

## Ejercicio 16

### Objetivo:

Utilizar el método Delphi para llegar a un consenso sobre la tecnología y la arquitectura más adecuadas para el desarrollo de una billetera virtual segura, escalable y confiable.

### Descripción:

El método Delphi es una técnica de consulta estructurada que se utiliza para obtener opiniones expertas sobre un tema complejo. En este caso, el método Delphi se utilizará para recopilar información y opiniones de expertos en blockchain, seguridad, desarrollo de software y arquitectura de sistemas sobre la mejor tecnología y arquitectura para una billetera virtual.

### 1. Definición del problema:

- Describir claramente los objetivos y requisitos de la billetera virtual, tal como se presentó en el enunciado anterior.
- Identificar los factores clave que se deben considerar al seleccionar la tecnología y la arquitectura, como la seguridad, la escalabilidad, la confiabilidad, la facilidad de uso y el costo.

La billetera debe ofrecer seguridad, tanto para el cuidado del dinero, el logueo, como para las transacciones, ya que, son muy propensos a ataques. Se pueden incorporar aplicaciones para la doble autenticación. No debe tener retardos, ni andar lento, debe reflejar las transacciones en tiempo real. Debe ser robusta porque se manejan muchas transacciones. La billetera debe poder procesar un alto volumen de transacciones por segundo sin afectar su rendimiento.

Factores clave. Seguridad, como dije más arriba, implementar métodos de autenticación y el uso de protocolos y estándares de seguridad. Escalabilidad, para tener una app robusta, puede tener una arquitectura de microservicios o monolítica y bases de datos escalables. Usabilidad, un diseño centrado en el cliente, que la app sea compatible con muchas plataformas.

### 2. Selección del panel de expertos:

- Identificar y reclutar a un grupo de expertos con experiencia en las áreas relevantes, como blockchain, seguridad, desarrollo de software y arquitectura de sistemas.
- El panel de expertos debe estar compuesto por individuos con diferentes perspectivas y experiencias para garantizar la diversidad de opiniones.
- Es importante que los expertos sean independientes y no tengan conflictos de intereses.

El proceso de selección comienza con la identificación de los candidatos, donde luego de investigar se elaborará una lista de posibles expertos a través de redes profesionales, conferencias, publicaciones y recomendaciones. Ej linkedin. Luego se revisarán los antecedentes profesionales, publicaciones y proyectos relevantes de cada candidato y se realizarán entrevistas preliminares para evaluar su idoneidad y disposición a participar. Y a los seleccionados se los invitará a una entrevista formal explicando los objetivos del proyecto, y la importancia de su participación.

- Blockchain: deberán tener experiencia en criptomonedas y billeteras digitales.

- Seguridad: deben tener conocimiento en ciberseguridad con experiencia en protección de datos, autenticación y autorización.
- Desarrollo de software y arquitectura de sistemas: deben tener experiencia en la creación de aplicaciones móviles y web, y en diseño de sistemas escalables y de alta disponibilidad, conocimiento de lenguajes de programación Arquitectos de software con experiencia en diseño de sistemas escalables y de alta disponibilidad y en microservicios, contenedores y bases de datos escalables.

Para tener una variedad de perspectivas se podrían seleccionar expertos de diferentes industrias y antecedentes para obtener una variedad de perspectivas.

### 3. Elaboración del cuestionario:

- Diseñar un cuestionario que presente a los expertos una lista de opciones de tecnología y arquitectura para la billetera virtual.
- El cuestionario debe incluir preguntas que permitan a los expertos evaluar cada opción en función de los factores clave identificados en el paso 1.
- Las preguntas pueden ser de tipo Likert, abiertas o una combinación de ambas

1. Nombre:

2. Área de Especialización:

Blockchain

Seguridad

Desarrollo de Software

Arquitectura de Sistemas

3. Años de Experiencia:

4. ¿Qué tecnología de blockchain considera más apropiada para el desarrollo de la billetera virtual?

Ethereum

Bitcoin

Hyperledger Fabric

Otro (especificar): \_\_\_\_\_

5. ¿Qué tipo de monedero (wallet) considera más adecuado para la billetera virtual?

Monedero de custodia (hot wallet)

Monedero en frío (cold wallet)

Monedero de hardware

Otro (especificar): \_\_\_\_\_

6. ¿Qué tipo de arquitectura considera más apropiada para la billetera virtual?

Arquitectura centralizada

Arquitectura descentralizada (p2p)

Arquitectura híbrida

Otro (especificar): \_\_\_\_\_

7. ¿Qué medidas de seguridad adicionales recomendaría implementar para esta tecnología?

8. ¿Qué tan eficaz considera la implementación de autenticación multifactor (MFA) en la tecnología y para la billetera virtual?

