Indian Institute of Technology Jodhpur

Department of Computer Science and Engineering

Course: CSL7490: Introduction to Blockchain

Miner Examination-2

Max. Marks: 20 **Time: 01:00 Hour**

Note:

1. **Draw the diagrams wherever required**
2. **Assume the data, if required.**
3. **The word limit to answer the questions**
    a. **For Fill in the blanks up to 100 words**
    b. **For Short Answer type questions 200-300 words**

Q.1	**Fill in the blanks with a proper justification.** 1. Once the data is confirmed and appended in the blockchain, then _____can access it. 2. Creation of an alternate version of the blockchain ledger is called _____. 3. Solidity is the _____ to develop _____ for the ethereum blockchain. 4. When 51% of computation is occupied by an attacker in PoW, then it is called _____ attack. 5. Let two miners have created the two blocks at the same time, i.e., the new two blocks have the same parent. Following the longest chain rule, only one block is added to the existing blockchain ledger, and then the other block will be called _____.	**1X5**
Short answer type questions		
Q.2	Write at least two advantages of private blockchain over the public blockchain.	**3**
Q.3	Explain what the byzantine problem is. Describe one of the blockchain protocols which is used to solve this problem. **Or** What is the longest chain rule? Describe in which scenarios this longest chain rule applied.	**2**
Q.4	The company you work for is considering introducing blockchain technology for banking software development. To do this, they have considered the Ethereum Blockchain as suitable blockchain technology. To develop banking software using the ethereum blockchain, you need to create 2 smart contracts for customer KYC and transfer of money. Answer the following: 1. What is a smart contract? Why is a smart contract suitable for developing banking software?	**3**

<table>
<tr>
<td>Q.5</td>
<td>Complete the following blank table and justify your answers.
PoW: Proof of Work, PoS: Proof of Stake, DPoS: Delegated proof of stake, BFT: Byzantine fault tolerance, DAG: Directed Acyclic Graph

<table>
<tr><th>Features</th><th>PoW</th><th>PoS</th><th>DPoS</th><th>BFT</th><th>DAG</th></tr>
<tr><td>Energy Consumption</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Throughput (Transaction per Seconds)</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Structure</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>Example</td><td></td><td></td><td></td><td></td><td></td></tr>
</table>
</td>
<td>4</td>
</tr>
<tr>
<td>Q.6</td>
<td>In the various phases of the blockchain working, describe which cryptographic technique is used and why. The phases are as follows: Initialization and broadcasting, Validation of transaction, and chaining of Blocks.</td>
<td>3</td>
</tr>
</table>

Answers:

Q.1 Fill in the blanks

1. All the nodes or open to all
2. Fork
3. Programming language, smart contract
4. 51%
5. Orphan Block

Q.2 Advantages of Private Blockchain over the Public blockchain.

1. The consortium or company running a private blockchain can easily, if desired, change the rules of a blockchain, revert transactions, modify balances, etc. In some cases, e.g. national land registries, this functionality is necessary; there is no way a system would be allowed to exist where Dread Pirate Roberts can have legal ownership rights over a plainly visible piece of land, and so an attempt to create a government-uncontrollable land registry would in practice quickly devolve into one that is not recognized by the government itself. Of course, one can argue that one can do this on a public blockchain by giving the government a backdoor key to a contract; the counter-argument to that is that such an approach is essentially a Rube Goldbergian alternative to the more efficient route of having a private blockchain, although there is, in turn, a partial counter-argument to that that I will describe later.
2. The validators are known, so any risk of a 51% attack arising from some miner collusion in China does not apply.
3. Transactions are cheaper since they only need to be verified by a few nodes that can be trusted to have the very high processing power, and do not need to be verified by ten thousand laptops. This is a hugely important concern right now, as public blockchains tend to have transaction fees exceeding $0.01 per tx, but it is important to note that it may change in the long term with scalable blockchain technology that promises to bring public-blockchain costs down to within one or two orders of magnitude of an optimally efficient private blockchain system
4. Nodes can be trusted to be very well-connected, and faults can quickly be fixed by manual intervention, allowing the use of consensus algorithms which offer finality after much shorter block times. Improvements in public blockchain technology, such as Ethereum 1.0's uncle concept and later proof of stake, can bring public blockchains much closer to the "instant confirmation" ideal (e.g. offering total finality after 15 seconds rather than 99.9999% finality after two hours as does Bitcoin), but even still private blockchains will always be faster, and the latency difference will never disappear as unfortunately the speed of light does not increase by 2x every two years by Moore's law.
5. If read permissions are restricted, private blockchains can provide a greater level of, well, privacy.

Q.3

Byzantine General Problem: The Byzantine Generals Problem is a game theory problem that describes how difficult it is for network node parties to reach a consensus without the help of a trusted central party. How can network nodes collectively agree on a specific value in a network when no member can verify the identity of other members?

