CBCS SCHEME

USN | 2 | V | D | 2 | 2 | C | S | 0 | 53 |

BCS613A

Sixth Semester B.E./B.Tech. Degree Examination, June/July 2025

Blockchain Technology

Time: 3 hrs. Max. Marks: 100

Note: 1. Answer any FIVE full questions, choosing ONE full question from each module.
2. M : Marks , L: Bloom's level , C: Course outcomes.

		Module – 1	**M**	**L**	**C**
Q.1	**a.**	Define Blockchain and explain centralized, decentralized and distributed systems with a suitable diagram.	**05**	**L2**	**CO1**
	b.	Explain the generic structure of a block with a diagram.	**05**	**L2**	**CO1**
	c.	Discuss the growth of the blockchain with an Architecture / network view of blockchain with a neat diagram.	**10**	**L2**	**CO1**
		OR			
Q.2	**a.**	Illustrate the Byzantine General Problem with a suitable example.	**05**	**L2**	**CO1**
	b.	Describe about CAP theorem in block chain.	**05**	**L2**	**CO1**
	c.	Why are Consensus Algorithm needed in Blockshain? Explain in detail.	**10**	**L2**	**CO1**
		Module – 2			
Q.3	**a.**	Explain the methods of decentralization in detail.	**10**	**L2**	**CO2**
	b.	Write an algorithm for working of SHA- 256	**10**	**L3**	**CO2**
		OR			
Q.4	**a.**	Write the steps involved in RSA key pair generation with an example.	**10**	**L3**	**CO2**
	b.	Illustrate with a diagram point addition in Elliptic Curve Cryptography.	**10**	**L2**	**CO2**
		Module – 3			
Q.5	**a.**	Explain transaction life cycle in a Bit coin system.	**10**	**L2**	**CO3**
	b.	Discuss the different types of transaction in Bit Coin.	**10**	**L3**	**CO3**
		OR			
Q.6	**a.**	What is the wallet in bit coin? Explain in detail about the different types of wallet with example.	**10**	**L2**	**CO3**
	b.	Write a short note on : Privacy and Anonymity.	**10**	**L2**	**CO3**
		Module – 4			
Q.7	**a.**	What are the two types of accounts that exists in Ethereum. Explain.	**10**	**L2**	**CO4**
	b.	With a neat bowtie model diagram explain Ricardian contracts.	**10**	**L2**	**CO4**
		OR			
Q.8	**a.**	Explain any five standard fields in Ethereum transaction.	**10**	**L2**	**CO4**
	b.	Write a short note on Ethereum virtual machine.	**10**	**L2**	**CO4**
		Module – 5			
Q.9	**a.**	Explain the architecture and key components of Hyperledger Fabric.	**10**	**L2**	**CO5**
	b.	Compare and contrast Hyperledger Fabric and Hyperledger sawtooth in terms of architecture consensus and user.	**10**	**L3**	**CO5**
		OR			
Q.10	**a.**	What is Hyperledger? Discuss its objectives, structure as a protocol suite and list key projects under the hyperledger umbrella with a brief description of each.	**10**	**L2**	**CO5**
	b.	Discuss the architecture of corda. What makes it suitable for financial institutions and how does it handle consensus and privacy?	**10**	**L3**	**CO5**

* * * * *

KLS VDIT HALIYAL

DEPT. OF COMPUTER SCIENCE & ENGG.

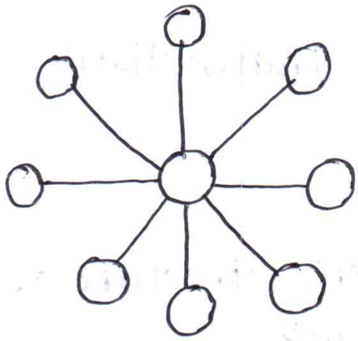
SCHEME OF EVALUATION.

SUB :- BLOCKCHAIN TECHNOLOGY. BCS613A. M.Marks 100.

1.a) Defn : Blockchain consists of list of records. It is a peer to peer distributed ledger that is cryptographically secure, append only, immutable and updateable only via consensus among peers.

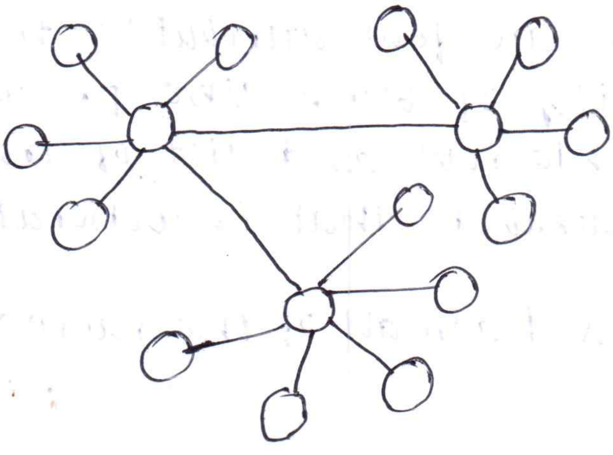
i) Centralized

- Centralized systems are conventional IT systems in which there is a single authority that controls the system



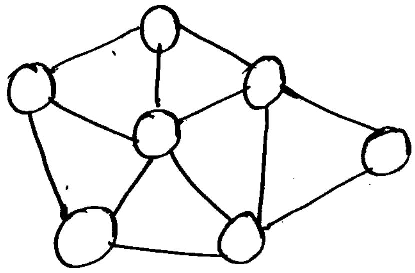
ii) Decentralized

- A decentralized syetem is a type of network where nodes are not dependent on a single master node, instead control is distributed among many nodes.



iii) Distributed systems

- A distributed system ,data and computation are spread across multiple node in the network.



