COL867: Major Exam

Max. Marks: 60, May 8th 2018, Duration: 1 hour

1. (14 marks) Explain the following about replicated services and Byzantine fault tolerance.

   (a) (2 marks) Define the terms Safety and Liveness for a replicated service. You need not give a lengthy explanation. Simple definitions will suffice.

   (b) (4 marks) Byzantine Fault Tolerant protocols assume that the number of Byzantine nodes f is less than one-third of the total number of nodes n. Explain why this assumption is necessary for safety and liveness with an example involving writing and reading of a variable in a replicated state machine.

   (c) (4 marks) The Practical Byzantine Fault Tolerant (PBFT) protocol uses Quorums. Define what a Quorum is and prove the Intersection Property of Quorums.

   (d) (4 marks) In Zyzzyva, suppose a client sends a request and after a timeout the client gets between $(2f+1)$ and $3f$ consistent replies from nodes. What message does it send out next? Explain what each field in the message contains and which part of messages are signed by whom. You can use the format $< field1, field2, \ldots >_\sigma$ for the messages, where σ refers to a signature.

2. (10 marks) Explain the following about Algorand.

   (a) (4 marks) Explain what a Verifiable Random Function (VRF) is by stating what its inputs and outputs are. Give a practical example using signatures and hash functions.

   (b) (3 marks) Give the pseudocode for the Sortition procedure. State clearly what the inputs and outputs are. You need not give any lengthy explanation, just the pseudocode is sufficient.

   (c) (3 marks) Explain how Sortition reduces the ability of an adversary to launch a denial-of-service (DoS) attack on the committee selected by Sortition.

3. (10 marks) Explain the following about Bitcoin-NG.

   (a) (2 marks) Bitcoin-NG generates two types of blocks, key-blocks and microblocks. Explain who is allowed to generate each type of block and what are the contents of each type of block.

   (b) (3 marks) How does Bitcoin-NG increase the throughput (average number of transactions per second) and reduce latency (time between when a transaction is broadcast and when it appears in a block) compared to Bitcoin? Explain whether or not Bitcoin-NG decreases the confirmation time (time between when a transaction appears on the blockchain and when a user is certain it will be in the chain with high probability) compared to Bitcoin.

   (c) (5 marks) Consider a modified Bitcoin-NG in which each microblock is required to have proof-of-work (PoW) equal to a fraction $\alpha \in (0, 1]$ of the PoW of a key-block, with everything else in the protocol remaining the same. In other words, if the hash of a key-block must be less than threshold τ, then the hash of a microblock must be less than τ/α. Suppose a particular key-block is created by a miner who has hashing power β

fraction of the total hashing power in the network. How many microblocks is this miner likely to generate *on average* before the next key-block is created? (You will get 2 bonus marks if you give the entire *probability distribution* of the same quantity.) What are the consequences for the throughput and latency while this miner is generating microblocks? In what scenario will this modified Bitcoin-NG have throughput close to zero?

4. (10 marks) Explain the following about computationally intensive transactions (CIT) and Truebit.

   (a) (3 marks) For a CIT in Bitcoin or Ethereum, miners have a *Verifier's Dilemma*. Explain what this dilemma is and why it occurs.

   (b) (1 marks) How does Truebit determine who is the Solver for a given CIT?

   (c) (6 marks) Truebit uses the value of a bit to decide whether the Solver points to the correct or wrong solution submitted. Explain the following with a diagram depicting the blockchain. How is the value of the bit decided? How is it ensured that the Solver does not know the bit value before submitting his two solutions? How does the Solver get to know the value of the bit before anyone else? When do all miners become aware of the value of the bit?

5. (6 marks) In the Lightning Network, commitment transactions contain Revocable Sequence Maturity Contracts (RSMC). Explain what an RSMC is and how it can be used to prevent someone from broadcasting an old commitment transaction.

6. (10 marks) Answer the following briefly. The answer to each sub-question is not expected to be more than 1 page in length.

   (a) (5 marks) Traditional blockchains such as Ethereum first order transactions and then execute them. This leads to sequential execution of smart contracts. How does Hyperledger allow parallel execution of smart contracts? Explain by describing the roles of Orderers and Endorsers.

   (b) (5 marks) In Fruitchain, miners can try to create blocks and fruits simultaneously. State what fields a block contains and what fields a fruit contains. Explain the process of creating a block or a fruit.