Biskra University

Computer Science Department

Exam: BT-2024-GLSD… Family name: ……//////…….. First name: ……./////…….

Questions: 10/10

1) Mention three basics sciences that are required to understand and to implement Blockchain? **Distributed Systems, Cryptography, Algorithmics and data structures**
2) Why Blockchain was seen as a revolution against the capitalist system? **No need for banks. Transactions peer to peer**
3) Mention the basic parts of a block in bitcoin blockchain: **Block Identifier, Block Header, Transaction**
4) What means a fork in blockchain? **a new path of the blockchain**
5) Why the problem of forks appears in bitcoin and how it appears? **when two miners build correct blocks at the same time and they are considerd by different nodes separately**
6) How the problem of forks is resolved in bitcoin blockchain?**Adopt the longest chain**
7) Which protocol is used in bitcoin? **PoW (Proof of works)**
8) What is the basic problem of this protocol? **requires computing power**
9) In bitcoin, mention the types of nodes (components) involved in the building of blocks: **miners**
10) How a node proves that it has built a correct block? **compute the nounce**
11) Who is responsible of the validation of a block which was built by some node in bitcoin blockchain? **miners**
12) Give the steps required from some node to validate a block which was built by another node: **Check the previous block; Check the nonce; check the transactions,**
13) For a client who sent a transaction, when his transaction is considered validated? And what is the estimated time for that? **Almost after the validation of three blocks, so 10*3=30minutes almost**
14) The previous time is it long? If yes, why this time is so long? **Yes. It is long because finding a nonce requires time**
15) Mention a blockchain where the time has been reduced compared to the bitcoin blockchain: **Ethereum**
16) What means a problem of double-spending in bitcoin blockchain? **A client uses the same amount to make more than one transaction**
17) At which levels, cryptography is used in bitcoin blockchain? **Computing keys (Private and Public), encryption of transaction, signatures,**
18) At which levels, hashing is used in bitcoin blockchain?

- **To compute the hash of the block**
- **To check the nonce of a built block**
- **To compute the merkle tree**

Exercise: **10/10**

In this exercise, you will use a ***sequence like diagram*** to show how the system components interacts. Each node in the blockchain (BC) has a life line which models its **intern actions** and **external interactions** as well as a **copy of the blockchain**. The evolution is represented as a sequence of steps, and you are asked to model the system in each step.

1) Step1: BCis initially composed **of three miners**. m1, m2, m3.
2) Step2:
   - User u1 sends a transaction t1
   - User u2 sends a transaction t2

3) Step3: m1 builds a block and broadcast it, m2 and m3 validate the block. Do the necessary and update the blockchain!
4) Step4: miner m4 joins the blockchain
5) Step5: user u3 joins the blockchain and sends transaction t3, then user u1 sends transaction t4, then user 2 send transaction t5.
6) Step 6: m1 and m2 builds two blocks(at the same time, maybe), broadcast their blocks. We admit that the block of m1 reaches m3, m4 before the block of m2. Do the necessary and update the blockchain!

RK: Don’t miss the transactions pool. It can be added as a component of the blockchain.

	M1	**M2**	**M3**	**Pool of transactions**				
Step1	BC= B0	BC= B0	BC= B0					
Step2				t1, t2	**U1** Send t1	**U2** Send t2		
Step3	BC=B0 - Build block1 - Broadcast block1 BC= B0->B1(t1,t2)	BC= B0 - Gets block1 - Validate block1 - Add it BC= B0->B1(t1,t2)	BC= B0 - Gets block1 - Validate block1 - Add it BC= B0->B1(t1,t2)					
Step4							**M4** - Get the BC BC= B0->B1(t1,t2)	
Step5				t3, t4, t5	Send t4	send t5		**U3** send t3
Step6	-Build block 2 B2(t3,t4,t5) -Broadcast B2 BC= B0-> B1(t1,t2)-> B2(t3,t4,t5)	-Build block 2 B2’(t3,t4,t5) -Broadcast B2’ BC= B0-> B1(t1,t2)-> B2(t3,t4,t5)	Get B2 Check B2 Validate B2 Add B2 BC= B0->B1(t1,t2)-> B2(t3,t4,t5) Get B2’ Check B2’ Reject B2’				Get B2 Check B2 Validate B2 Add B2 BC= B0-> B1(t1,t2)-> B2(t3,t4,t5) Get B2’ Check B2’ Reject B2’	