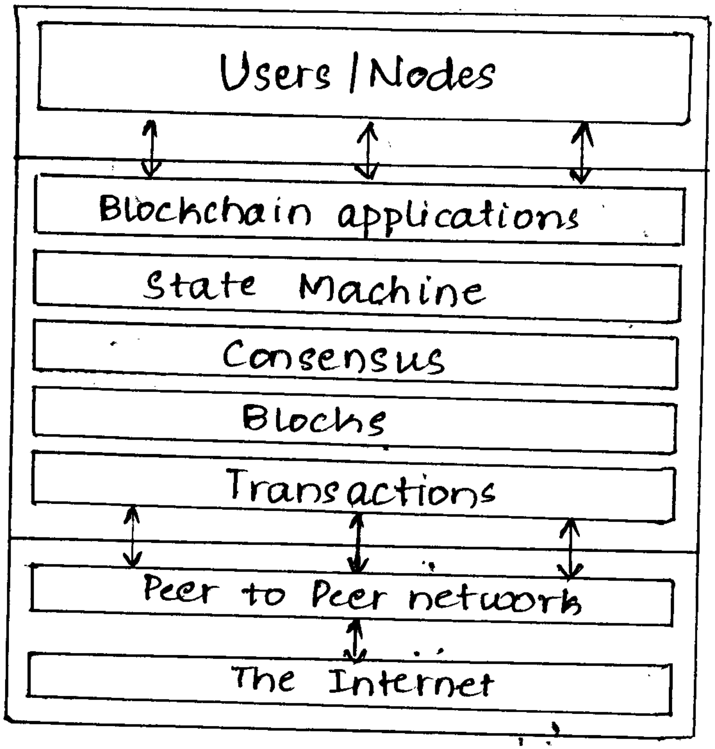
1.b)

Pointer to Previous block's hash
Nonce.
Time stamp
Merkle Root
List of Transactions

The generic structure of a block.

- A block is merely a selection of transactions bundled together and organized logically.
- The structure of a block is also dependent on the type and design of a blockchain.
- Generally, there are few attributes that are essential to the functionality of block like previous block, nonce, time stamp, merkle root and list of transactions.
- A nonce is a number that is generated and used only once.
- Merkle root is a hash all of the nodes of a merkle tree.

1.c)

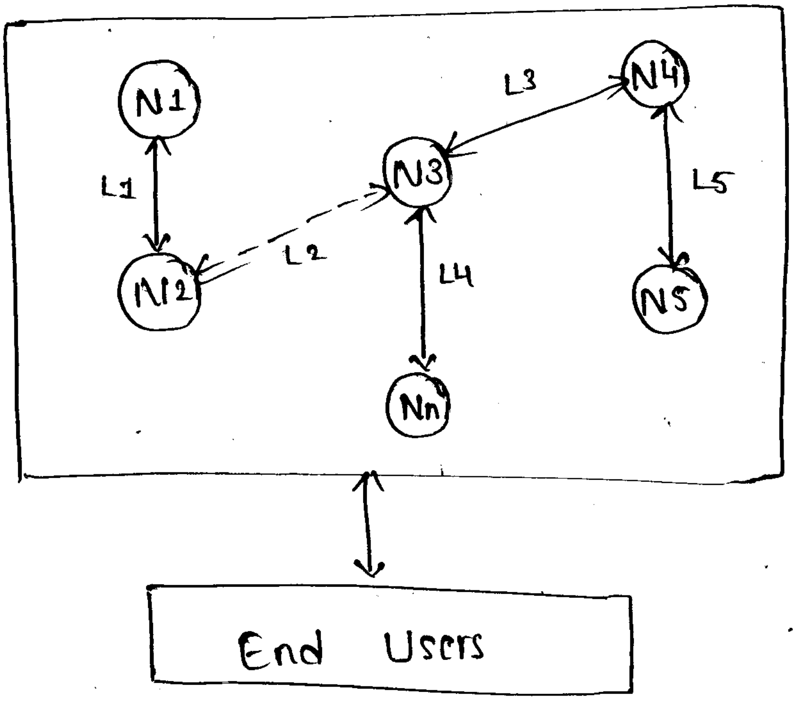


The network view of blockchain

- Blockchain can be thought as a layer of a distributed peer to peer network running on the top of a internet.
- At the bottom layer in the preceding diagram, there is the internet, which provides a basic communication layer for any network.
- In this case, a peer to peer network runs on top of the internet, which hosts another layer of blockchain.
- That layer contains transactions, blocks, consensus, mechanisms, state machines and blockchain smart contracts.
- All of these components are shown as single logical entity in a box, representing blockchain above the peer to peer network.
- Finally, at the top, there are users or nodes that connect to the blockchain and perform various operations such as consensus, transaction verfication and processing.
- A block is made up of transactions, and its size varies depending on the type and design of the blockchain in use.

- A transaction is record of an event, for example, the event of transferring cash from a sender to receiver.

2.a)



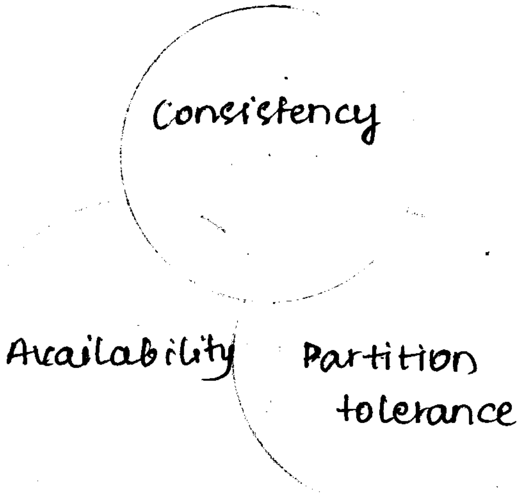
- In the diagram nodes (N1, N2, N3 - - Nn) are like generals and the links (L1-L5) are their communication lines, End users send requests & all nodes must agree on a common decision.

