***Question 1***

1. Alone, Alice and Bob's signatures cannot match the threshold they set, but both together OR either one with any one of the three judges' signatures must match the threshold. All three judges' signatures together also cannot match the threshold. Hence, we can set the threshold to 4 and distribute the keys as follows:

**Alice**: 3 keys

**Bob**: 3 keys

**Judges**: 1 key each (3 total)

The single standard multisig transaction should then be:

4 <pub\_Alice1> <pub\_Alice2> <pub\_Alice3> <pub\_Bob1> <pub\_Bob2> <pub\_Bob3> <pub\_Judge1> <pub\_Judge2> <pub\_Judge3> 9 OP\_CHECKMULTISIGVERIFY

1. One example could be:

<sig\_Alice> OP\_0 <sig\_Judge1>

<pub\_Alice> OP\_CHECKSIG

OP\_IF <pub\_Bob> OP\_CHECKSIG

OP\_IF OP\_VERIFY

OP\_ELSE 1 <pub\_Judge1> <pub\_Judge2> <pub\_Judge3> 3 OP\_CHECKMULTISIGVERIFY

OP\_ENDIF

OP\_ELSE <pub\_Bob> OP\_CHECKSIGVERIFY 1 <pub\_Judge1> <pub\_Judge2> <pub\_Judge3> 3 OP\_CHECKMULTISIGVERIFY

OP\_ENDIF

***Question 2***

***Question 3***

1. Assuming 12.5 BTC/10 mins, this gives us approximately spent on electricity, which leads to a power consumption of , that is 30 million kW.
2. The estimate may be too high (low) if the total network hash rate decreases (increases) in the next difficulty adjustment.
3. The estimate may be too high (low) if the total network hash rate decreases (increases) in the next difficulty adjustment.

***Question 4***

1. The probability of success in each active state is:

**Tie**,

**1 behind**,

**2 behind**,

Solving for ,

1. The number of additional blocks on average:

**Tie**,

**1 behind**,

**2 behind**,

Solving for ,