Mario Mendoza – Ignacio García – Diego Calvache

Apartado 1

a) Definición de DLT (Distributed Ledger Technology)

Una DLT o Tecnología de Registro Distribuido es un sistema digital que permite registrar y compartir datos de forma sincronizada entre múltiples nodos (computadores) sin necesidad de un intermediario central.
Cada nodo mantiene una copia del registro y las actualizaciones se validan mediante un mecanismo de consenso, asegurando que todos los participantes tengan una versión idéntica y verificable de la información.

b) Definición de Blockchain

La Blockchain es un tipo específico de DLT en la que los datos se agrupan en bloques enlazados criptográficamente entre sí formando una cadena secuencial e inmutable.
Cada bloque contiene un conjunto de transacciones, un hash del bloque anterior y un sello temporal, lo que garantiza la integridad de toda la cadena.
Su principal característica es que las modificaciones son imposibles sin alterar todos los bloques posteriores, lo que le otorga un alto nivel de seguridad y confianza.

Palabras clave: cadena de bloques, hash, bloques, seguridad, inmutabilidad.

Apartado 2: Tabla Comparativa – Blockchain vs Otras DLT

Criterio	**Blockchain**	**Otras DLT (ej. Hashgraph, IOTA, Corda)**
Estructura de datos	Cadena lineal de bloques enlazados por hash	Grafo acíclico dirigido (DAG) u otras estructuras no lineales
Mecanismo de consenso	Proof of Work (PoW), Proof of Stake (PoS), BFT, etc.	Gossip about Gossip (Hashgraph), Tangle (IOTA), Notary (Corda)
Grado de descentralización	Alta (en redes públicas)	Variable (algunas son más centralizadas o híbridas)
Permisos	Puede ser pública o privada	Generalmente privadas o de consorcio
Ejemplos de plataformas	Bitcoin, Ethereum, Hyperledger Fabric	Hashgraph (Hedera), IOTA, Corda, Quorum

Apartado 3

a) Almacenamiento de la información en Blockchain

- La información se agrupa en bloques que contienen:
    - Datos de las transacciones
    - Hash del bloque anterior
    - Sello temporal
- Cada bloque está enlazado criptográficamente con el anterior, formando una cadena inmutable.
- Si se modifica un bloque, su hash cambia, rompiendo la cadena y evidenciando la alteración.

b) Pasos básicos de validación de una transacción (Ejemplo: Bitcoin/Ethereum)

1. **Creación:** un usuario genera una transacción y la firma digitalmente con su clave privada.
2. **Difusión:** la transacción se transmite a la red P2P.
3. **Verificación:** los nodos validan la autenticidad (firma, saldo, formato).
4. **Agrupación:** las transacciones válidas se agrupan en un bloque.
5. **Consenso:** los mineros o validadores compiten o colaboran según el algoritmo (PoW, PoS, etc.).
6. **Confirmación:** el bloque validado se añade a la cadena y se propaga por toda la red.
7. **Registro inmutable:** una vez añadido, la transacción se considera confirmada y permanente.

c) Papel de los nodos y del consenso

- **Nodos:**
  Son los participantes de la red que almacenan, verifican y transmiten información.
  Pueden ser nodos completos (full nodes) o ligeros (light nodes).
  Los mineros o validadores son nodos especializados que crean y confirman bloques.
- **Mecanismos de consenso:**
  Permiten acordar qué transacciones son válidas sin una autoridad central.
    - **Proof of Work (PoW):** requiere resolver un problema criptográfico (usado por Bitcoin).
    - **Proof of Stake (PoS):** los validadores se seleccionan según la cantidad de tokens en stake (usado por Ethereum 2.0).

- **Byzantine Fault Tolerance (BFT):** votación entre nodos confiables (usado en redes privadas).

Apartado 4: Ventajas y Limitaciones de Blockchain

Ventajas	**Limitaciones**
1. **Transparencia**: todos los participantes pueden auditar el registro.	1. **Escalabilidad limitada**: las transacciones por segundo son bajas.
2. **Inmutabilidad y seguridad**: los datos no pueden alterarse sin consenso.	2. **Alto consumo energético** (en PoW).
3. **Desintermediación**: elimina la necesidad de terceros de confianza.	3. **Privacidad reducida** en redes públicas.

Apartado 5: Casos de uso reales

Caso 1 – Blockchain pública: Criptomoneda (Bitcoin)

- **Problema que resuelve:** Permite realizar transferencias de valor sin intermediarios (bancos), de forma segura y global.
- **Por qué se eligió esta tecnología:** Su naturaleza descentralizada y resistente a la censura la hace ideal para pagos entre pares.
- **Beneficios frente a soluciones tradicionales:**
    - Transacciones internacionales sin bancos.
    - Costes reducidos.
    - Transparencia total y resistencia a fraudes.

Caso 2 – DLT privada: IBM Food Trust (basado en Hyperledger Fabric)

- Problema que resuelve: Falta de trazabilidad y confianza en la cadena alimentaria (origen de productos, contaminación, fraudes).
- Por qué se eligió esta tecnología: Permite compartir información entre empresas (productores, distribuidores, minoristas) de forma controlada y privada.
- Beneficios frente a soluciones tradicionales:
    - Mayor trazabilidad y seguridad alimentaria.
    - Reducción del tiempo de rastreo (de días a segundos).
    - Confianza entre actores sin revelar datos sensibles.h