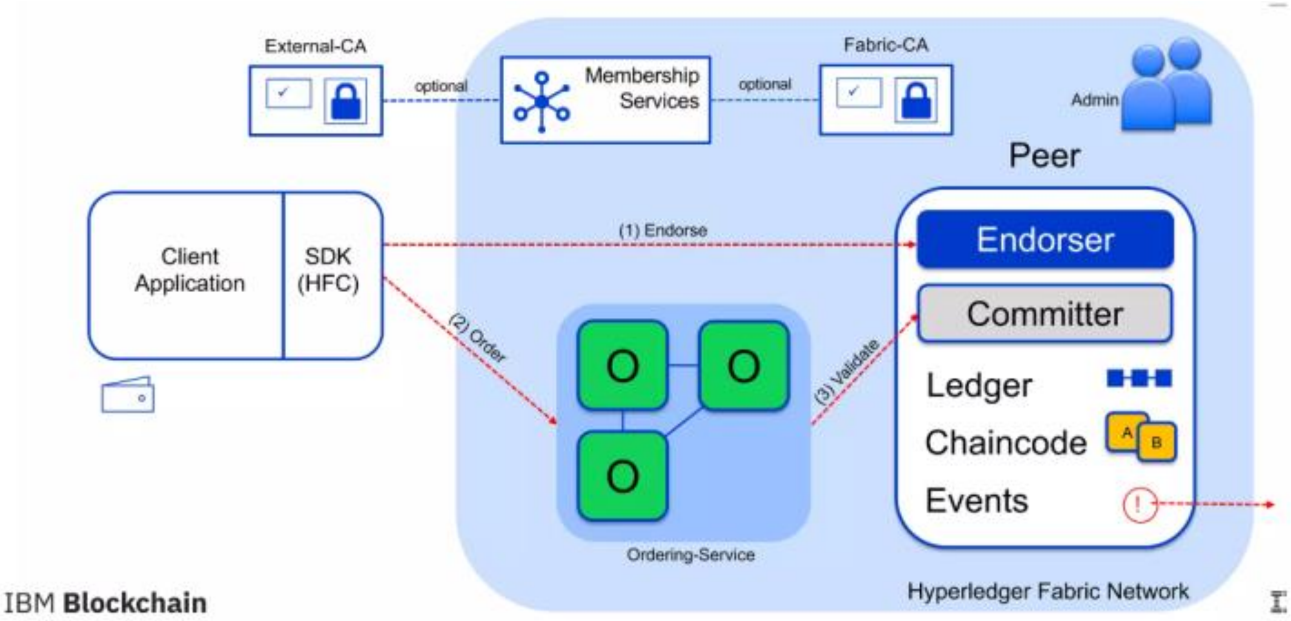
BLOCKCHAIN TT2 ANSWER KEY

1. Describe the role of Microsoft Azure's Blockchain as a Service (BaaS).

- ✓ Blockchain-as-a-service (BaaS) is the third-party creation and management of cloud-based networks for companies that build blockchain applications. These third-party services are a relatively new development in the growing field of blockchain technology.
- ✓ Azure Blockchain Service is a fully managed ledger service that gives users the ability to grow and operate blockchain networks at scale in Azure, via unified control for both infrastructure management as well as blockchain network governance.
- ✓ It provides the following:
  - i. Simple network deployment and operations
  - ii. Consortium management
  - iii. Smart contracts with development tools
- ✓ It provides support for the Ethereum Quorum ledger using the Istanbul Byzantine Fault Tolerance (IBFT) consensus mechanism.
- ✓ Features of Microsoft Azure's Blockchain
  - i. **Multiple Frameworks:** Supports Quorum, Ethereum, Corda, Hyperledger Fabric, with more Azure frameworks to come.
  - ii. **Managed Backend:** Azure handles all backend tools and infrastructure.
  - iii. **Easy Deployment:** Quickly deploy via Azure CLI, Portal, or Visual Studio Code with Azure Blockchain extension. Security and storage on Azure Virtual Networks are managed seamlessly.
  - iv. **Security:** Firewall protection and TLS encryption for transaction and validator nodes. Configurable firewall, authentication, and access keys.
  - v. **Auto-Maintenance:** Nodes are maintained to stay updated; fully managed by Azure.
  - vi. **Consortium Management:** Easily manage consortiums, node access, membership, policy enforcement, and permissions.
  - vii. **Monitoring:** Comprehensive monitoring with Azure Monitor Service for node performance, storage, and transaction metrics.

