**Final term Exam**

**CSE528-Introduction to Blockchain and Crypto Currency (2021 Monsoon), IIIT Delhi**

**Max Points : 50 (There are 5 questions.)**

**Total Time : 1 Hour, starting at 10am on Saturday 4 December 2021 (IST)**

**Roll number: Mihir Chaturvedi**

**Name: 2019061**

*Instruction: The exam is open-book. It is strictly disallowed to copy&paste from the Internet, publicly available literature, or even from my lecture notes. Please rephrase your answers in your own language according to your understanding within the scope covered by the lecture notes. If you do not follow this instruction for a question, you will not get any points for that question. Within 1 hour and 5 minutes, where 5 mins are buffer for uploading in the MS word format (doc or docx), you should successfully upload through the google classroom to avoid any penalty: 5 points will be deducted for every additional minute. Note that those who are slow in typing can submit in any format but within* ***five days*** *its MS word format with 100% matching should be sent directly to my email account,* ***donghoon@iiitd.ac.in****.*

**Question 1. [10 Points] In PBFT ((Practical Byzantine Fault Tolerance), assume that the total number of Replica is 3f+1, where f is the maximum number of faulty Replica. Why does PBFT need the requirement that at least 2f+1 replies that agree with the same message in several stages? Explain in detail.**

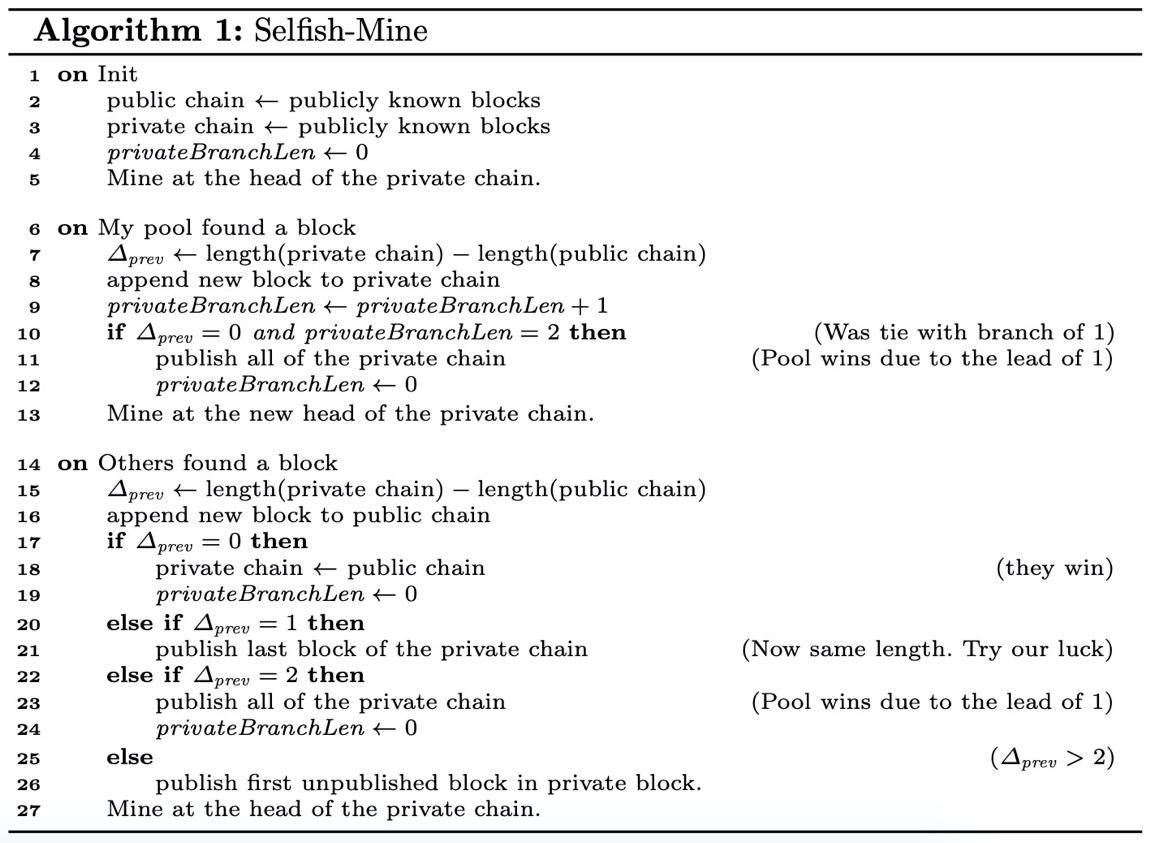
**Answer:**

* At the PREPARED and COMMITTED stage of the PBFT protocol, the nodes must wait for at least 2f+1 similar messages to arrive in order to broadcast their message.
* Let us assume that f is the number of traitor/dishonest nodes and N is the total number of nodes altogether, then we must show that by receiving 2f+1 similar messages we can make the decision and come to the same conclusion as other honest members.
* We show this by assuming that:
  + Suppose X received > 2f votes
  + Y also received > 2f votes
  + Thus total number of votes received by both is >= 2f+2
  + Number of traitors = f
  + Thus total number of votes is >= 2f+2 + f

**>= 3f+2**

* But the highest possible number of votes can only be N = 3f+1
* Thus a contradiction has arisen and our initial assumption that both X and Y received > 2f votes is wrong
  + More than two parties CANNOT simultaneously receive more than 2f votes
* Thus a node can be sufficiently confident of the voting winner when it receives at least 2f+1 same votes (or same messages).
* The requirement for PBFT at “prepared” and “committed” stages is thus made that at least 2f+1 replies must be of the same message.

