COLOMBIA POTENCIA DE LA VIDA

TIC

Conceptos de web 3.0 y uso **de blockchain en plataformas web**

Lección 1- Módulo 2 - Unidad 2

TALENTO TECH

AZ | PROYECTOS EDUCATIVOS

UTP Universidad Tecnológica de Pereira

Desarrollo de la sesión:

Esta lección, es un punto de partida para adquirir una comprensión profunda de cómo estas tecnologías están moldeando el futuro del espacio digital. A través de la exploración de los principios básicos del blockchain y su integración en la web 3.0, los estudiantes estarán equipados para identificar las oportunidades y desafíos que estas tecnologías presentan en el panorama actual.

Durante la sesión, se implementará un enfoque crítico para evaluar el impacto y la viabilidad de la implementación de blockchain en plataformas web. Se destacará la importancia de entender cómo se utilizan los principios de seguridad, descentralización y consenso en esta tecnología para garantizar la integridad y la confianza en las transacciones en línea. Asimismo, se abordarán los desafíos de escalabilidad y consumo de recursos, junto con las soluciones propuestas para abordar estos aspectos cruciales en el desarrollo y adopción masiva de la tecnología.

Al finalizar la sesión, se adquirirá una comprensión sólida de los conceptos de web 3.0 y blockchain, así como la capacidad de identificar oportunidades de aplicación y resolver desafíos en el contexto de las plataformas web. Estarán preparados para explorar y aprovechar las infinitas posibilidades que estas tecnologías ofrecen para innovar y mejorar las experiencias en línea en el futuro.

Exploración de conceptos clave:

Una parte integral de la web 3.0 es la integración de blockchain en plataformas web. El blockchain, una tecnología descentralizada que permite el almacenamiento y verificación de datos de manera distribuida y segura, es un componente clave de esta nueva fase de la web. El blockchain proporciona una base sólida para garantizar la seguridad, transparencia y confianza en las transacciones en línea al eliminar la necesidad de intermediarios y proporcionar un registro inmutable de datos.

Al comprender los principios fundamentales del blockchain, incluidos los conceptos de bloques, cadenas de bloques, consenso y descentralización, los usuarios pueden apreciar cómo esta tecnología está transformando las plataformas web. Desde la gestión de identidades digitales hasta la trazabilidad de productos y la ejecución de contratos inteligentes, el blockchain está siendo utilizado en una variedad de aplicaciones en línea para mejorar la seguridad y eficiencia de las transacciones.

Una de las características más importantes del blockchain es su capacidad para garantizar la integridad de la información al proporcionar un registro inmutable y verificable de datos. Esto significa que una vez que se registra la información en la cadena de bloques, no se puede modificar ni eliminar, lo que aumenta la confianza en la autenticidad de los datos y reduce el riesgo de fraude o manipulación.

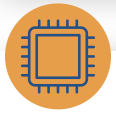
Además, el blockchain también está facilitando la descentralización de las plataformas web al permitir la creación de aplicaciones y servicios que operan sin la necesidad de un servidor centralizado. Esto significa que los usuarios tienen un mayor control sobre sus datos y transacciones, lo que puede conducir a una mayor privacidad y autonomía en línea.

Generación de firmas digitales:

A continuación se nombran algunas plataformas web que ya utilizan blockchain:

OpenSea:
Un mercado para comprar y vender NFTs (tokens no fungibles).

Rarible:
Otra plataforma para comprar y vender NFTs.



Augur:
Un mercado de predicción descentralizado.

Gnosis:
Otra plataforma de predicción descentralizada.

Aave:
Un protocolo de préstamos descentralizado.

Compound:
Otro protocolo de préstamos descentralizado.

COLOMBIA POTENCIA DE LA VIDA

TIC

La web 3.0 se define como una red inteligente, personalizada y conectada, que cuenta con la siguiente propiedades:

1. Búsquedas inteligentes:

- Clasificación personalizada: La Web 3.0 no solo clasifica páginas web, sino que también las relaciona con las necesidades y características de cada usuario.
- Experiencia personalizada: Al conectarse a internet, cada usuario disfruta de una plataforma adaptada a sus intereses y preferencias.

2. Evolución de las redes sociales:

- Crecimiento exponencial: Las comunidades sociales en la red aumentan en número y complejidad.
- Conectividad diversificada: Se multiplican las formas de conectarse a estas redes, creando una experiencia social más rica.

3. Mayor rapidez:

- Funcionalidades exigentes: Las nuevas funcionalidades de la Web 3.0 demandan una conexión a internet más rápida.
- Banda ancha como respuesta: Las operadoras de telecomunicaciones implementan conexiones de banda ancha para garantizar una experiencia fluida.