2. Explain Hyperledger Fabric.

- ✓ Hyperledger Fabric is an open source, permissioned blockchain framework, started in 2015 by The Linux Foundation.
- ✓ It is a modular, general-purpose framework that offers unique identity management and access control features, which make it suitable for a variety of industry applications such as track-and-trace of supply chains, trade finance, loyalty and rewards, as well as clearing and settlement of financial assets.
- ✓ It provides high levels of secrecy, robustness, adaptability, and scalability.
- ✓ **Architecture**:



- ✓ **Working:**
  - o **Network Structure:** Fabric networks consist of organizations (members), each with its own certificate authority (CA) and peer nodes. An ordering service, shared by all members, manages transaction sequencing.
  - o **Certificates and Permissions:** Each organization has a root certificate, with derived certificates for users and components, defining permissions for secure interactions.
  - o **Peer Nodes:** Peer nodes validate transactions, store chaincode (smart contracts), and maintain a local ledger.
  - o **Ordering Service:** Ensures transactions are ordered and endorsed correctly, broadcasting new transaction blocks to all peers for ledger updates.

- ✓ **Core Components**:
  - o **Assets**: Assets are digital representations of tangible or intangible items (e.g., goods, services, or entitlements) stored as key-value pairs in JSON or binary format. Chaincode allows assets to be traded or updated on the ledger, with transitions recorded as trades.
  - o **Chaincode**: Chaincode, or smart contracts in Fabric, drives network transactions. It interacts with the ledger's current state, verifies transaction validity, and applies necessary updates.
  - o Chaincode operations can be executed across all network nodes to synchronize state changes, establishing a shared ledger.
  - o **Ledger**: The ledger is an immutable, chronological record of transactions. Each transaction logs changes as asset key-value pairs. Every organization holds a synchronized ledger, ensuring consistency across the network.
  - o **Security**: Hyperledger Fabric ensures secure operations through cryptographic identities and permissions. Public Key Infrastructure (PKI) is used for managing access control at network and channel levels, ensuring only authorized users interact with data.
  - o **Consensus**: Consensus in Fabric encompasses transaction endorsement, ordering, validation, and commitment. This process ensures that transactions are verified, sequentially ordered, and meet network policies, confirming integrity before adding them to the ledger.

- ✓ **Hyperledger Fabric Transaction Flow**:
  - o The transaction flow begins when a client application sends a transaction proposal to peers in each organization for endorsement.
  - o The peers verify the submitting client's identity and authority to submit the transaction. Next, they simulate the outcome of the proposed transaction and if it matches what was expected, it sends an endorsement signature back to the client.
  - o The client collects endorsements from peers, and once it receives the proper number of endorsements defined in the endorsement policy, it sends the transaction to the ordering service.
  - o Lastly, the ordering service checks to see if the transaction has the proper number of endorsements to satisfy the endorsement policy. It then chronologically orders and packages the approved transactions into blocks, and sends these blocks to peer nodes in each organization. Peer nodes receive new blocks of transactions from the ordering service, and then do a final validation for transactions in that block. Once this is complete, the new block is added to the ledger and the state of the ledger is updated. The new transactions are now committed.

- ✓ **Benefits of Hyperledger Fabric:**
  - o **Network With Authorization:** Instead of an open network of anonymous participants, establish decentralized confidence in a web of known members.
  - o **Transactions Are Private:** Only share the info you want with the people you want.
  - o **Architecture Is Pluggable:** Rather than a one-size-fits-all strategy, tailoring the blockchain to industry demands a pluggable design.
  - o **Starting-up Is Simple:** Instead of learning proprietary languages and architectures, smart program contracts in the languages your team uses. The number of trust levels and verification is minimized, which keeps the network and processing clean.
  - o **Access, Control and Governance:** Fabric networks are composed of channels that are a private 'subnet' of communication between different or more specified users on the web, allowing them to interact securely and secretly.

