Question 1

a) 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
```

b) 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

a) Assuming 12.5 BTC/10 mins, this gives us approximately $12.5 \times 6 \times \$40000 = \$3000000/\text{hour}$ spent on electricity, which leads to a power consumption of $\frac{\$3000000/\text{hour}}{\$0.10/\text{kWH}} = 30000000\text{kW}$, that is 30 million kW.

b) The estimate may be too high (low) if the total network hash rate decreases (increases) in the next difficulty adjustment.

c)

d) The estimate may be too high (low) if the total network hash rate decreases (increases) in the next difficulty adjustment.

Question 4

a) The probability of success in each active state is:

Tie, $p_0 = \alpha$
1 behind, $p_1 = \alpha p_0 + (1 - \alpha) p_2$
2 behind, $p_2 = \alpha p_1$

Solving for p_1,

$$p_1 = \alpha p_0 + (1-\alpha)p_2$$
$$p_1 = \alpha(\alpha) + (1-\alpha)(\alpha p_1)$$
$$p_1 = \alpha^2 + \alpha p_1 - \alpha^2 p_1$$
$$p_1 = \frac{\alpha^2}{\alpha^2 - \alpha + 1}$$

b) The number of additional blocks on average:

Tie, $b_0 = (1-\alpha)b_1 + 1$
1 behind, $b_1 = \alpha b_0 + (1-\alpha)b_2 + 1$
2 behind, $b_2 = \alpha b_1 + 1$

Solving for b_1,

$$b_1 = \alpha b_0 + (1-\alpha)b_2 + 1$$
$$b_1 = \alpha\big((1-\alpha)b_1 + 1\big) + (1-\alpha)(\alpha b_1 + 1) + 1$$
$$b_1 = \alpha b_1 - \alpha^2 b_1 + \alpha + \alpha b_1 + 1 - \alpha^2 b_1 - \alpha + 1$$
$$b_1 = -2\alpha^2 b_1 + 2\alpha b_1 + 2$$
$$b_1 = \frac{2}{2\alpha^2 - 2\alpha + 1}$$