MDS6117, Spring 2022 Sample Midterm Examination

Part I: True/False Questions (4 point each, 20 points total)

1. **(T)** The structure of chained blocks gives blockchain the tamper-proof property that is difficult to implement in the relational data structure.
2. **(F)** Consortium blockchain is an instance of Blockchain 1.0.
3. **(T)** Multiple network nodes in Bitcoin help make blockchain difficult to attack.
4. **(T)** Ethereum is a system that is Turing-complete because it can be used to create blockchains.
5. **(F)** Domain specific blockchain languages include C++.

Part II: Multiple Choice (4 points each, 20 points total)

Note that the best answer to a question is not necessarily a definition, but the most suitable answer.

1. The following is a blockchain consensus algorithm:
   a. proof-of-work b. proof-of-time c. queueing algorithm d. payment-of-stake

2. A Merkle tree is an index used to:
   a. Speed up database queries.
   b. Store blockchain procedures.
   c. Ensure security in Hyperledger Fabric.
   d. **Verify blockchain transactions.**

3. Which of the following is NOT a property of Bitcoin blockchain?
   a. Tamper-proof
   b. History of transactions
   c. Encryption of user names
   d. Hash values

4. The chronological order of blockchain evolution is:
   a. Ethereum → Quorum → Bitcoin
   b. Bitcoin → Ethereum → Fabric
   c. Bitcoin → Quorum → Ethereum
   d. Fabric → Bitcoin → Ethereum

5. A blockchain is ___________.
   a. a representation of world state in a business network.
   b. a chain of blocks that contain transaction records
   c. a collection of related data records.
   d. a collection of data tables.

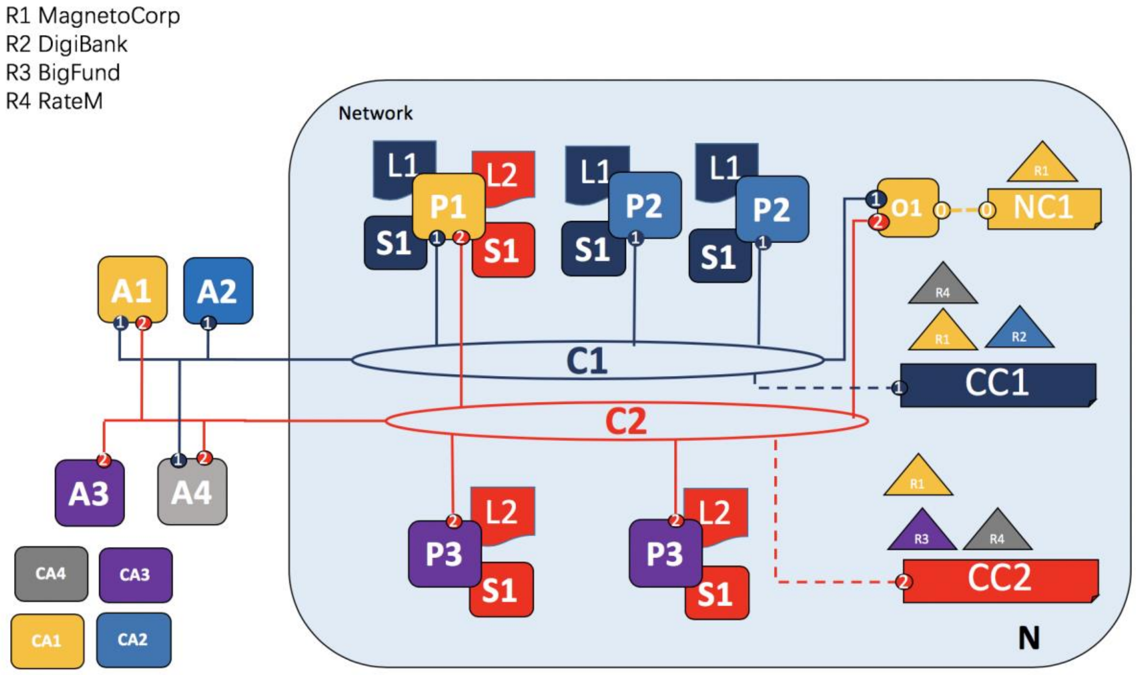
Part III: Enterprise Business Network Diagram (20 points total):

Four organizations, which form two consortiums, decide to build a blockchain based on Hyperledger Fabric. MagnetoCorp and DigiBank form consortium X1, while MagnetoCorp and BigFund form consortium X2. RateM does not participate in transactions. In Table 1, you can find the number of peer nodes provided by the organizations participating in transactions. MagnetoCorp is the network initiator and governs the ordering service.