- If one node (e.g. N3) becomes malicious, it may send different or false messages to other nodes (e.g., telling N4 "attack" and Nn "retreat") this creates confusion - the Byzantine Generals Problem.

- The solution is consensus mechanism that ensures all honest nodes (N1, N2, N4, N5 - -) agree on the same result, even if some nodes act dishonestly.

2.b) • CAP theorem, also known as Brewer's theorem, was introduced by Eric Brewer in 1998.

- The theory states that any distributed system cannot have consistency, availability and partition tolerance simultaneously.
- Consistency is a property which ensures that all nodes in a distributed system have a single, current and identical copy of the data.
- Availability means that the nodes in the system ar up, accesible for use, and are accepting incoming requests and responding with data without any failures as and when required. In other words, data is available at each node and the nodes are responding to requests.
- Partition tolerance ensures that if a group of nodes is unable to communicate with other nodes due to network failures, the distributed system continues to ~~theorem~~ operate correctly. This can occur due to network and node failures.



2.c Why?

- It is a fault tolerance mechanism.
- To achieve necessary agreement.
- It is useful in record keeping.

(POB) proof of Burn:

- It is used as an alternative method for distributed consensus to POW and POS.
- The aforementioned example for burning coins applies to a one-way pegged sidechain.
- The second type is called a two-way pegged sidechain, which allows the movement of coins from main chain to the sidechain.

(POW) proof of Work:

- This type of consensus mechanism relies on proof that adequate computational resources have been spent before proposing a value for acceptance by the network.
- This scheme is used in Bitcoin, Litecoin and other cryptocurrency blockchains.

(POS) proof of stake:

- this algorithm works on the idea that a node or user has an adequate stake in the system; that is the user has invested enough in the system so that any malicious attempt by that user would outweigh the benefits of performing such as attack on the network.

(POC) proof of capacity :

- This scheme uses hard disk space as a resource to mine the blocks. This is different from POW where CPU resources are used.
- In POC, hard disk space is utilized for mining and as such is also known as hard drive mining.
- This concept was first introduced in the Burstcoin crytocurrency.

M-2

3.a) Methods of decentralization :

- Two methods can be used to achieve decentralization : disintermediation and competition.

i) Disintermediation :

- The concept of disintermediation can be explained with the aid of an example. Imagine that you want to send money to ~~the bank of~~ your friend in other country.
- You go to a bank who, for a fee, will transfer your money to the bank in that country.
- In this case, the bank maintains a central database that is updated, confirming that you have sent the money. With block chain technology, it is possible to send this money directly to your friend without the need for a bank.
- All you need is the address of your friend on the blockchain. This way, the intermediary; that is the bank is no longer required, and decentralized is achieved by disintermediation.

ii) contect - driven decentralization (competition)

- In the method involving competition, different service providers compete with each other in order to be selected for the provision of services by the system.
- This paradigm does not achieve complete decentralization. However, to a centain degree, it ensures that an intermediary or service provider is not monopolizing the service.
- In the context of blockchain technology, a system can be envisioned in which smart contracts can choose an external data provider from large number of providers based on their reputation, previous score, reviews and quality of service.
- This method will not result in full decentralization but it allows smart contracts to make a free choice based on the criteria just mentioned.

3b) SHA-256 has the input message size < 2^{64}-bits. Block size is 512 bits, and it has a word size of 32-bits. The output is a 256-bit digest.

- There are two main components of this function:

Prepoccinge:-

1. Padding of the message is used to adjust the length of a block to 512-bits if it is smaller than the required block size of 512 bits.

2. Parsing the message into message blocks, which ensures that the message and it's padding is

divided into equal blocks of 512 - ~~blocks~~ bits.

3. Setting up the initial hash value, which consists of the eight 32-bit words obtained by taking the first 32-bits of the fractional parts of square roots of the first eight prime numbers. These initial values are randomly chosen to initialize the process, and they provide a level of confidence that no backdoor exists in the algorithm.

2. Hash computation:

4. Each message block is then processed in a sequence, and it requires 64 rounds to compute the full hash output. Each round uses slightly different constants to ensure that no two rounds are the same.

5. The message schedule is prepared.

6. Eight working variables are initialized.

7. The intermediate hash value is calculated.

8. Finally, the message is processed, and the output hash is produced.

(OR)

4.a) An RSA key pair is generated by performing the following steps:

1. Modulus generation:

- select p and q, which are very large prime numbers
- Multiply p and q, $n = p \cdot q$ to generate modulus n.

2. Generate co-prime :
   - Assume a number called e.
   - e should satisfy a certain condition; that is, it should be greater than 1 and less than $(p-1)(q-1)$. In other words, e must be number such that no number other than 1 can divide e and $(p-1)(q-1)$. This is called co-prime, that is, e is the co-prime of $(p-1)(q-1)$.

3. Generate the public key:
   - The modulus generated in step 1 and co-prime e generated in step 2 is a pair together that is a public key. This part is the public part can be shared with anyone; however, p and q need to be kept secret.

4. Generate the private key:
   - The private key, called d here, is calculated from p, q and e. The private key is basically the inverse of e modulo $(p-1)(q-1)$. In the equation form, it is this as follows
   $ed = 1 \bmod (p-1)(q-1)$

5. RSA uses the equation to produce ciphertext:
   $C = P^e \bmod n$

6. Decryption in RSA is provided in the following equation:
   $P = C^d \bmod n$

Ex :

