1. That the mining reward is large enough, and bitcoin itself would lose its value if people knew one person could control/undo valid transactions. Eventually he would be figured out and the trust in bitcoin as a currency would be lost.
2. There is less than 0.1% chance the attacker will catch up to the honest chain given the attacker has a 45% chance to find the next block and is 340 blocks behind.
3. q: z
   .10: 3
   .15: 3
   .20: 5
   .25: 6
   .30: 10
   .35: 17
   .40: 36
   .45: 137
4.
   a. Signing it only verifies that you wrote the data, not necessarily the order in which it was written. You don't know that the data retrieved at position i is necessarily the data you wrote to position i.
   b. Not necessarily. We can be sure we wrote the data, but we can't be sure it's the data we wrote at position i.
5.
   a. Write – retrieve all transactions, calculate new hash with new transaction concatenated at end of all transactions, store transaction
      Read – retrieve all transactions, concatenate all transactions and hash to verify against local hash, keep transaction you wanted to read
      verify – Hash the concatenation of all transactions and verify it on the locally stored hash
   b. Write – O(n) have to retrieve all, calculate 1 hash, store 1
      read – O(n) have to retrieve all, calculate 1 hash
6.
   a. Write – Hash the transaction, concatenate hash with the hash of a transaction of the same height and with the same parent (if exists), and repeat going up in level, concatenating neighboring hashes and hashing them together to form a parent hash until you reach the root.
      read – Retrieve the desired transaction, hash it, and recalculate the root hash by concatenating the transaction hash with its neighboring hash (stored locally), hashing them together, and repeating the process going up the tree until you reach the root, and compare the generated root hash with one stored locally.
      verify – Hash all of the transactions, concatenate with the neighboring hashes, hash the results, repeat until the root hash is formed and compare that to the locally stored root hash.
   b. Write – O(log n)
      read – O(log n)
7.

   a. ~24.5 blocks
   b. Using the formula for R_{pool} given in the paper with γ set to 1 ((a(1-a)^2(4a+(1-2a))-a^3)/(1-a(1+(2-a)*a)))/10
8.
9.
10. B. Is current legislation up to the task of handling cryptocurrency-based crimes? Are there any upcoming bills to pay attention to in this area? Have you run into any cases where you had a hard time prosecuting somebody due to shortcomings of the current legal system?