3. **Differentiate between pseudo-anonymity and full anonymity in Blockchain networks.**

- ✓ Blockchain networks generally provide **pseudo-anonymity**, not full anonymity. Here's a detailed comparison:
- ✓ **Pseudo-Anonymity:**
  - o **Identifier-Based Transactions**: Users' identities are masked by pseudonyms like public keys or wallet addresses, rather than real names.
  - o **Traceable Activity**: Transactions and activities can be traced to a specific identifier. Analysis techniques can reveal patterns in activity, potentially linking addresses to real identities.
  - o **Linkability to Identity**: If an identifier (e.g., a public key) is linked to an individual's identity, for example through a cryptocurrency exchange that requires identity verification (KYC), all related transactions become traceable.
  - o **Example**: Seen in public blockchains like **Bitcoin** and **Ethereum**, where addresses are public but not directly linked to identities. However, if someone's public key is linked to their identity (through an exchange or other means), all their transactions can be traced.
  - o **Re-identification Risk**: Even if real names aren't used, external data sources can sometimes be combined with blockchain data to infer identities, a technique known as **de-anonymization**.
- ✓ **Full Anonymity:**
  - o **Complete Obfuscation**: Both user identities and transaction details are completely hidden from view, preventing linkages to real-world identities or any transaction history.
  - o **Advanced Privacy Protocols**: Anonymous blockchains employ cryptographic techniques like **zk-SNARKs** (Zero-Knowledge Succinct Non-Interactive Arguments of Knowledge), **ring signatures**, or **stealth addresses**. These protocols obscure both the transaction details and the participants' identities.
  - o **Example: Zcash** offers full anonymity through the use of cryptographic techniques like Zk-SNARKS (ZeroKnowledge Succinct Non-Interactive Arguments of Knowledge), which allow transactions to be verified without revealing information about the sender, receiver, or the transaction amount.
  - o **Reduced Traceability**: Since these systems avoid linking any identifiable entity to transactions, they offer higher privacy standards, though they may face increased scrutiny by regulators due to potential misuse.

4. **Differentiate between sharding and Algorand's Pure Proof of Stake (PPoS) model in terms of scalability and their respective security challenges.**

- ✓ **Scalability**:
  - o Algorand PPoS: Achieves scalability by randomly selecting validators, allowing efficient, congestion-free processing without additional scaling layers.
  - o Sharding: Increases scalability by dividing the network into shards, each processing a subset of transactions, thus boosting throughput through parallel processing.
- ✓ **Security**:
  - o Algorand PPoS: Uses random validator selection and a forkless design to prevent 51% attacks, as attackers cannot predict or manipulate block validators.
  - o Sharding: Improves security by requiring attackers to control 51% in multiple shards, which is much harder than attacking a single blockchain, and cross-shard protocols maintain consistency and security across the network.
- ✓ Algorand is a blockchain that uses a Pure Proof-of-Stake (PPoS) consensus mechanism, which is inherently resistant to 51% attacks.
  - o How Algorand Prevents 51% Attacks:
    - ▪ Random Validator Selection: Instead of a few powerful entities controlling the consensus, Algorand randomly selects validators from the pool of users holding ALGO tokens. This random selection makes it almost impossible for attackers to predict or manipulate who will validate the next block.
    - ▪ Decentralized Participation: Every ALGO holder has a chance to participate in the consensus, regardless of how much ALGO they own. This makes it much harder for a single entity to accumulate enough power to control more than 50%.
    - ▪ Forkless Design: Algorand is designed to prevent forks. When a block is finalized, it's added permanently to the blockchain, and there are no competing versions of the chain. This ensures that attackers can't create alternative blockchains even with significant control.