1. $p = 61$ $q = 53$

2. compute $n = p \times q$

   $n = 61 \times 53$

   $= 3233$

3. Compute Euler's totient

   $\varphi(n) = (p-1)(q-1) = 60 \times 52$

   $= 3120$

4. choose a public exponent e such that

   $1 < e < \varphi(n)$ and $\gcd(e, \varphi(n)) = 1$

   $e = 17$

5. Find the private exponent d

   $d \times e \equiv 1 \pmod{\varphi(n)}$

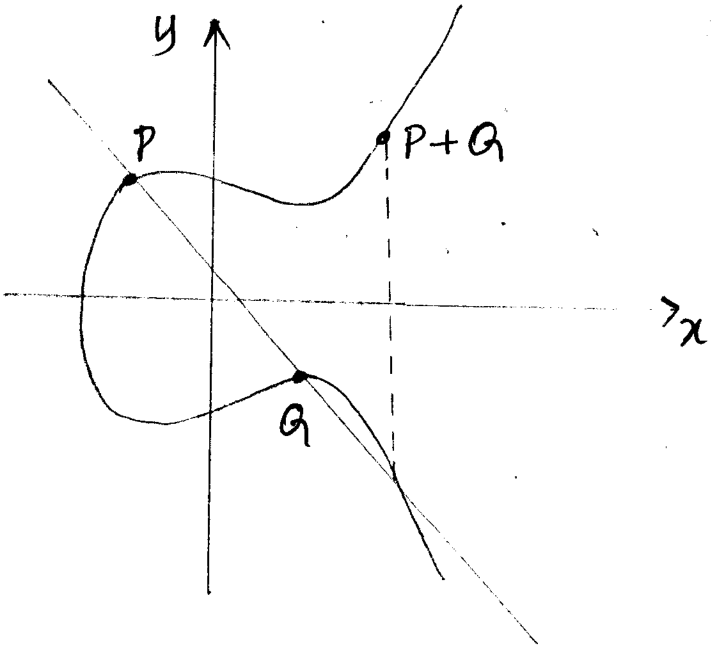
   $d = 2753$

   key pair is :

   public key $= (e = 17, n = 3233)$

   private key $= (d = 2753, n = 3233)$

4b) Elliieptic Curve Crytpography.



- Point addition is shown in the following diagram.
- This is a geometric representation of point addition on elliptic curve. In this method, a diagonal line is drawn through the curve that intersects the curve at two points P & Q, which yields a third point between the curve and the line.
- This points is mirrored as P+Q, which represents the result of the addition as R.

- The group operation denoted by the + sign for addition yields the following equation:

$$P + Q = R$$

- In this case, two points are added to compute the coordinates of the third point on the curve:

$$P + Q = R$$

- More precisely, this means that coordinates are added.

$$(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$$

- The equation of point addition is

$$X_3 = s^2 - x_2 - x_2 \bmod p$$

$$y_3 = s(x_1 - x_3) - y_1 \bmod p$$

- result,

$$S = \frac{(y_2 - y_1)}{(x_2 - x_1)} \bmod p.$$

M-3

5.a) The following steps describe the transaction lifecycle.

1. A user /sender sends a transaction using wallet software or some other interface.

2. The wallet software signs the transaction using the sender's private key.

3. The transaction is broadcasted to the Bitcoin network using a flooding algorithm.

4. Mining nodes who are listening for the transactions verify and include this transaction in the next block to be mined. Just before the transaction are placed in the block they are placed in a special memory buffer called transaction pool.

5. Mining starts, which is a process by which the blockchain is secured and new coins are generated as a reward for the miners who spend appropriate computational resources.

6. Once a miner solves the POW problem it broadcast the newly mined block to the network.

~~POW~~

7. The nodes verify the block and propagate & the block further, and confirmations start to generate.

8. Finally, the confirmations start to appear in the receiver's wallet.

Different types of Transaction in Bitcoin

5b) • Pay to Public key Hash (P2PKH):

P2PKH is most commonly used transaction type and is used to send transactions to the bitcoin addresses.

• The format of the transaction is as follows

scriptPubkey : OP_DUP OP_HASH160 <pubKeyHash> OP_EQUALVERIFY OP_CHECKSIG

scriptSig : <sig> <pubkey>

• Pay to Script Hash (P2SH):

P2SH is used in order to send transactions to a script hash and was standardized in BIP16.

• In addition to passing the script, the redeem script is also evaluated and must be valid.

The template is as follows

scriptPubkey : OP_HASH160 <redeemScriptHash> OP_EQUAL.

scriptSig : [<sig>... <sign>] <redeemScript>

• MultiSig (Pay to Multisig):

m-of-N MultiSig transaction script is a complex type of script where it is possible to construct a script that required multiple signatures to be valid in order to redeem a transaction.

The template is as follows:

ScriptPubkey : <m> <pubkey>[<pubkey>. .]<n> OP_CHECKMULTISIG

scriptsig : 0[<sig>. . . <sign>]

- Pay to pubkey:
  This script is a very simple script that is commonly used in coinbase transactions. It is now obsolete and was used in an old version of bitcoin.
  The template is as follows:
  <pubkey> OP- CHECKSIG

- Null data:
  This script is used to store arbitrary data on the blockchain for a fee. The limit of the message is 40 bytes.
  The template is as follows
  OP_ RETURN <data>

(OR)

6.a) ~~What is~~ ~~the~~ Wallet software is used to store private or public keys and Bitcoin address. It performs various functions, such as receiving and sending bitcoins.

Types of Wallets:

i) Non-deterministic wallets:

- These wallets contain randomly generated private keys and are also called just a bunch of key wallets..

ii) Deterministic wallets:

- In this type of wallet, keys are derived out of a seed value via hash functions.
- This seed number is generated randomly and is commonly represented by human-readable mnemonic

code words.

iii) Hierarchical Deterministic wallets:

- Defined in BIP32 and BIP44, HD wallets store keys in a tree structure derived from a seed.
- The seed generates the parent key, which is used to generate child keys and subsequently, grandchild keys.

iv) Brain wallets:

- The master private key can also be derived from the hash of passwords that are memorized.
- The key idea is that this passphrase is used to derive the private key

v) Paper wallets:

- The ~~master~~ paper wallets, as the name implies this is a paper-based with the required key material printed on it.
- It requires physical security to be stored.

vi) Hardware wallets:

- Another method is to use a tamper-resistant device to store keys.
- This tamper-resistant device can be custom-built or with the advent of NFC-enabled phones, this can also be a Secure Element (SE) in NFC phones.

vii) Online wallets:

- Online wallets, as the name implies, are stored entirely online and are provided as a service usually via the cloud.

