COLOMBIA POTENCIA DE LA VIDA

TIC

Creación y **uso de Wallets**

Lección 3 - Módulo 2 - Unidad 3

TALENTO TECH

AZ | PROYECTOS EDUCATIVOS

UTP Universidad Tecnológica de Pereira

Desarrollo de la sesión:

Una wallet, también conocida como cartera digital, es una aplicación o dispositivo diseñado específicamente para almacenar, gestionar y facilitar transacciones con criptomonedas. Funciona como una interfaz crucial entre el usuario y la blockchain, que es el registro público descentralizado donde se registran todas las transacciones de criptomonedas.

Una wallet almacena dos componentes esenciales para interactuar con la blockchain: la dirección pública y la clave privada. La dirección pública es una cadena alfanumérica única que actúa como el equivalente digital de una cuenta bancaria. Se utiliza para recibir fondos y cualquier persona puede verla, ya que se comparte abiertamente.

Por otro lado, la clave privada es una cadena de caracteres similar a una contraseña que es conocida únicamente por el propietario de la wallet. Es esencialmente la llave de acceso a los fondos almacenados en la dirección pública. La clave privada se utiliza para firmar digitalmente las transacciones salientes, lo que garantiza la autorización y seguridad de las mismas.

La wallet proporciona una interfaz intuitiva y fácil de usar para que los usuarios puedan visualizar su saldo de criptomonedas, realizar transacciones, y acceder a funciones adicionales como la generación de nuevas direcciones, el historial de transacciones y la configuración de seguridad.

Existen varios tipos de wallets disponibles, incluyendo:

Wallets de Software: Son aplicaciones instaladas en dispositivos como computadoras de escritorio, teléfonos inteligentes o tabletas. Estas wallets ofrecen una combinación de accesibilidad y seguridad, y pueden ser tanto hot wallets (conexión a internet) como cold wallets (sin conexión a internet).

Wallets de Hardware: Son dispositivos físicos diseñados específicamente para almacenar claves privadas de forma segura. Estas wallets ofrecen un alto nivel de seguridad, ya que las claves privadas se mantienen fuera de línea y protegidas por medidas de seguridad física.

Wallets Móviles: Son aplicaciones diseñadas específicamente para dispositivos móviles, lo que permite a los usuarios llevar sus criptomonedas consigo y realizar transacciones sobre la marcha. Estas wallets suelen ser muy convenientes, pero pueden ser más vulnerables a ataques cibernéticos si el dispositivo no está adecuadamente protegido.

Wallets de Papel: Son una forma de almacenamiento físico donde las claves privadas se imprimen en papel. Aunque son altamente seguras contra ataques cibernéticos, pueden ser vulnerables a daños físicos o pérdida si no se almacenan adecuadamente.

El proceso de creación de una wallet es fundamental para asegurar que los usuarios puedan almacenar y gestionar sus criptomonedas de manera segura. A continuación observará el proceso de creación de las **Wallets** paso a paso:

1. Generación de Claves Pública y Privada:

- La primera etapa en la creación de una wallet implica la generación de un par de claves única: una clave pública y una clave privada. La clave pública es una dirección alfanumérica que se utiliza para recibir fondos en la blockchain, mientras que la clave privada es una cadena de caracteres secreta que se utiliza para autorizar transacciones salientes desde la wallet. Estas claves se generan mediante algoritmos criptográficos y son esenciales para la seguridad de la wallet.

2. Creación de una Contraseña Segura:

- Además de las claves pública y privada, se suele requerir la creación de una contraseña segura para proteger el acceso a la wallet. Esta contraseña se utiliza para cifrar y proteger la clave privada almacenada en la wallet. Es importante que la contraseña sea lo suficientemente robusta y única para evitar el acceso no autorizado a la wallet y a los fondos almacenados en ella.

3. Verificación de la Información Proporcionada:

- Antes de finalizar el proceso de creación de la wallet, es importante que el usuario verifique cuidadosamente toda la información proporcionada. Esto incluye verificar la precisión de la clave pública y asegurarse de que la contraseña elegida sea segura y se haya ingresado correctamente. La verificación de la información ayuda a garantizar que la wallet se cree correctamente y que el usuario tenga acceso seguro a sus fondos.

