双花问题（Double Spend Problem）

假设某区块链的最长链每收到一个区块确认一次。由于区块链的最长链原则，链上已确认的区块可能会由于其他分支的延长而被舍弃，使得区块中包含的数字资产可能被重复消费。这就是区块链中常见的双花问题。为应对该问题，人们提出了“k 确认交易”的概念，它是指在某笔交易上链后再得到区块链 k 个确认才正式成交。

在某笔交易确认后，现有一位攻击者试图通过建立分支链的方式使该笔交易被舍弃。已知攻击者获取该区块链中全网 51%的算力的单位时间成本是 1 万元，且全网 51%算力在单位时间内成功生成一个区块出现在目标分支上的概率是 51%（若单位时间内攻击者生成区块成功，视为分支链增加一个新区块且主链上未生成新区块；若单位时间内攻击者生成区块失败，视为分支链未增加新区块且其他人在主链上成功生成一个区块）。现有一笔价值 100 万元的交易经过 k 个确认后正式成交。请问 k 至少要多大，才能确保此后攻击者利用 51%算力成功篡改该笔交易所需成本的期望值高于该笔交易额？