4. Conectividad multidispositivo:

- Más allá del PC: La Web 3.0 se adapta a celulares, tablets, relojes inteligentes y una amplia gama de dispositivos.
- Acceso ubicuo: Los usuarios pueden conectarse desde cualquier lugar y en cualquier momento.

5. Contenido libre:

- Predominio del software libre: Los programas libres y las licencias Creative Commons se vuelven más comunes.
- Acceso abierto al conocimiento: Se facilita la difusión y el intercambio de información.

TALENTO TECH

AZ | PROYECTOS EDUCATIVOS

Universidad Tecnológica de Pereira

La web 3.0 se define como una red inteligente, personalizada y conectada, que cuenta con la siguiente propiedades:

6. Espacios tridimensionales:

- Visualización innovadora: La Web 3.0 permite acceder a la información en espacios tridimensionales.
- Experiencias inmersivas: Google Earth es un ejemplo de cómo la visualización 3D enriquece la experiencia del usuario.

7. Web geoespacial:

- Información contextualizada: Los usuarios pueden acceder a información relevante en base a su ubicación geográfica.
- Servicios personalizados: La geolocalización permite ofrecer servicios más precisos y relevantes.

8. Navegación intuitiva:

- Estandarización del diseño: Se busca facilitar la experiencia del usuario en la navegación.
- Espacios personalizables: Los usuarios pueden adaptar la web a sus necesidades y preferencias.

9. Computación en la nube:

- Almacenamiento y procesamiento: La web se convierte en un espacio de almacenamiento y procesamiento de datos.
- Computador universal: La nube permite ejecutar programas y aplicaciones desde cualquier dispositivo.

10. Vinculación de datos:

- Unificación de la información: Los servicios de información integran datos de diversas fuentes.
- Respuestas completas: Los usuarios obtienen respuestas más completas y precisas a sus necesidades.

COLOMBIA POTENCIA DE LA VIDA

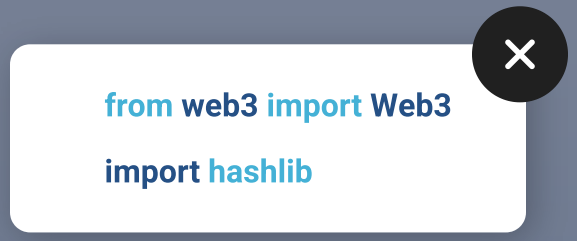
TIC

Caso de Uso de una Plataforma de Votación Descentralizada:

Enunciado: Simular el proceso de emisión de votos en una plataforma de votación descentralizada utilizando blockchain. Cada voto debe estar firmado digitalmente por el votante para garantizar su autenticidad y anonimato. Solución: Utiliza un lenguaje de programación como JavaScript para simular el proceso de emisión de votos en la plataforma.

Puedes utilizar bibliotecas de criptografía como crypto-js para generar claves privadas y firmas digitales. Además, puedes utilizar una red blockchain como Ethereum para registrar los votos y garantizar su integridad y transparencia. En la aplicación, los votantes pueden seleccionar sus opciones de voto y firmar digitalmente su voto antes de enviarlo a la red blockchain para su registro.

+ info


from web3 import Web3
import hashlib

```
# Conexión a la red Ethereum
web3 =
Web3(Web3.HTTPProvider('https://mainnet.infura.io/v3/your_infura_proje
ct_id'))

# ABI y dirección del contrato inteligente de votación
contractABI = [...] # ABI del contrato
contractAddress = '0x...' # Dirección del contrato

# Instanciar el contrato
contract = web3.eth.contract(address=contractAddress, abi=contractABI)
```

```
# Función para simular el proceso de emisión de votos
def emitir_voto(voto, clave_privada):
  # Firmar digitalmente el voto con la clave privada del votante
  firma = hashlib.sha256(voto.encode() +
clave_privada.encode()).hexdigest()

# Enviar el voto y la firma al contrato inteligente
 cuenta =
web3.eth.account.privateKeyToAccount(clave_privada)
 transaccion = contract.functions.emitirVoto(voto,
firma).buildTransaction({
    'from': cuenta.address,
    'gas': web3.eth.estimateGas({'from': cuenta.address}),
    'gasPrice': web3.eth.gasPrice,
    'nonce': web3.eth.getTransactionCount(cuenta.address),
})
```

```
# Firmar la transacción con la clave privada del votante
 transaccion_firmada = web3.eth.account.signTransaction(transaccion,
clave_privada)

 # Enviar la transacción firmada a la red Ethereum
 respuesta =
web3.eth.sendRawTransaction(transaccion_firmada.rawTransaction)

 return respuesta.hex()
```

```
# Ejemplo de uso: Emitir un voto con una clave privada simulada
voto = 'Candidato A'
clave_privada =
'0x123456789abcdef123456789abcdef123456789abcdef123456789abcd
ef1234'
resultado = emitir_voto(voto, clave_privada)
print('Voto emitido exitosamente:', resultado)
```