Muy Ineficaz (1)

Ineficaz (2)

Neutra (3)

Eficaz (4)

Muy Eficaz (5)

9. ¿Qué otros métodos de autenticación sugiere para mejorar la seguridad de la billetera?

10. ¿Qué enfoque de diseño de la interfaz de usuario considera más adecuado?

Diseño orientado a desktop

Diseño orientado a móvil

Diseño responsivo

Otro (especificar): \_\_\_\_\_

11. ¿Qué mejoras de diseño recomendaría para hacer la interfaz más intuitiva?

#### **4. Aplicación del método Delphi:**

- Distribuir el cuestionario a los expertos de forma anónima.
- Recopilar las respuestas de los expertos y analizarlas estadísticamente.
- Sintetizar los resultados y presentarlos al panel de expertos.
- Brindar a los expertos la oportunidad de revisar y comentar los resultados.
- Realizar una segunda ronda de cuestionarios, incorporando los comentarios de la primera ronda.
- Analizar nuevamente las respuestas y presentar los resultados finales al panel de expertos.

Tecnología de blockchain preferida:

Ethereum: 60%

Bitcoin: 20%

Hyperledger Fabric: 10%

Otro: 10% (especificar)

Tipo de monedero preferido:

Monedero de custodia: 30%

Monedero en frío: 40%

Monedero de hardware: 20%

Otro: 10% (especificar)

Tipo de arquitectura preferida:

Arquitectura centralizada: 20%

Arquitectura descentralizada: 50%

Arquitectura híbrida: 20%

Otro: 10% (especificar)

Eficacia de MFA:

Muy Ineficaz: 0%

Ineficaz: 10%

Neutra: 20%

Eficaz: 50%

Muy Eficaz: 20%

Comentarios y sugerencias comunes:

Implementación de cifrado de extremo a extremo.

Uso de autenticación biométrica como complemento a MFA.

Diseño responsivo recomendado para asegurar la accesibilidad en diferentes dispositivos.

Simplificación de la navegación y reducción de pasos para realizar transacciones.

Incluir tutoriales y guías dentro de la aplicación.

1. ¿Por qué considera que la tecnología Ethereum podría ser más adecuada en comparación con Bitcoin?
2. ¿Qué ventajas ofrece Ethereum en términos de seguridad, escalabilidad y confiabilidad?
3. Algunos expertos prefieren los monederos de hardware. ¿Qué ventajas específicas ve en los monederos de hardware que no se mencionaron previamente?
4. Además de la autenticación biométrica, ¿qué otras medidas de seguridad recomendaría para complementar la autenticación multifactor?
5. ¿Qué mejoras específicas recomendaría para hacer la interfaz de usuario más intuitiva?
6. ¿Hay algún otro aspecto que considere crucial para el desarrollo de la billetera virtual y que no se haya abordado en la primera ronda?

Ethereum vs. Bitcoin

Ventajas de Ethereum:

- Soporte para contratos inteligentes con auditorías de seguridad.
- Mayor capacidad para implementar medidas de seguridad avanzadas.
- Planes futuros de mejora con Ethereum 2.0 para aumentar la capacidad de transacciones por segundo.
- Mayor flexibilidad en la implementación de soluciones de escalado, como sidechains y rollups.
- Comunidad activa de desarrolladores y soporte continuo.

Ventajas de los monederos de Hardware:

- Almacenamiento fuera de línea (cold storage) que reduce el riesgo de ataques.
- Protección contra malware y virus.

Usabilidad:

- Interfaz de usuario generalmente amigable y fácil de entender.
- Proceso de configuración sencillo y guías de uso detalladas.
- Reducción de pasos necesarios para realizar transacciones.
- Asegurar que la interfaz se adapte a diferentes dispositivos y tamaños de pantalla.
- Incluir walkthroughs y consejos dentro de la aplicación para nuevos usuarios.
- 

Medidas de seguridad adicionales

- Autenticación biométrica: uso de huellas dactilares y reconocimiento facial para acceso.

- Cifrado de extremo a extremo.

Compatibilidad:

- Asegurar que la billetera soporte una amplia gama de criptomonedas y tokens.
- Facilitar la integración con exchanges, plataformas de trading y otros servicios financieros.

## **5. Selección de la tecnología y la arquitectura:**

- Con base en los resultados del método Delphi, seleccionar la tecnología y la arquitectura que mejor se adapten a los objetivos y requisitos de la billetera virtual.
- Justificar la selección de la tecnología y la arquitectura elegidas, considerando los aportes del panel de expertos y los resultados del análisis estadístico.