La seguridad de la wallet es de suma importancia para proteger los activos digitales de los usuarios contra posibles amenazas y riesgos. Aquí se destaca la importancia de la seguridad en la creación de wallets y se ofrecen prácticas recomendadas para garantizar la protección de las claves privadas y la integridad de los fondos almacenados:

1. Protección de Claves Privadas:

- Las claves privadas son la llave de acceso a los fondos almacenados en una wallet. Por lo tanto, es fundamental mantenerlas seguras y fuera del alcance de terceros no autorizados. Se recomienda no compartir nunca las claves privadas con nadie y almacenarlas en un lugar seguro, preferiblemente fuera de línea y lejos de dispositivos conectados a Internet.

2. Uso de Wallets Seguras:

- Es importante utilizar wallets confiables y seguras de fuentes conocidas y reputadas. Se deben evitar wallets desconocidas o de origen dudoso que podrían ser vulnerables a ataques cibernéticos o fraudulentas. Además, es aconsejable mantener siempre actualizada la versión de la wallet para incorporar las últimas mejoras de seguridad y correcciones de errores.

3. Autenticación de Dos Factores (2FA):

- Muchas wallets ofrecen la opción de habilitar la autenticación de dos factores (2FA) como una capa adicional de seguridad. Esta función requiere que los usuarios ingresen un segundo método de verificación, como un código generado o enviado a través de un mensaje de texto, además de la contraseña principal para acceder a la wallet. La autenticación de dos factores puede ayudar a proteger la cuenta de accesos no autorizados incluso si la contraseña se ve comprometida.

4. Respaldo de Claves Privadas:

- Es esencial realizar copias de seguridad regulares de las claves privadas y almacenarlas de forma segura en múltiples ubicaciones. Esto garantiza que, en caso de pérdida o daño del dispositivo que contiene la wallet, el usuario aún pueda acceder a sus fondos utilizando la copia de seguridad de las claves privadas. Se recomienda utilizar métodos de respaldo seguros, como almacenamiento encriptado en dispositivos externos o servicios de almacenamiento en la nube confiables.

5. Educación sobre Phishing y Estafas:

- Los usuarios deben estar alerta ante posibles intentos de phishing y estafas diseñados para robar claves privadas y otros datos confidenciales. Se recomienda verificar siempre la autenticidad de los sitios web y las comunicaciones antes de proporcionar información confidencial. Además, se debe evitar hacer clic en enlaces sospechosos o descargar archivos adjuntos de fuentes desconocidas.

El uso de una wallet implica una serie de acciones, como la recepción de fondos, que son fundamentales para gestionar criptomonedas de manera efectiva. Aquí se detalla el proceso de recepción de fondos en una wallet, junto con ejemplos y desarrollos adicionales:

Recepción de Fondos:

Cuando un usuario desea recibir fondos en su wallet, el proceso implica seguir estos pasos:

1. Proporcionar la Dirección Pública:

- Cada wallet tiene una dirección pública única, que es una cadena alfanumérica utilizada para recibir fondos en la blockchain. El usuario debe proporcionar esta dirección pública al remitente para que este pueda enviar los fondos a la wallet correctamente.

2. Verificar la Dirección:

- Es crucial verificar que la dirección pública proporcionada sea correcta y esté libre de errores. Incluso un pequeño error tipográfico en la dirección podría resultar en la pérdida irreversible de los fondos. Algunas wallets ofrecen la opción de escanear un código QR para garantizar la precisión de la dirección.

Confirmar la Recepción:

Una vez que el remitente envía los fondos a la dirección pública de la wallet, la transacción se registra en la blockchain y se envía a la red para su confirmación. La confirmación de la transacción puede tardar unos minutos o más, dependiendo de la congestión de la red y otros factores.

