Patrones de diseño para wallets

BLOCKCHAIN

un blockchain son bloques de información validados y enlazados unos con el otro, que soluciona sistemas distribuidos
un sistema distribuido es un conjunto de equipos independientes que actúan de forma transparente actuando como un único equipo.
generalmente no necesito blockchain y además son complicadas de implementar
resulta ser un patrón de diseño, ayuda en los siguientes problemas

- confirmación de información en base a un protocolo de consenso, blockchain es una forma de almacenar información donde todos los actores están de acuerdo
- inmutabilidad sobre la información acordada en base al consenso
- resistencia a censura: evitar que los buenos actores sean privados de operar en la red ya que todos están todos en el mismo nivel porque ninguno es más importante que el otro
- resistencia a la captura: para poder romper el consenso requiere lograr el 51% de los nodos de la red.
- tolerancia al problema de los generales bizantinos

hoy en día la blockchain se usa mucho como cadena de provisión (tratamiento de un recurso) por ejemplo el efectivo electrónico
el *bitcoin* es un sistema distribuido que

- tiene un asiento contable acordado mediante un protocolo que registra las monedas compradas, propietarios etc. y resulta ser inmutable hacia atrás por lo tanto solo modifica lo actual agregando bloques nuevos
- tiene una resistencia a la censura, evita que los buenos actores sean privados de operar en la red
- resistencia a la captura, para poder romper el consenso requiere lograr el 51% de los nodos de la red
- tolerancia al problema de los generales bizantinos (BFT)
- resistente a la falsificación (double-spend, finney attack)

POTESTAD CRIPTOGRÁFICA
para operar en una blockchain necesito una clave privada (genero nuevos elementos) y una pública (cualquiera puede tener la mía y funciona como una casilla de correo y cualquiera puede leer la info creada ya sea con clave privada). En el caso de bitcoin, las personas con una clave privada puede operar el control del dinero

CREACIÓN DE BLOQUES
cada vez que se crea un nuevo bloque, todos los integrantes de la red de pares deben verificar que sea válido y agregarlo a su copia de la cadena de bloques, así se garantiza que la única forma de alterar la cadena es tener la mayoría del poder de cómputo.

WALLET
una *wallet* es una representación de los datos de una blockchain desde el punto de vista de un conjunto de claves privadas. Elementos como el balance y las transacciones, son subproductos de un proceso denominado sincronización que consiste en tomar claves públicas y recorrer la cadena de bloques recolectando los elementos de interés para las mismas

para una ballet se requiere

- custodia de las claves del usuario
- usar criptomonedas con privacidad en el asiento contable
- desencriptación en el propio dispositivo
- enviar/ recibir fondos
- historial de transacciones
- estar al día con la blockchain

ANÁLISIS DE REQUERIMIENTOS

1) en los repositorios: buscar historias de usuario, documentación, análisis del código fuente
2) aplicaciones: contrastar con lo encontrado en los repositorios, analizar casos de uso presentes en la interfaz gráfica, comparar la funcionalidad entre todas las apps
3) documentación de Zcash y Monero: análisis de protocolo, documentación referente a wallets, buscar requerimientos no funcionales