双花问题

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。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。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，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失败，其他人会在主链上成功生成一个区块）。现有一笔价值 100 万元的交易等待成交，请问至少要在该交易上链后再得到多少个确认以上才能确保利用 51%算力篡改该笔交易所需成本的期望值高于该笔交易额？