6.b) Privacy and Anonymity:

- As the blockchain is a public ledger of all transactions and is openly available, it becomes trivial to analyze it.
- Combined with traffic analyses, transactions can be linked back to their source IP addresses, thus possibly revealing a transaction's originator.
- This is big concern from a privacy point of view.
- Even though in Bitcoin it is a recommended & common practice to generate a new address for every transaction, thus allowing some level of unlinkability, this is not enough, and various techniques have been developed and successfully used to trace the flow of transactions throughout the network and link them back to their originator.
- These techniques analyze blockchains by using transaction graphs, address graphs and entity graphs which facilitate linking users back to the transactions, thus raising privacy concerns.
- Mixing protocols:

These schemes are used to provide anonymity to bitcoin transactions. In this model, a mixing service provider is used.

- Third-party mixing protocols:

Various third party mixing services are available but if the service is centralized, then it poses the threat of tracing the mapping between senders and receivers because the mixing service known about all inputs and outputs.

- Inherent anonymity:

This category includes coins that support privacy inherently and is built into the design of the currency. The most popular is Zcash, which uses zero-knowledge Proofs (ZKP) to achieve anonymity.

M-4

7.a) Two kinds of accounts exist in Ethereum.

EOA's (Externally Owned Accounts)

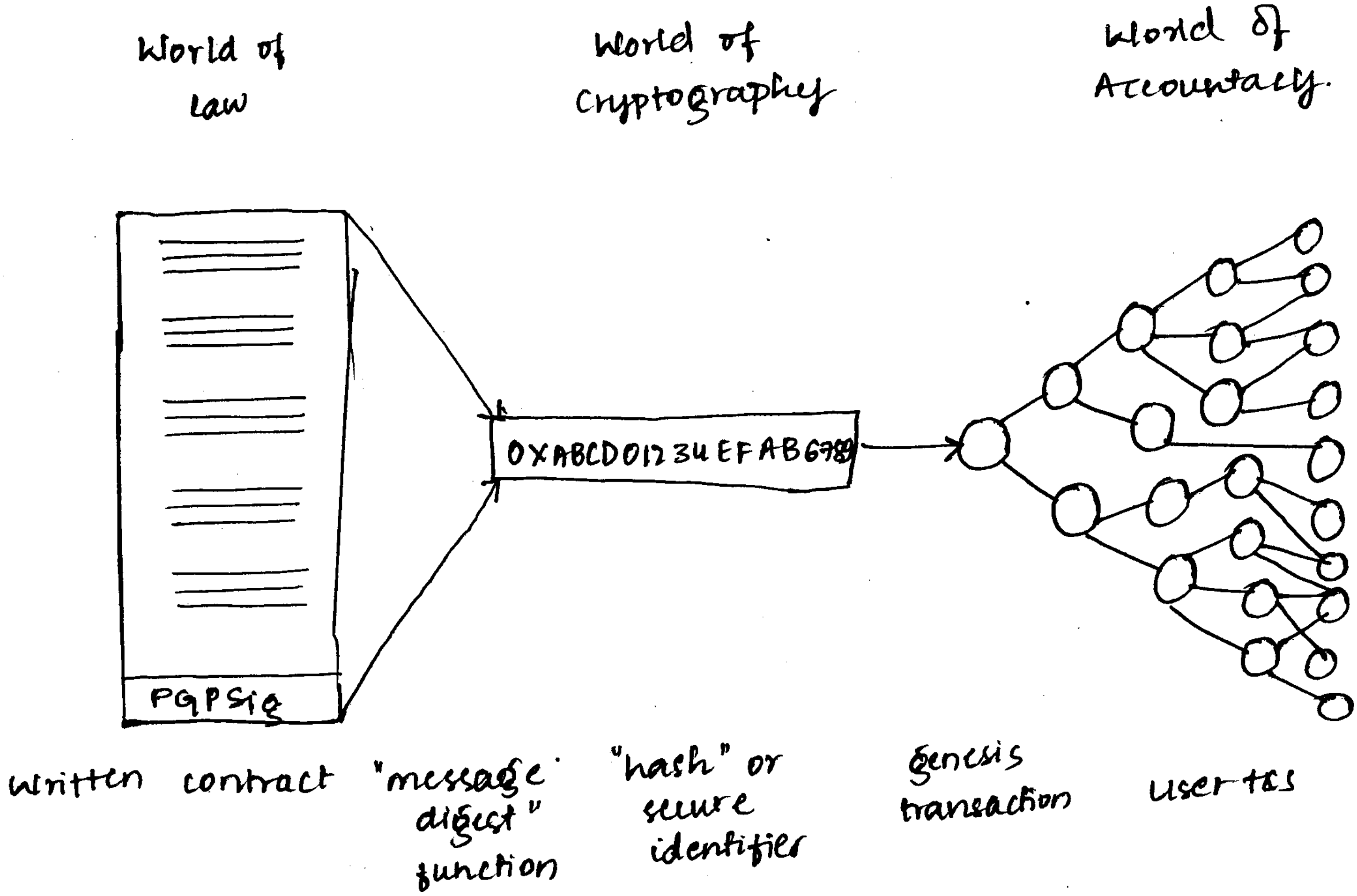
- EOA has ether balance
- They are capable of sending transactions
- They have no associated code.
- They are controlled by private keys.
- Accounts contain a key-value store.
- They are associated with a human user.

CA's (Contract Accounts)

- CA's have ether balance.
- They have associated code that is kept in memory on the blockchain.