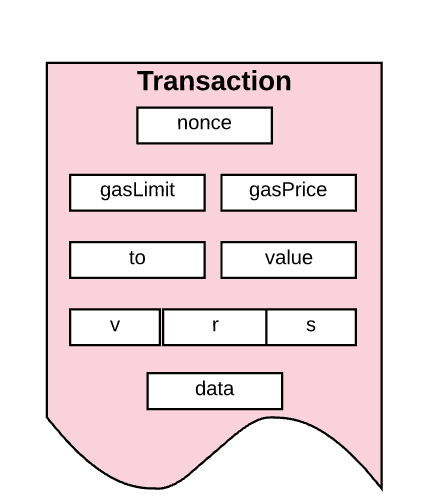
**Question 2. [10 Points] In the following selfish mining attack given by Eyal and Sirer, My pool means the selfish minor and others means honest minors. (1) Explain the meanings of lines 22, 23, and 24. (2) In line 23, why does the selfish minor need to publish all the private chain?**



**Answer:**

* The scenario laid out through lines 14--27 are if the honest miners are able to mine a new block first, from state 0.
* Once the honest miners find a new block, they immediately broadcast and notify publicly to all other nodes.
* Meanwhile, the private chain maintained by the selfish miner might have private blocks that secretly compete with the honest miner’s public chain.
* Lines 22-24:
  + Before the addition of the new honest miner’s block, if the length of the private chain maintained by the selfish miner is greater than the public chain by 2 blocks, they now have a lead of 1 block!
  + This means that the selfish miner pool can safely broadcast about their *longer* private chain which will automatically be accepted by all other nodes as the canonical chain, since this is now the longest chain in the network
  + **Thus at this step, the selfish miner publishes their entire private chain to announce their longer chain and sweep rewards.**
  + Honest miner’s computational work has been wasted, their blocks and rewards invalidated.
* As explained, the selfish miner must publish their entire chain to prove to the entire network and all nodes/miners that they have the current longest chain in the network.
* They must do this immediately to prevent a possibility that the honest miner finds another block and the algorithm goes back to line 20.

**Question 3. [10 Points] The following figure describes how a transaction of Ethereum 1.0 looks like. What is the roles of v? Explain in detail.**



**Answer:**

* **‘v’** is the Recovery Identifier.
  + In Ethereum transactions, sender’s address is not part of the transaction to reduce the payload size and not burden the blockchain/miners
  + It is used to accurately determine which point to be considered when recovering the Ethereum address from the ‘r’ and ‘s’.
  + It can have only two values that indicate the odd-y or even-y point to be considered:
    - 27 and 28
* **‘r’ and ‘s’** are the Elliptic curve equation parameters.
  + They are used to calculate the two possible cartesian points (x, y) by which the Ethereum address can be constructed.
  + Since there are two possibilities, with the help of **v**, the single point can be recovered.

**Question 4. [10 Points] In Ethereum 1.0, D(H) means the difficulty of Block header H. (1) Explain the role of y value. (2) Explain the role of .**



**Answer:**

* **‘y’** indicates whether the current block’s parent has an ommer/uncle block attached or not.
  + If y = 1, the uncle block is not present in the current block’s parent
  + Else, there is/are uncle block(s) present
  + ‘y’ is used to determine *ς2*, which is the weight of adjustment of difficulty during mining a block
* **ε** is the exponential difficulty symbol.
  + After block #5,000,000 It increases exponentially after every 100,000 blocks
  + **ε** was introduced as a push towards Ethereum 2.0 which is Proof of Stake based and not Proof of Work.
  + With exponentially increasing difficulty in Eth 1.0 due to **ε**, mining will eventually become impossibly difficult and thus discourage miners to continue with the PoW mechanism.
    - Due to environmental and power saving reasons.

**Question 5. [10 Points] In Ethereum 1.0, 1/64th Gas Reduction is introduced. Why not 1/128 or 1/32? Explain the issues for each of both cases.**

**Answer:**

* The EVM or Ethereum Virtual Machine, that performs the low-level blockchain-based actions and transactions, has a call-stack depth limit of 1024.
  + Commands that are used by the contract to call and reference *other* contracts must allocate a maximum amount of gas (specifically, g\*63/64)
  + This maximum limit is kept to ensure that gas runs out before the command even reaches the maximum call-stack limit of 1024.
* After reaching this limit, the calling contract request is ignored by the EVM.
* If this happens at scale, this can become a functional vulnerability and a possible attack vector on EVMs, wherein they perform contract request executions without properly validating the request or contract.
* **1/128:**
  + Calling other contracts from a contract will become too impractically expensive due to higher increased max-gas limits.
  + *Not suitable.*
* **1/32:**
  + This max-gas limitation would not be sufficient for it to run out before reaching 1024 blocks
  + There would still be gas left to invoke 1024+ call-stacks.
  + *Not suitable.*