Users from MagnetoCorp can issue, redeem, and query commercial paper. Users from DigiBank and BigFund can buy, sell, query and transfer commercial paper. Users from RateM can only query commercial paper.

Table 1. Details about the blockchain based on Hyperledger Fabric

	MagnetoCorp	DigiBank	BigFund	RateM
Transaction Types	Issue, redeem, query	Buy, sell, query	Buy, sell, query	Query
Number of peer nodes	1	2	2	-
Number of Users	10	5	5	2



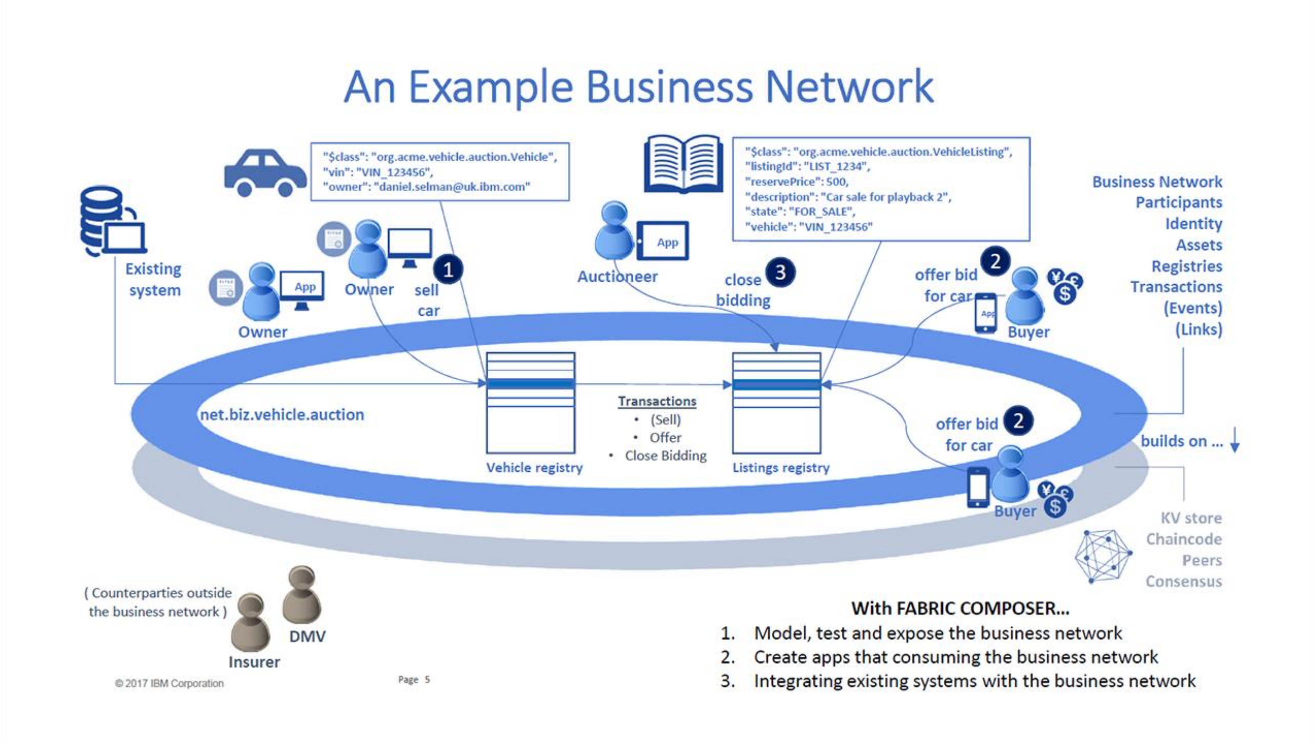
Given the Blockchain Network Diagram above using the 11 Elements explained in the tutorials of this course, please explain the diagram carefully, assuming that you are trying to explain it to a new blockchain developer.