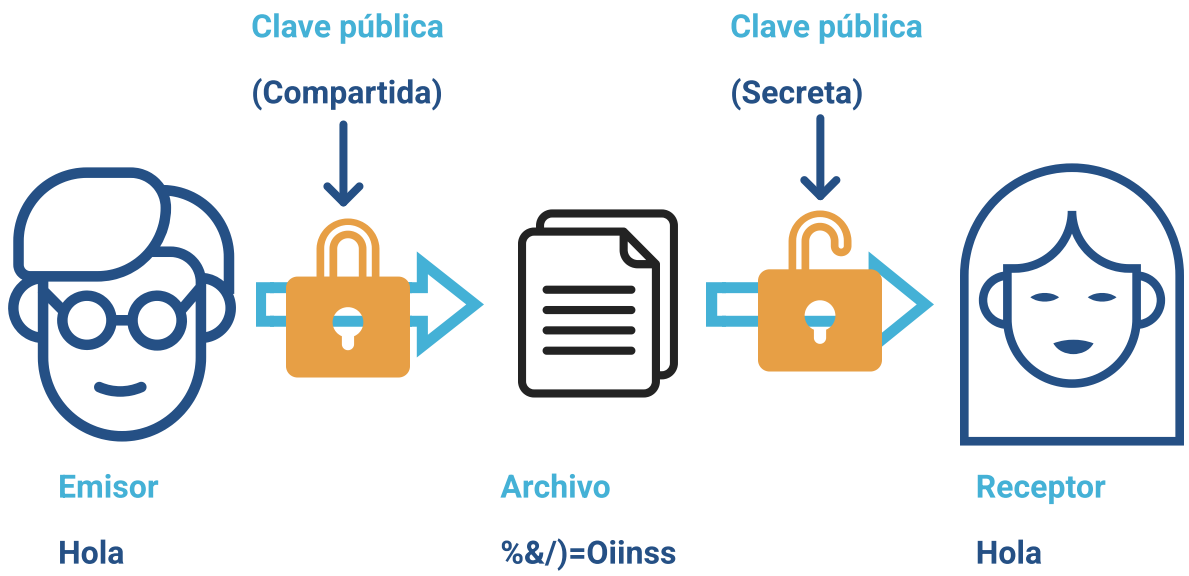
#En el ejemplo anterior, se utilizó la biblioteca **web3** para interactuar con la red Ethereum y el contrato inteligente de votación. La función **emitir_voto** simula el proceso de emisión de votos, generando una firma digital para cada voto utilizando la clave privada del votante. Luego, construimos y firmamos la transacción que contiene el voto y la firma, y la enviamos a la red Ethereum para su procesamiento. Finalmente, mostramos el hash de la transacción que confirma que el voto ha sido emitido con éxito.

Estrategias de seguridad y mejores prácticas:

Es fundamental abordar las estrategias de seguridad y las mejores prácticas para garantizar la integridad y confiabilidad de las transacciones en línea. Una de las principales estrategias de seguridad en la integración de blockchain en plataformas web es la autenticación de usuarios mediante claves criptográficas. Al implementar un sistema de autenticación basado en claves públicas y privadas, se puede verificar la identidad de los usuarios de manera segura y reducir el riesgo de acceso no autorizado a las plataformas.

Otra estrategia clave es la gestión adecuada de claves criptográficas. Las claves privadas deben mantenerse en secreto y protegidas en todo momento, preferiblemente utilizando mecanismos de almacenamiento seguro como billeteras de hardware. Además, es importante implementar procedimientos de gestión de claves que incluyan la rotación regular de claves y la revocación de acceso en caso de compromiso.

+ info


Clave pública
(Compartida)
Clave pública
(Secreta)
Emisor
Hola
Archivo
%&/)=Oiinss
Receptor
Hola

Además de la autenticación y la gestión de claves, es crucial implementar medidas de protección de datos para garantizar la confidencialidad y la privacidad de la información del usuario. Esto incluye el cifrado de datos sensibles en reposo y en tránsito, así como la implementación de políticas de acceso y control de datos para limitar el acceso a la información solo a aquellos usuarios autorizados.
Otra mejor práctica es la auditoría y el monitoreo continuo de la plataforma para detectar y responder rápidamente a posibles vulnerabilidades o ataques. Esto puede incluir la implementación de registros de actividad, sistemas de detección de intrusiones y análisis de seguridad en tiempo real para identificar y mitigar amenazas en tiempo real.

Además, se recomienda realizar pruebas de penetración y evaluaciones de seguridad de forma regular para identificar y corregir posibles vulnerabilidades en la plataforma. Estas pruebas deben realizarse tanto en el nivel de aplicación como en el nivel de infraestructura para garantizar una protección completa contra ataques.