Verificar el Saldo:

Después de que la transacción se confirma y se registra en la blockchain, el usuario puede verificar el saldo de su wallet para confirmar que los fondos se han recibido correctamente. La wallet mostrará el nuevo saldo disponible, que reflejará la cantidad de fondos recibidos.

+ info

Ejemplo:

Por ejemplo, supongamos que Juan quiere enviarle 0.1 Bitcoin a María. María le proporciona su dirección pública de Bitcoin, que es una cadena única de caracteres alfanuméricos. Juan utiliza esta dirección para enviar los 0.1 Bitcoin desde su wallet a la de María.

Después de unos minutos, María verifica su wallet y confirma que los 0.1 Bitcoin han sido recibidos correctamente. Ahora puede ver el saldo actualizado en su wallet, que refleja la cantidad de Bitcoin que Juan le envió.

El envío de fondos desde una wallet es un proceso clave en la gestión de criptomonedas. Aquí se detalla cómo enviar fondos desde una wallet, junto con ejemplos y desarrollo:

Envío de Fondos:

El proceso de envío de fondos desde una wallet implica seguir estos pasos:

Verificación de la Dirección del Destinatario:
Antes de iniciar el proceso de envío, es crucial verificar la dirección del destinatario para asegurarse de que sea precisa y esté libre de errores. La dirección del destinatario es una cadena única de caracteres alfanuméricos que identifica su wallet en la blockchain. Incluso un pequeño error tipográfico en la dirección podría resultar en la pérdida irreversible de los fondos.

Autorización de la Transacción:

Para autorizar la transacción y enviar los fondos, el usuario debe utilizar su clave privada correspondiente. La clave privada es esencial para demostrar la propiedad de los fondos y autorizar la transferencia. Es crucial mantener la clave privada segura y protegida en todo momento, ya que cualquier persona que tenga acceso a ella puede realizar transacciones en nombre del propietario de la wallet.

Confirmación de la Transacción:

Una vez que la transacción se ha autorizado y enviada a la red blockchain, se registra y se envía a la red para su confirmación. La confirmación de la transacción puede tardar unos minutos o más, dependiendo de la congestión de la red y otros factores. Una vez confirmada, la transacción se vuelve irreversible y los fondos se transfieren al destinatario.

+ info

Ejemplo:

Por ejemplo, supongamos que María desea enviar 0.05 Bitcoin a su amigo Juan. María inicia el proceso de envío desde su wallet y proporciona la dirección pública de la wallet de Juan como el destinatario de los fondos. Luego, ingresa la cantidad de Bitcoin que desea enviar (0.05 BTC) y firma la transacción utilizando su clave privada correspondiente.

Una vez que María confirma la transacción, esta se registra en la blockchain y se envía a la red para su confirmación. Después de unos minutos, Juan verifica su wallet y confirma que los 0.05 Bitcoin han sido recibidos correctamente.

La gestión de fondos es una parte crucial en el uso de las wallets de criptomonedas, y algunas ofrecen funciones adicionales que facilitan la compra, venta o intercambio de criptomonedas directamente desde su interfaz. A continuación se explica cómo funcionan estas funciones, junto con ejemplos y desarrollo:

Gestión de Fondos:

Algunas wallets de criptomonedas ofrecen funciones avanzadas de gestión de fondos que permiten a los usuarios realizar diversas operaciones directamente desde la interfaz de la wallet. Estas funciones pueden incluir:

+ info

Compra de Criptomonedas:

Algunas wallets permiten a los usuarios comprar criptomonedas directamente desde la aplicación utilizando métodos de pago convencionales, como tarjetas de crédito o transferencias bancarias. Esta función facilita a los usuarios adquirir criptomonedas de manera rápida y conveniente sin tener que recurrir a plataformas de intercambio externas.

Venta de Criptomonedas:

Además de la compra, algunas wallets también permiten a los usuarios vender sus criptomonedas directamente desde la interfaz de la wallet. Esto les permite convertir sus activos digitales en moneda fiduciaria y retirar los fondos a sus cuentas bancarias de manera sencilla.