(Suggested answer)

- Four organizations in the network: R1, R2, R3 and R4.
- R1 is the network initiator with network configuration NC1.
- R4 does not do transactions but only query information.
- Two channels: C1 for R1, R2 and R4 and C2 for R1, R3 and R4.

- Four Applications, A1 to A4 for R1 to R4, respectively.
- A1 does issue/redeem/query on C1 and C2, A2 (A3) does buy/sell/query on C1 (C2), and A4 does query on C1 and C2.
- Peer node P1 maintains ledger L1 in C1 and ledger L2 in C2, and Peer node P2 (P3) maintains ledger L1 (L2).
- Network N is governed with NC1 controlled by R1.
- Channel C1 (C2) is governed by channel configuration CC1 (CC2) and controlled by R1, R2, R4 (R1, R3, R4).
- Ordering service O1 is for network N under the system channel and supports channels C1 and C2.
- Each of {R1, R2, R3, R4} has a preferred Certificate Authority.

Part IV: Hyperledger Blockchain Design (20 points total)



An Example Business Network

```
"$class": "org.acme.vehicle.auction.Vehicle",
"vin": "VIN_123456",
"owner": "daniel.selman@uk.ibm.com"
```

```
"$class": "org.acme.vehicle.auction.VehicleListing",
"listingId": "LIST_1234",
"reservePrice": 500,
"description": "Car sale for playback 2",
"state": "FOR_SALE",
"vehicle": "VIN_123456"
```

With FABRIC COMPOSER...

1. Model, test and expose the business network
2. Create apps that consuming the business network
3. Integrating existing systems with the business network

Given the business network above, what elements do you see that can be modelled with an Enterprise Business Network model in Hyperledger Composer and how. Please apply what you have learned in the lectures and the labs.

(Suggested answer)

In the Example Business Network, three types of elements can be modelled in Composer:

Assets: Vehicles, Listings

Participants: Owner, Auctioneer, Buyer

Transactions: Register, Sell, Offer, Close Bidding

General Transaction Flow is shown below:

1) The car owner runs register function by submitting the information about the vehicle, where the original owner will fill in the VIN and initiate the class: org.acme.vehile.auction.Vehicle. The ownership will automatically be certified with the owner’s identity. (Possible verification from DMV/Insurer)

2) In the Vehicle registry, entries will be created accordingly whilst Step 1 is done. Or the record is directly imported from the existing system.

3） Next, listing registry will be updated when the seller uses the sell function and the auction begins. Information such as description from Vehicle Registry will be used in an entry of listing. The listing entry also entails the reserve price, listingId. Also, class:org.acme.vehicle.auction.VehicleListing will be instantiated. And the state for the listing is marked as FOR_SALE.

4) Then, buyers can browse the current available listings and offer bid for their interests with Offer function.

5) Finally, the auctioneer announces the close of the auction by function Close Bidding. The state of this listing is then set as CLOSED. The deal is either successfully made with the best offer or the reserve price has not been reached. This transaction flow is ended. (In this step, the insurance/ownership may be updated to outside counterparties such as DMV or Insurer)

Part V: Short answer questions (10 points each, 20 points total)

1. What is machine trust, and how does blockchain achieve machine trust?

Machine trust is a term mentioned in the Economist’s article on Oct 31, 2015 -- *The Trust Machine*. In general, machine trust is to use computer algorithms to guarantee certain governance procedure without human interference. For instance, Bitcoin uses the proof-of-work consensus algorithm to select bookkeepers and ensure accurate maintenance of the Bitcoin accounts and exchanges.

2. Discuss the importance of nonce in the consensus algorithm under proof-of-work.

Nonce is a number that used to achieve a given pattern of Hash value in the proof-of-work process. Determinacy of a particular nonce requires brute-force computation that can take about 10 minutes with a powerful mining computer under certain Bitcoin mining difficulty. This time-consuming process of proof-of-work helps make Bitcoin tamper-proof, and that is why Bitcoin has been running successfully over the past 12 years.