Exercise 1 (Attacks)

You are a bitcoin user and you are running the bitcoin client. Your internet provider completely controls your network. Which of the following attacks can they carry out against you successfully, and why/why not?

1. Steal your coins.
2. Create money.
3. Censor your transactions.
4. Double-spend attack you.
5. Hide confirmed transactions from you, without you noticing.

Exercise 2 (Probability of a Successful Double-Spend)

Alice has 10% of the hash power of the bitcoin network. She sends you a transaction. How many confirmations do you require such that her probability of a successful double spend attack is lower than guessing your private key? Your private key has 256 bits. Use the formula or code from Nakamoto's paper.

prob.py

```python
from math import exp


def attack_success_probability(q, z):
    """
    Returns the success probability of a double-spending attack of an
    attacker with hashpower share q against a transaction with z confirmations
    """
    p = 1.0 - q
    lamb = z * (q / p)
    thesum = 1.0
    for k in range(0, z + 1):
        poisson = exp(-lamb)
        for i in range(1, k + 1):
            poisson *= lamb / i
        thesum -= poisson * (1 - (q / p) ** (z - k))
    return thesum


for z in range(100):
    if attack_success_probability(.1, z) < 1 / 2 ** 256:
        print(z)
        break

# prints "30"
```