Intercambio de Criptomonedas:

Otra función común en algunas wallets es la capacidad de intercambiar criptomonedas por otras directamente desde la aplicación. Esto permite a los usuarios diversificar sus carteras y aprovechar las oportunidades de mercado sin tener que utilizar servicios externos de intercambio.

+ info

Ejemplo:

Por ejemplo, supongamos que María utiliza una wallet que ofrece funciones avanzadas de gestión de fondos. Ella decide comprar 0.1 Bitcoin utilizando su tarjeta de crédito directamente desde la interfaz de la wallet. María selecciona la opción de compra, ingresa la cantidad deseada y completa el proceso de pago. Una vez confirmada la transacción, los 0.1 Bitcoin se agregan automáticamente a su saldo en la wallet.

Posteriormente, María decide intercambiar una parte de sus Bitcoin por Ethereum. Utiliza la función de intercambio de la wallet para seleccionar la cantidad de Bitcoin que desea intercambiar y la criptomoneda que desea recibir a cambio. Después de confirmar la transacción, los Bitcoin se intercambian por Ethereum y el nuevo saldo se refleja en su wallet.

Actividad:
Interacción con Wallets en Ganache

A continuación, se proporciona un código en Python que interactúa con wallets en una red local de Ganache. Sigue los pasos a continuación para ejecutar el código en tu máquina local y experimentar con la creación de cuentas y la firma de mensajes.

```
from web3 import Web3
from eth_account import Account

# Conexión a la red Ethereum utilizando web3.py y Ganache
ganache_url = 'http://127.0.0.1:7545' # La URL puede variar dependiendo de la
configuración de Ganache
web3 = Web3(Web3.HTTPProvider(ganache_url))

# Verificación de la conexión a Ganache
if web3.isConnected():
 print("Conexión exitosa a Ganache.")

# Obtención de cuentas disponibles en Ganache
```

```python
accounts = web3.eth.accounts
 if len(accounts) > 0:
    active_account = accounts[0] # Seleccionar la primera cuenta como activa
    print("Cuenta activa:", active_account)

    # Creación de una nueva cuenta Ethereum utilizando web3.py
    new_account = web3.eth.account.create()
    print("Nueva cuenta creada:")
    print("Dirección:", new_account.address)
    print("Clave privada:", new_account.privateKey.hex())
```

```
# Firmar un mensaje utilizando la clave privada de la nueva cuenta
message = "Hello, Ganache!"
signature = web3.eth.account.sign_message(message,
private_key=new_account.privateKey)
print("Firma del mensaje:", signature.signature.hex())
else:
print("No se encontraron cuentas en Ganache.")
else:
print("No se pudo conectar a Ganache.")
```

Pasos para hacerlo funcionar:

Confirmación de la Transacción:

- Descarga e instala Ganache desde el sitio web oficial:
- Sigue las instrucciones de instalación proporcionadas para tu sistema operativo.

Inicio de Ganache:

- Una vez instalado, inicia Ganache desde tu sistema operativo.

Ejecución del Código:

- Copia y pega el código anterior en un archivo Python en tu editor de código preferido (por ejemplo, Visual Studio Code, PyCharm, etc.).
- Guarda el archivo con un nombre adecuado, como wallet_interaction.py.
- Abre una terminal o línea de comandos y navega hasta el directorio donde guardaste el archivo Python.
- Ejecuta el archivo Python ejecutando el comando python wallet_interaction.py en la terminal.

Verificación del Funcionamiento:

- Si todo va bien, deberías ver mensajes en la terminal que indican que la conexión a Ganache fue exitosa, así como información sobre la cuenta activa, la nueva cuenta creada y la firma del mensaje.
- Verifica que no haya errores durante la ejecución y que todos los pasos se completen con éxito.

En esta actividad, has tenido la oportunidad de interactuar con wallets en una red local de Ganache utilizando Python y las bibliotecas web3.py y eth_account. A través de los pasos proporcionados, has explorado la creación de nuevas cuentas Ethereum, la firma de mensajes y otros aspectos relacionados con la gestión de wallets en el entorno de desarrollo de blockchain.