Tecnología de Blockchain seleccionada: Ethereum

- Soporte robusto para contratos inteligentes y auditorías regulares para identificar y solucionar vulnerabilidades.
- Mejoras significativas con Ethereum 2.0, aumentando la capacidad de transacciones por segundo y reduciendo costos.
- Flexibilidad para implementar sidechains y rollups, gestionando eficientemente la carga de transacciones.
- Gran comunidad de desarrolladores, recursos abundantes, tutoriales y documentación que facilitan el desarrollo y la implementación de soluciones.

Tipo de monedero seleccionado: Monedero de hardware

- Almacenamiento fuera de línea que reduce significativamente el riesgo de ataques cibernéticos y accesos no autorizados.
- Protección adicional que los monederos de software no pueden ofrecer.
- Interfaces intuitivas y fáciles de usar, con guías detalladas de configuración y uso para facilitar la adopción por parte de los usuarios.

Arquitectura Descentralizada (p2p)

- Eliminación de puntos únicos de falla, mejorando la resistencia frente a ataques y fallas del servidor.
- Naturaleza peer-to-peer que permite distribuir la carga entre los nodos, mejorando rendimiento y disponibilidad.
- Capacidad de añadir y remover nodos fácilmente, adaptándose a cambios en la demanda sin grandes inversiones en infraestructura.

## **6. Documentación y comunicación:**

- Documentar cuidadosamente el proceso de toma de decisiones, incluyendo los criterios utilizados, las opciones consideradas y la justificación de la selección final.
- Comunicar la decisión tomada a las partes interesadas, incluyendo a los desarrolladores, inversores y usuarios potenciales.

### **Proceso de toma de decisiones**

A lo largo del proyecto, se siguió un proceso estructurado para seleccionar la tecnología y arquitectura más adecuada para la billetera virtual. Este proceso incluyó los siguientes pasos:

- Definición de criterios de evaluación: Se establecieron una serie de criterios clave que debían cumplir las diferentes opciones, incluyendo seguridad, escalabilidad, facilidad de desarrollo, costo, madurez de la tecnología, entre otros.
- Recopilación de opciones: Se analizaron diversas alternativas de tecnologías blockchain, tipos de monederos y arquitecturas, como Ethereum, Bitcoin, monederos de software, monederos de hardware, soluciones centralizadas, etc.
- Evaluación de opciones: Cada una de las alternativas fue evaluada en detalle considerando los criterios definidos. Se revisaron las características técnicas, fortalezas, debilidades y adecuación al contexto del proyecto.
- Consulta a expertos: Se convocó a un panel de expertos de la industria blockchain y pagos digitales para obtener sus opiniones y recomendaciones sobre las mejores opciones.
- Análisis y selección final: Tras ponderar todos los factores, se seleccionó la tecnología de Ethereum, el monedero de hardware y la arquitectura descentralizada como la combinación óptima para cumplir con los objetivos y requisitos del proyecto.

### **Justificación de la selección**

La selección de Ethereum como la tecnología blockchain se justifica por los siguientes factores clave:

- Soporte robusto para contratos inteligentes y auditorías regulares que permiten identificar y solucionar vulnerabilidades.
- Mejoras significativas previstas con la transición a Ethereum 2.0, que aumentará la capacidad de transacciones por segundo y reducirá los costos.
- Flexibilidad para implementar sidechains y rollups, lo cual permite gestionar eficientemente la carga de transacciones.
- Gran comunidad de desarrolladores y abundantes recursos, tutoriales y documentación que facilitan el desarrollo e implementación.

En cuanto al tipo de monedero, se seleccionó un monedero de hardware debido a:

- El almacenamiento fuera de línea que reduce significativamente el riesgo de ataques cibernéticos y accesos no autorizados.
- La protección adicional que los monederos de software no pueden ofrecer.
- Las interfaces intuitivas y fáciles de usar, con guías detalladas de configuración y uso para facilitar la adopción por parte de los usuarios.

Finalmente, la arquitectura descentralizada (P2P) fue elegida porque:

- Elimina los puntos únicos de falla, mejorando la resistencia frente a ataques y fallas del servidor.
- Su naturaleza peer-to-peer permite distribuir la carga entre los nodos, mejorando el rendimiento y la disponibilidad.
- Facilita añadir y remover nodos fácilmente, adaptándose a cambios en la demanda sin grandes inversiones en infraestructura.

### **Comunicación a las partes interesadas**

Se informó al equipo de desarrollo sobre las tecnologías y arquitectura seleccionadas, proporcionando detalles técnicos y documentación de soporte para que puedan proceder con el diseño e implementación de la solución.

Se presentó a los inversionistas y patrocinadores del proyecto los motivos y justificación de la selección realizada, enfatizando los beneficios en términos de seguridad, escalabilidad y eficiencia que aportan las tecnologías elegidas.

Se comunicó a los usuarios potenciales de la billetera virtual la decisión tomada, destacando las características clave de la solución, como la protección del monedero de hardware, la facilidad de uso y la solidez de la arquitectura descentralizada.