The practical byzantine fault tolerance (PBFT), Proof of Work (PoW), Proof-of-stake (PoS) and Delegated proof-of-stake (DPoS) are some of the blockchain protocols that solve the problem of Byzantine general problem.

The student should describe any protocol to defend how these protocols solve the problem in 4-5 lines or 150-200 words.

Q.4 SmartContract: Smart contracts are simply programs stored on a blockchain that run when predetermined conditions are met. They are typically used to automate the execution of an agreement so that all participants can be immediately certain of the outcome without any intermediary's involvement or time loss. They can also automate a workflow, triggering the next action when conditions are met.

Smart contracts follow simple "if/when…then…" statements written into code on a blockchain. A network of computers executes the actions when predetermined conditions have been met and verified. These actions could include releasing funds to the appropriate parties, registering a vehicle, sending notifications, or issuing a ticket. The blockchain is then updated when the transaction is completed. That means the transaction cannot be changed, and only parties who have been granted permission can see the results.

Within a smart contract, there can be as many stipulations as needed to satisfy the participants that the task will be completed satisfactorily. To establish the terms, participants must determine how transactions and their data are represented on the blockchain, agree on the "if/when...then…" rules that govern those transactions, explore all possible exceptions, and define a framework for resolving disputes.

Then the smart contract can be programmed by a developer – although increasingly, organizations that use blockchain for business provide templates, web interfaces, and other online tools to simplify structuring smart contracts.

Why Smart Contracts are suitable for Banking:

Speed, efficiency and accuracy
Once a condition is met, the contract is executed immediately. Because smart contracts are digital and automated, there's no paperwork to process and no time spent reconciling errors that often result from manually filling in documents.

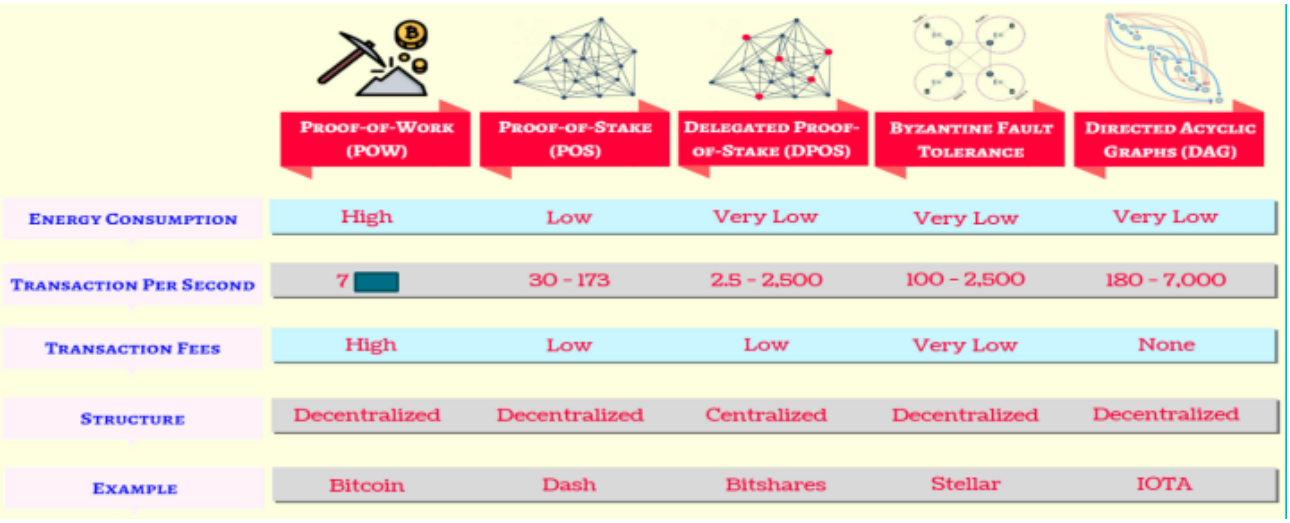
Trust and transparency
Because there's no third party involved, and encrypted transaction records are shared across participants, there's no need to question whether information has been altered for personal benefit.

Security
Blockchain transaction records are encrypted, which makes them very hard to hack. Moreover, because each record is connected to the previous and subsequent records on a distributed ledger, hackers would have to alter the entire chain to change a single record.

Savings

Smart contracts remove the need for intermediaries to handle transactions and, by extension, their associated time delays and fees

Q.5



	Proof-of-Work (POW)	Proof-of-Stake (POS)	Delegated Proof-of-Stake (DPOS)	Byzantine Fault Tolerance	Directed Acyclic Graphs (DAG)
Energy Consumption	High	Low	Very Low	Very Low	Very Low
Transaction Per Second	7	30 - 173	2.5 - 2,500	100 - 2,500	180 - 7,000
Transaction Fees	High	Low	Low	Very Low	None
Structure	Decentralized	Decentralized	Centralized	Decentralized	Decentralized
Example	Bitcoin	Dash	Bitshares	Stellar	IOTA

Q.6