COL867: Mid-Term

Max. Marks: 35, March 16th 2018, Duration: 1 hour

1. (15 marks) Let us call the i^{th} block ($i = 0, 1, \ldots$) of a blockchain B_i. Suppose the blockchain uses a hybrid proof-of-work (PoW) and proof-of-stake (PoS) consensus protocol in which B_{Nk} for $k = 1, 2, \ldots$ are mined using PoW for some $N \in \{1, 2, \ldots\}$, and the rest of the blocks (except for the predefined genesis block B_0) are mined using PoS. Note that if $N = 1$ the blockchain is a pure PoW blockchain, and if $N = \infty$ it is a pure PoS blockchain. Assume that the price of the blockchain's cryptocurrency is constant at Rs. 1 per unit and that the price does not vary with time or depend on any parameter of the blockchain (such as N). Suppose that the targets for PoW and PoS are chosen such that a new block is generated every 10 minutes on average and that the mining rewards for all blocks constant and hence does not depend on the choice of N. Assume that the choice of 10 minutes makes forking very rare, assuming that all miners broadcast their mined blocks immediately and also mine only on the longest chain. In order to resolve forks, honest miners always mine on the longest chain in terms of total number of blocks (that is, number of PoW blocks + number of PoS blocks). State clearly any other assumptions you make. *Discuss your answers for the following questions in terms of the value of N.*

   (a) (3 marks) Is the scheme with $N > 1$ more energy efficient than a pure PoW blockchain? Why?

   (b) (3 marks) Is the scheme more robust to the nothing-at-stake problem than a pure PoS scheme? Why?

   (c) (3 marks) Is the scheme more robust to a long-range attack than a pure PoS scheme? Why?

   (d) (6 marks) What resources in terms on percentage of mining power and/or stake would an attacker need in order to perform a successful selfish-mining attack? Recall that in such an attack the miner deliberately delays his mined blocks to get a higher mining fee than if he played by the rules.

2. (10 marks) Let us call the i^{th} block ($i = 0, 1, \ldots$) of a proof-of-work blockchain B_i. Suppose that B_n for some $n > 0$ is the latest block mined and that all miners are trying to create B_{n+1}. Now an attacker named Otomakan[1] who has so far not been mining, publicly announces that he is going to fork the blockchain starting from B_{n-K}, that is, he plans to generate blocks B'_j which compete with B_j for $j = n-K+1, n-K+2, \ldots$. Suppose all miners other than Otomakan continue mining on the original blockchain and after some time has elapsed, B_{n+L} and B'_{n-K+L} are the last blocks successfully generated. Assume that all miners including Otomakan immediately broadcasts blocks as soon as they mine them. Suppose that out of M blocks mined in the original blockchain after B_n, a rational miner Hal who is not the attacker, has mined Q blocks. Assume that the total hashing power used in creating blocks (in both chains) remains constant after Otomakan starts his attack.

   (a) (4 marks) At this point in time, Hal wants to decide whether to continue mining on the original chain or to switch permanantly to mining on Otomakan's chain. Discuss whether he should switch or not based on the values of L, K, M and Q. Hal wants to maximize the total mining fees he earns *in the final winning chain*. Assume that no other miner switches his mining from one chain to the other. You need not do an exact analysis based on Poisson processes etc. You can give a rough qualitative answer based on the parameters mentioned.

   (b) (6 marks) Suppose Hal does not want to make a permanent switch to Otomakan's chain but is interested in using the competing chains to perform *arbitary number* of double spends. Discuss whether he can to do so based on the values of L, K, M and Q. Assume that no other miner switches his mining power from one chain to the other.

3. (10 marks) Answer the following briefly. The answer to each sub-question is not expected to be about 1 page in length.

   (a) (5 marks) Explain what a Merkle tree is and for what purpose(s) it is used in the Bitcoin blockchain. In particular, explain how the use of a Merkle tree in a Bitcoin block is superior to simply putting all transactions directly inside the block header.

   (b) (5 marks) Explain what Escrow is and how it can be implemented as a Bitcoin smart contract.

[1] The attacker's intentions seem to be opposed to that of the Bitcoin founder. Maybe that explains the name.