  - o Why Algorand is Safe:
    - ▪ Attacking Algorand would require a majority of the token holders to act maliciously, which is extremely costly and against the economic interests of honest participants. This economic disincentive makes 51% attacks highly unlikely

- ✓ Sharding is a technique that divides the blockchain network into smaller groups, or shards, where each shard processes a portion of the total transactions. This division increases scalability and security by reducing the chance of a 51% attack.
  - o How Sharding Prevents 51% Attacks:
    - ▪ Decentralization by Division: In sharding, the network is split into shards, each with its own validators. An attacker would need to control 51% of the validators in every shard, which is far more difficult than attacking a single, unified blockchain.
    - ▪ Cross-shard Security: Sharded blockchains have mechanisms to ensure that transactions in one shard are consistent and secure with transactions in another shard, further complicating attacks.
    - ▪ Adaptive Selection: Some sharded blockchains, like Ethereum 2.0 (moving to Proof-of-Stake with sharding), use random validator assignment to each shard, preventing attackers from targeting specific shards.
  - o Sharding Strengths:
    - ▪ Improved Scalability: Sharding spreads the load across multiple shards, allowing the network to handle more transactions per second without compromising security.
    - ▪ Enhanced Security: Since an attacker would need to compromise several shards simultaneously, the likelihood of a successful 51% attack is drastically reduced

5. Describe how a Sybil attack is executed.

- ✓ Definition: A Sybil attack occurs when a single malicious entity creates multiple fake identities or nodes in a blockchain network to gain control or influence the network.
- ✓ How it works:
  - o In decentralized networks, decisions are made through consensus mechanisms. By creating many fake nodes, an attacker can disrupt consensus, gain undue influence, or manipulate the network's behaviours.
  - o For example, in Proof-of-Work or Proof-of-Stake systems, having multiple identities can allow the attacker to try and outvote honest nodes or overwhelm the system.
- ✓ Consequences:
  - o Disrupting consensus: Attacker may prevent legitimate transactions from being verified or double-spend their coins.
  - o Reducing reliability: When too many fake nodes are involved, the network becomes unreliable as it's no longer truly decentralized.
- ✓ Mitigations:
  - o Proof-of-Work (PoW): Requires computational effort to create blocks, which prevents an attacker from creating multiple fake nodes cheaply.
  - o Proof-of-Stake (PoS): Requires validators to hold a stake, or a certain amount of cryptocurrency, making it costly to launch a Sybil attack.
  - o Identity verification: Some blockchain networks use identity systems that ensure each participant is a real entity.

6. What is selfish mining in Blockchain networks?

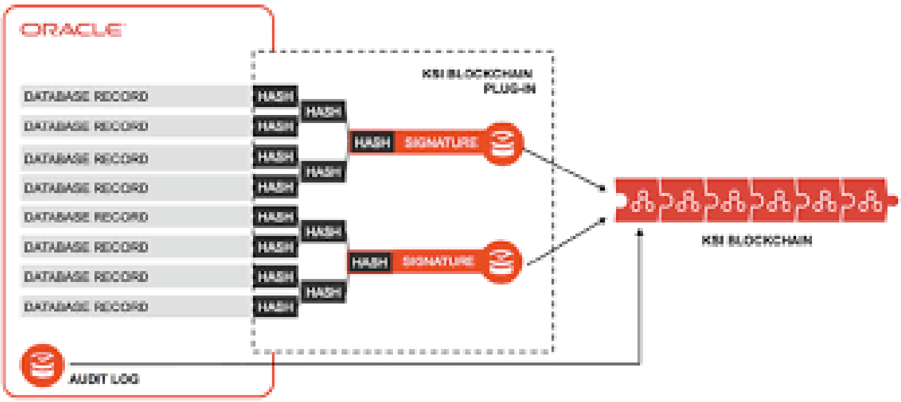
- ✓ Definition: Selfish mining occurs when a miner or group of miners withhold newly mined blocks to gain an advantage over honest miners.
- ✓ How it works:
  - o Selfish miners privately mine blocks instead of broadcasting them to the network immediately. By secretly building a private chain, they can eventually reveal their chain to invalidate the honest miners' work.
  - o This allows them to gain more rewards by temporarily having a longer chain than the public one.
- ✓ Consequences:
  - o Centralization of mining power.
  - o Unfair distribution of block rewards.
- ✓ Mitigations: Adjust reward structures to discourage withholding blocks.