- CA's can maintain their permanent state & can call other contracts.
- It is envisaged that in the serenity release.
- They are not intrinsically associated with any user or actor on the blockchain.
- CA's contain a key-value store.

7.b)



- A Ricardian contract is different from a smart contrait in the sense that a smart contract does not include any contratual document.
- It is focused purely on the execution of the contract.
- A Ricardian contract, on the other hand, is more concerned with the semantic richness and production of a document that contains contratual legal prose.

- The semantics of a contract can be divided into two types: operational semantic and denotational semantics.
- These contracts were used initially in a bond trading and payment system called Ricardo.
- The fundamental idea is to write a document that is understandable and acceptable by both a court of law and computer software.

(OR)

8.a)

- Nonce:

→ Nonce is a number that is incremented by one every time a transaction is sent by the sender.

→ It must be equal to the number of transactions sent and is used as a unique identifier for the transaction.

- Gas Price:

→ The gas price field represents the amount of wei required to execute the transaction.

→ In other words, this is the amount of Wei you are willing to pay for this transaction.

→ Wei is the smallest denomination of ether.

- Gas Limit:

→ The gas limit field contains the value that ~~responds~~ represents the maximum amount of gas that can be consumed to execute the transaction.

→ This is the amount of fee in ether that a user is willing to pay for computation.

- To:

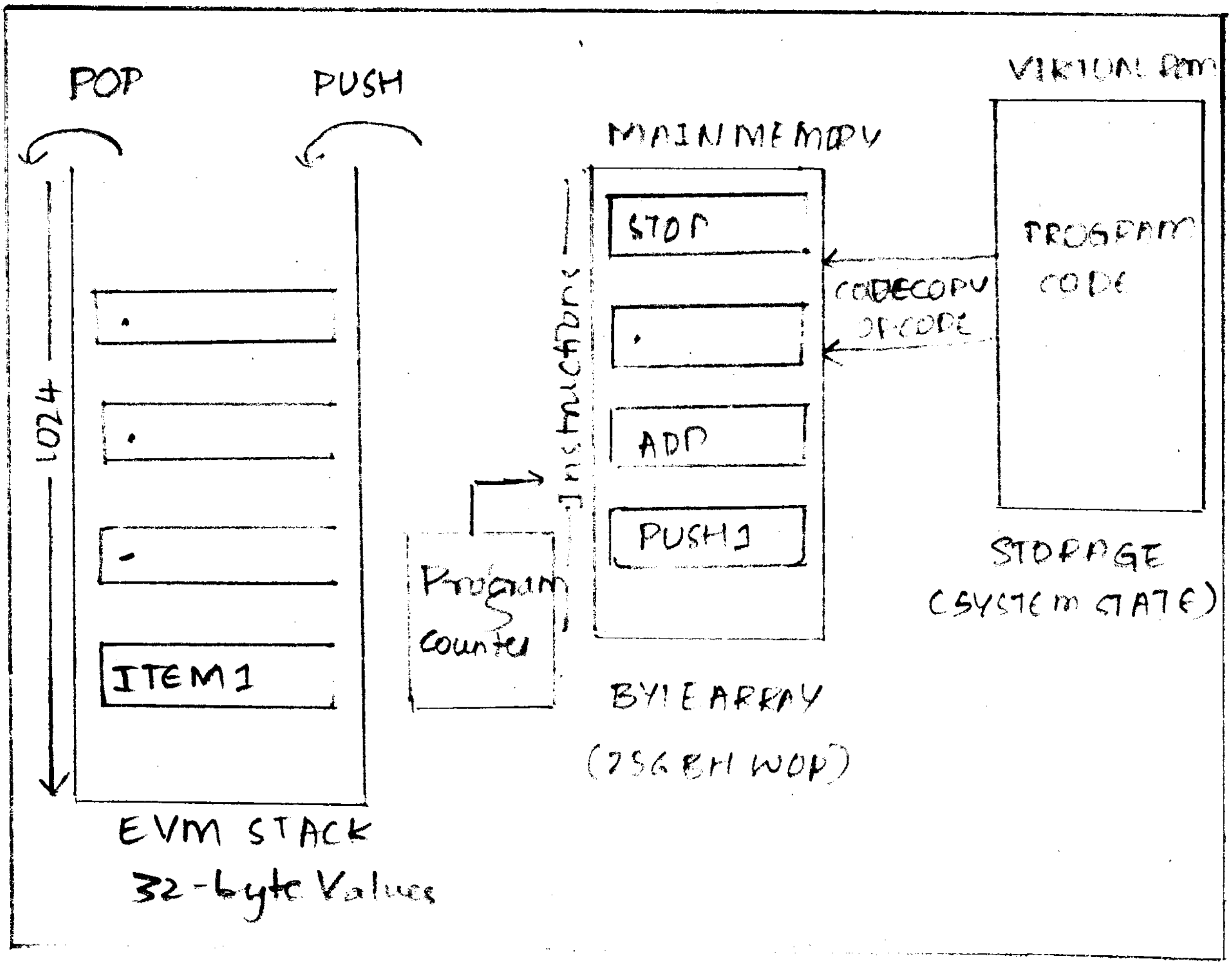
→ As the name suggests, the to field is a value that represents the address of the recipient of the transaction.

→ This is a 20-byte value.

- Value:

→ Value represents the total number of wei to be transferred to the recipient; in the case of a contract account, this represents the balance that the contract will hold.

8.b)



EVM Operation

- EVM is a simple stack-based execution machine that runs bytecode instructions to transform the system state from one state to another.
- The word size of the virtual machine is set to 256-bi
- The stack size is limited to 1024 elements and is based on the Last In, First Out (LIFO) queue.
- EVM is a turing-complete machine but is limited by the amount of gas that is required to run any instruction.
- EVM is an entirely isolated and ~~isolated~~ sandboxed runtime environment. The code that runs on the EVM does not have access to any external resources.
- This results in increased ~~true~~ security, deterministic execution and allows untrusted code to be run on Ethereum blockchain.
- The preceding diagram shows on EVM stack on the left side showing that elements are pushed and popped from the stack.

