没有成本。

在第二个方程中，就算节点0积累了足够多的CC，他不会有激励来拥有超过50%的CC，因为对于他来说持有CC并获得利息比杀死CC要好。因为形成了这样的预期，

其他节点不会在他们的预期价值r/β以下卖出CC。

# 讨论

使用一个简单的模型（也许会有人说过于简化了），我们证明了流行于数字货币社区的一个说法是错误的，即POS机制免疫与51%攻击，因为其攻击成本太高了。

实际上，有一个问题没有考虑到，就是如果存在一个愿意杀死数字货币的人，其他节点会产生价值归零的预期，从而以极低的价格将数字货币卖给攻击者。

一个更加实际的模型会把攻击者的动机考虑进其中，即攻击者的动机（U），所以在这里需要引入贝叶斯分析，流动性限制，不同的未来预期……但是我们选择了

一个最简单的市场模型。我们检查过了，对于其他的市场模型，结果是一样的。特别的是，即使攻击者在“交易或走人”中符合史塔克堡模型中的追随者

（Stackelberg follower）时，我们的结果同样不变。得到我们结果的最基本的一个需求就是卖家们在面临攻击者时会争相出售自己的数字货币。

不管后面会不会出现真实的攻击，CC已经失去了价值，实际上攻击者无需真正开始购买CC。

我们相信，从最低程度上估计，我们认为POS更容易遭受51%攻击，而且POS作为POW的替代品是不可靠的。考虑到我们的模型对于POW机制不适用。实际上，

在POW机制中，节点需要投资固定成本来购买算力，承受挖矿利润的不断下降。在这种情况下，一个攻击者实际上需要购买超过50%系统算力硬件的固定成本。

而攻击者公布自己的动机，即使是真实的，也不会让其他节点放弃自己的前期投入。