7. Describe how a 51% attack is executed.

- ✓ Definition: A 51% attack occurs when an entity controls more than 50% of the mining or computational power in a Proof-of-Work blockchain, or more than 50% of the stakes in a Proof-of-Stake blockchain.
- ✓ How it works:
  - The attacker can reverse transactions, double-spend coins, or prevent new transactions from being added to the blockchain.
  - Essentially, they can rewrite the blockchain at will.
- ✓ Consequences:
  - Loss of trust in the network.
  - Potential theft through double-spending.
- ✓ Mitigations:
  - Larger, more decentralized networks (like Bitcoin) are highly resistant because of the enormous amount of computational power or capital required.
  - Smaller blockchains are more vulnerable and need added layers of security, such as additional consensus algorithms.

8. What role does the Keyless Signature Infrastructure (KSI) Blockchain play in the Estonian e-government system?

- ✓ Estonia is popularly claimed to use blockchain technology to secure e-voting and to provide "the ability to 100% trust government data in any situation".
- ✓ Estonian Blockchain relies on three distinct digital systems, so-called "three technological pillars of the digital state": "e-ID", "X-Road", and "KSI Blockchain".
- ✓ The technology chosen for Estonian systems is Keyless Signature Infrastructure (KSI) Blockchain, also used by NATO and the U.S. Department of Defense.



- ✓ It allegedly refers to a timestamp system used for "preserving the integrity of the digital documents within multiple public registries (e.g., healthcare, property), identities, transactions and data privacy of its users".
- ✓ In basic terms, from each document, a "hash" is extracted, i.e., a unique sequence of codified characters that represent exactly that document.
- ✓ If the document is ever changed, its hash would change, and thus if a document is tampered with, it would be easily detected.
- ✓ The hash signatures are recorded in the "KSI Blockchain", as a sequence of those hashes.

9. Discuss the application of Blockchain technology in the healthcare sector.

- ✓ **Patient Identity Management:**
  - Unique Patient Identification: Blockchain can provide a robust and secure way to create and manage unique patient identities, reducing errors and ensuring data accuracy.
- ✓ **Clinical Trials and Research:**
  - Data Integrity: Blockchain can help ensure the integrity and transparency of data collected in clinical trials and research studies, reducing the risk of data tampering and fraud.
  - Data Sharing: Researchers and organizations can securely share data with each other, enabling collaboration while protecting sensitive information.
- ✓ **Drug Traceability:**
  - Supply Chain Management: Blockchain can be used to track the production, distribution, and authentication of pharmaceuticals. This can help combat counterfeit drugs and ensure the safety of patients.
- ✓ **Prescription Management:**
  - e-Prescriptions: Blockchain can be used to securely transmit and manage electronic prescriptions, reducing the risk of prescription fraud and errors.

- ✓ **Telemedicine and Telehealth:**
  - o Remote Patient Monitoring: Blockchain can securely collect and transmit patient data from remote monitoring devices to healthcare providers, ensuring data privacy and integrity.
- ✓ **Consent Management:**
  - o Patient Consent: Blockchain can track and manage patient consent for data sharing, ensuring that patients have control over how their data is used.

10. Examine the impact of Blockchain on governance and public services.

- ✓ **Notary Services:**
  - o Notarization: Blockchain can be used for notarizing documents and ensuring their authenticity, reducing the need for traditional notary services.
- ✓ **Healthcare Data Management:**
  - o Secure Health Records: Government health agencies can use blockchain to securely manage and share health records, improving data accuracy and privacy.
- ✓ **Education Records:**
  - o Academic Credentials: Academic certificates and transcripts can be stored on a blockchain, making it easier to verify the authenticity of educational records.
- ✓ **Smart Contracts for Government Services:**
  - o Automated Processes: Government agencies can use smart contracts for automating processes like permit approvals, licensing, and contract management, reducing administrative overhead and enhancing efficiency.
- ✓ **Tax Collection and Compliance:**
  - o Transparent Tax Records: Blockchain can provide a transparent and unchangeable record of tax payments, making it easier for citizens and businesses to track and comply with tax regulations.
- ✓ **Public Health and Safety:**
  - o Disease Surveillance: Blockchain can help in securely and transparently tracking disease outbreaks and vaccination records, aiding public health efforts.
- ✓ **Intellectual Property Rights**:
  - o Protecting IP: Governments can use blockchain to protect intellectual property rights, copyrights, and patents, ensuring fair compensation for creators.