M-5

9.a) components of the fabric :

i) Peers

- Peers participate in maintaining the state of the distributed ledger.

ii) Orderer nodes

- Ordering nodes receive transactions from endorsers along with read-write sets, arrange the sequence

iii) Clients

- Clients are software that make use of API s to interact with the Hyperledger Fabric and propose transactions.

iv) Channels

- Channels allow the flow of confidential transactions between different parties on the network.

v) World state database

- World state reflects all committed transaction on the blockchain.

vi) Transactions

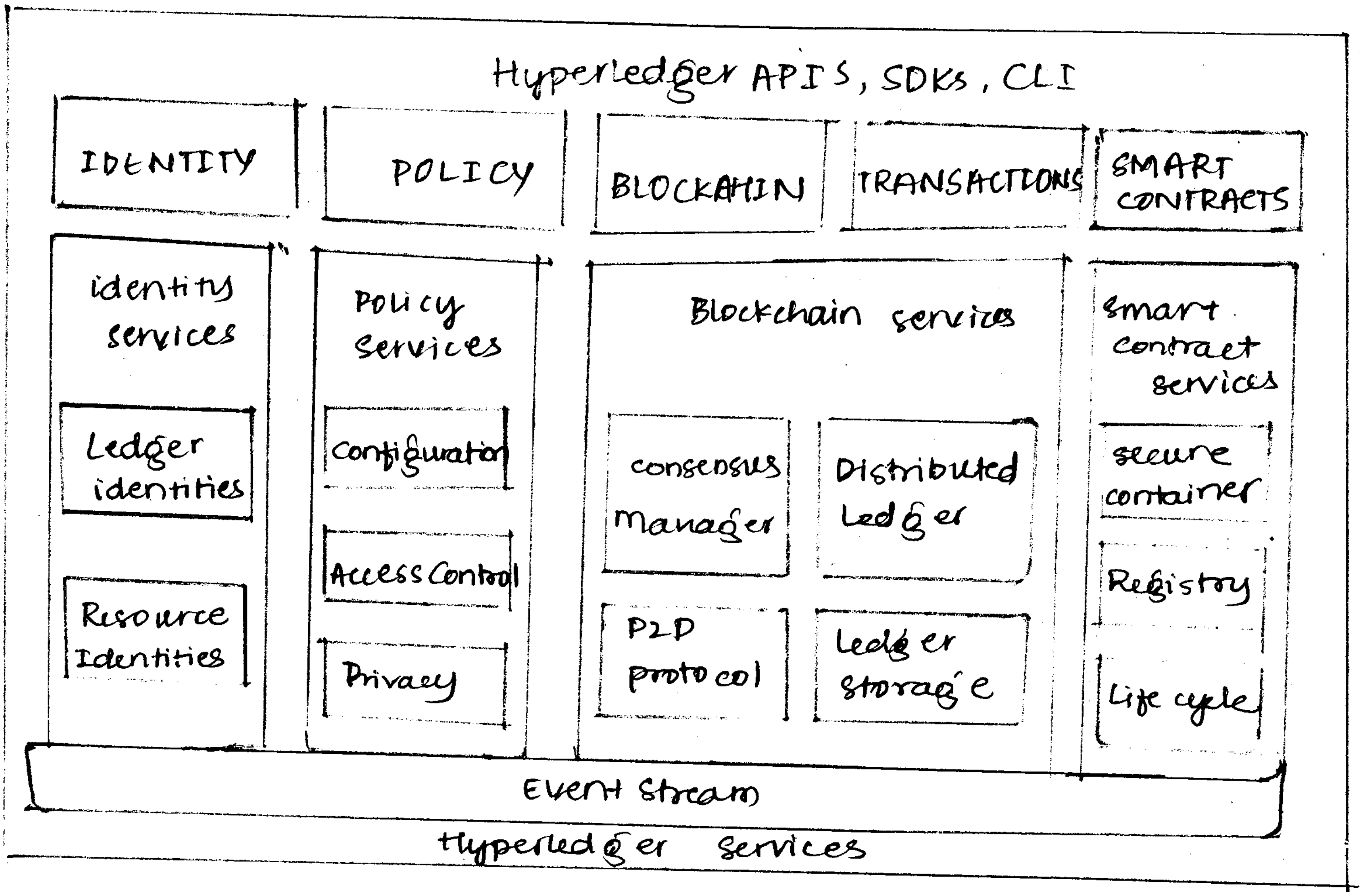
- Transaction message can be divided into two types: deployment transactions & invocation transactions.

vii) Membership Service Provider (MSP)

- MSP is a modular component that is used to manage identities on the blockchain network.

viii) Smart contracts

- They contain conditions and parameters to execute transactions and update the ledger.



a.b)

- Hyperledger Fabric: Modular architecture with pluggable components. It separates transaction processing into three phases: execution, ordering and validation. Hyperledger Sawtooth: Follows a modular architecture but introduces a unique transaction family concept

- In Fabric conensus is pluggable. Ordering services nodes handle consensus, whereas sawtooth uses Proof Elapsed Time (POET) as the primary consensus algorithm.

- Hyperledge fabric follows execute-order-validate model whereas sawtooth follows parallel transaction execution which improves scalability.

- Fabric uses permissioned blockchain with strong identity management using MSP while sawtooth can be permissioned or permissionless.
- In Fabric it uses chaincode, typically written in Go, Java or node.js and executed in Docker containers.
- Sawtooth uses transaction families, supporting EVM & solidity.

(OR)

10.a) Defn:

- It is an open-source distributed ledger framework that can be used to develop and implement cross-industry blockchain ~~applic~~ applications and systems.