11. Explain Zcash and Zk-SNARKS for anonymity preservation.

- ✓ **Zcash**:
  - o Zcash is a privacy-focused cryptocurrency that enhances anonymity by allowing users to shield transaction details such as sender, receiver, and transaction amount.
  - o It provides two types of addresses:
    - ▪ Transparent addresses (t-addresses): These work similarly to Bitcoin addresses, offering pseudo-anonymity where transaction details are visible on the blockchain.
    - ▪ Shielded addresses (z-addresses): These offer full anonymity by hiding transaction details from the public blockchain, preserving user privacy.
- ✓ **Zk-SNARKS**:
  - o Zk-SNARKS (Zero-Knowledge Succinct Non-Interactive Argument of Knowledge) is a cryptographic method that allows someone to prove possession of certain information (like a secret key) without revealing that information.
  - o In the context of Zcash, Zk-SNARKS allows for shielded transactions where:
    - ▪ Users can validate transactions without revealing any details, like who sent the money, who received it, or how much was sent.
    - ▪ The transaction is still verified as valid by the network, but no sensitive data is disclosed.
  - o How Zk-SNARKS Work in Zcash:
    - ▪ When someone sends a shielded transaction, Zk-SNARKS ensures the transaction is valid without revealing the actual information behind it.
    - ▪ This process prevents any traceable links between transactions and participants, enabling privacy while maintaining the integrity of the blockchain.

- Advantages:
  - Complete Privacy: Zcash with Zk-SNARKS provides endto-end privacy by hiding all aspects of the transaction.
  - Verifiable: Even though the details are hidden, the blockchain can still verify that the transaction is valid.

12. Explain DeFi foundation in detail.

- ✓ Decentralized Finance (DeFi) is all about monetary systems using public blockchains.
- ✓ At the core, the term "public" is important here. It can be equated to similar to that of Ethereum public blockchain. In the public blockchain, there is no place for centralized authority.
- ✓ The need for DeFi comes from the fact that financial services are not available to everyone around the world. Almost 1.7 billion people all around the world have no means and access to financial services. The financial institutes can also not provide the necessary infrastructure to make people more access to money. The existing infrastructure is huge, but it does lack when it comes to reaching everyone out there.
- ✓ With decentralization, the current infrastructure failures are solved. It removes the failure point and ensures that the records can be stored and shared among different nodes across the network. It can work on a peer-to-peer network without any centralized authority.
- ✓ Another key element of the DeFi is the decentralized apps (dApps). DApps enable the financial institutes to create functional apps on the public blockchain and ensure that anyone can interact with them with minimal cost per interaction.
- ✓ DeFi eliminates the fee that banks and other financial institutions charge for using their services and promotes the use of P2P transactions.
- ✓ DeFi is open, pseudonymous, flexible and fast.
- ✓ Key ingredients of DeFi are:
  - 1. Lending and Borrowing: With DeFi lending, investors deposit crypto through a decentralized application, and someone can then borrow the crypto through a P2P network, paying interest on the loan.
  - 2. Stable Coins: These are crypto that has its value pegged to another asset like fiat money, exchange-traded commodity, etc.
  - 3. Decentralized Exchanges (DEX): Connect buyers and sellers and allows users to make transactions via P2P network.
  - 4. Derivatives: These are the contracts whose values are derived from the performance of the underlying financial asset.
  - 5. Crypto-margin Trading: It means utilizing the borrowed funds to increase the position in a certain asset.
  - 6. DeFi Insurance: It ensures the guarantees of compensation in exchange for payment of a premium