Objectives

- To support business use cases with permissioned and modular blockchain solutions.
- Provides interoperability, modularity and scalability in enterprise blockchain.

Structure of Hyperledger as a Protocol suite

- Consensus layer - Manages agreement on the order of transactions.
- Smart contract layer - Executes business logic
- Communication layer - Ensures peer to peer communication.
- Data layer - stores the distributed ledger
- Identity layer - Provides membership services & identity management.

- Key projects

(i) Hyperledger Fabric - permissioned blockchain Framework

ii) Hyperledger Sawtooth - supports parallel transaction execution

iii) Iroha - Designed for mobile and simple use cases.

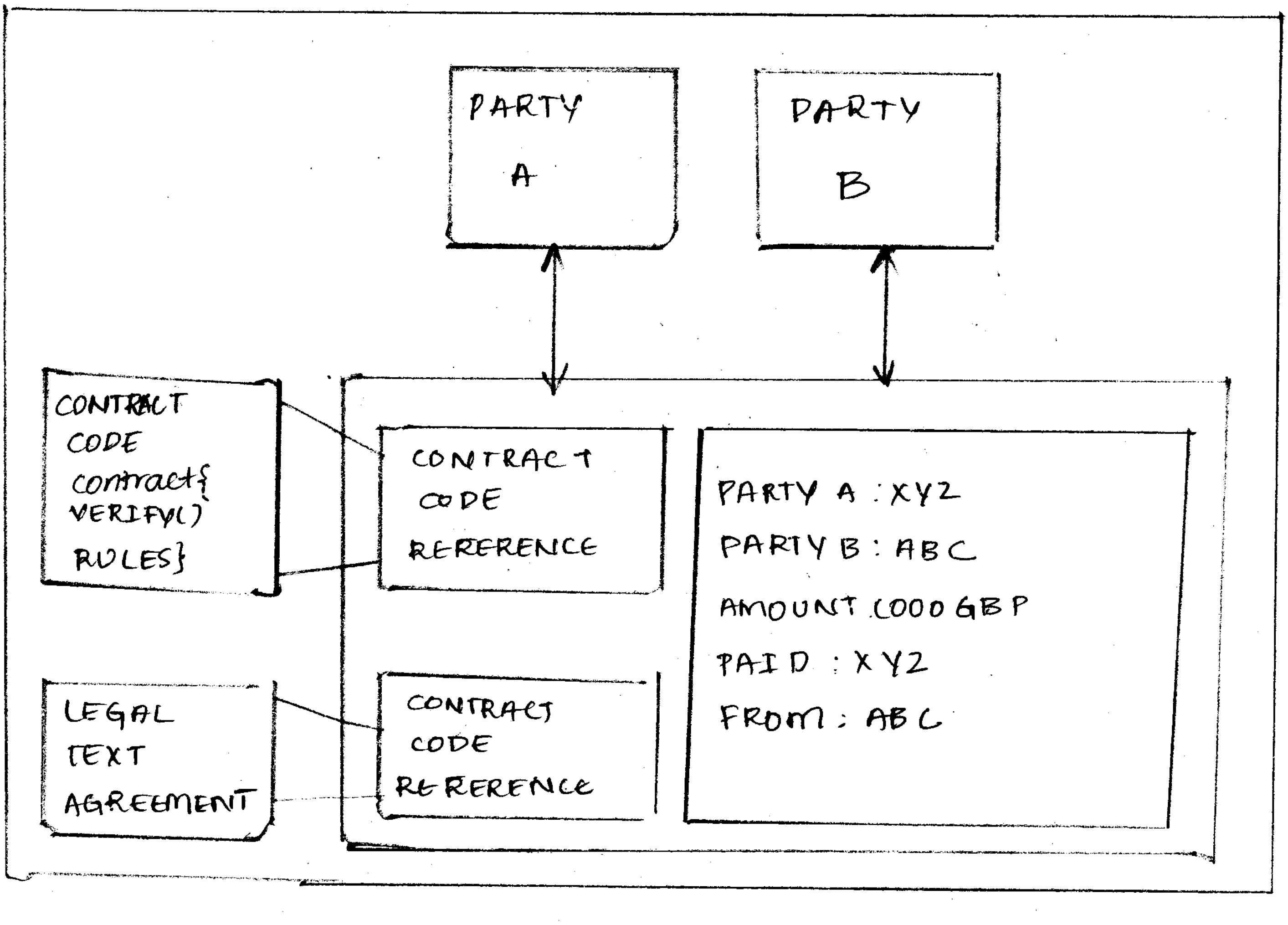
iv) Burrow - Provides a permissioned smart contract machine with EVM support.

v) Indy - specializes in decentralized identity management

vi) Explorer - visualization tool of blockchain

vii) Caliper - A benchmarking tool for blockchain platforms.

10.b)



- The main components of the corda platform include state objects, contract code, legal prose, transactions consensus and flows

→ state objects represent the smallest unit of data that represent a financial agreement.

→ They are created or deleted as a result of a transaction execution. They refer to contract code & legal prose.

→ Transactions are used to perform transitions between different states.

→ consensus model in corda is quite simple and is based on notary services that are available.

→ Flows in corda are novel idea that allows the development of decentralized workflows.

- Corda has been designed entirely from scratch with new model for providing all blockchain models.

- But, without traditional blockchain, it has been developed purely for the financial industry to solves issues arrising from the fact that each organizations manages their own ledgers and thus have their own view of truth, which leads to contradictions and operational ~~disk~~. risk.

- The consensus model in corda is quite simple and is based on notary services that are available.

- The general idea is that the transactions are evaluated for their uniqueness by the notary service.

Prof. F. N. Nadaf

HOD
Computer Science & Engineering
KLS Vishwanathrao Deshpande
Institute of Technology, Haliyal.