Por último, pero no menos importante, la educación y la concienciación del usuario son fundamentales para garantizar la seguridad en la plataforma. Los usuarios deben estar informados sobre las mejores prácticas de seguridad, como la creación de contraseñas seguras, el uso de la autenticación de dos factores y la protección de sus claves privadas. Además, deben estar al tanto de las amenazas comunes, como el phishing y el malware, y saber cómo detectar y evitarlos.

Caso de Uso de una Plataforma de Votación Descentralizada:

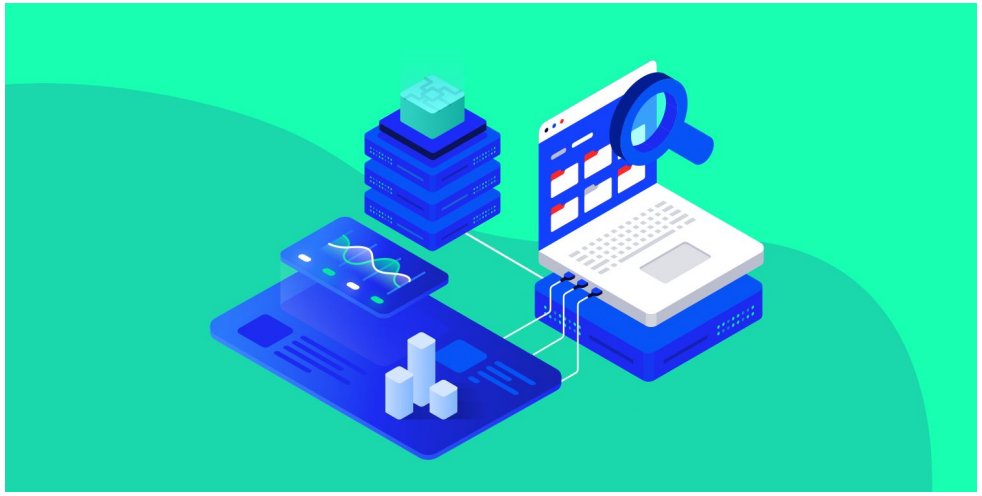
Las pruebas de penetración y las evaluaciones de seguridad son prácticas fundamentales para garantizar la integridad y la protección de las plataformas web que utilizan tecnologías como web 3.0 y blockchain. Estas pruebas permiten identificar vulnerabilidades y debilidades en la seguridad de la plataforma, así como evaluar su resistencia frente a posibles ataques.

En el contexto de web 3.0 y blockchain, las pruebas de penetración pueden incluir la evaluación de la seguridad de los contratos inteligentes utilizados en la plataforma. Los contratistas inteligentes son programas informáticos que se ejecutan en la cadena de bloques y pueden contener vulnerabilidades que podrían ser explotadas por atacantes. Las pruebas de penetración se centran en identificar y explotar posibles vulnerabilidades en estos contratos inteligentes, como errores en la lógica del negocio, condiciones de carrera y vulnerabilidades de desbordamiento de entero.

Además de las pruebas de penetración de contratos inteligentes, también se deben realizar evaluaciones de seguridad de la infraestructura subyacente de la plataforma. Esto incluye la evaluación de la seguridad de los nodos de la red blockchain, la seguridad de la capa de transporte (por ejemplo, SSL/TLS), la configuración de firewalls y la protección contra ataques de denegación de servicio (DDoS).

Otro aspecto importante de las pruebas de seguridad en el contexto de web 3.0 y blockchain es la evaluación de la seguridad de las billeteras digitales utilizadas para almacenar claves privadas. Las billeteras digitales son un objetivo común para los atacantes, ya que contienen las claves privadas que permiten acceder y controlar los activos digitales en la cadena de bloques. Las pruebas de seguridad de las billeteras digitales se centran en identificar posibles vulnerabilidades, como la falta de cifrado adecuado o la exposición de claves privadas.

Es importante tener en cuenta que las pruebas de penetración y las evaluaciones de seguridad deben realizarse de forma regular y sistemática, ya que las amenazas y vulnerabilidades pueden cambiar con el tiempo. Además, es crucial que las pruebas sean realizadas por profesionales de seguridad calificados que tengan experiencia en el uso de tecnologías de web 3.0 y blockchain, así como en la identificación y mitigación de posibles riesgos y vulnerabilidades. En resumen, las pruebas de penetración y las evaluaciones de seguridad son prácticas esenciales para garantizar la protección y la integridad de las plataformas web que utilizan tecnologías emergentes como web 3.0 y blockchain.



Las evaluaciones de seguridad, también conocidas como pruebas de penetración, no solo se limitan a la identificación de vulnerabilidades. Estas pruebas también son herramientas valiosas para:

- **Garantizar el cumplimiento de las políticas de seguridad:**
Permiten verificar que la organización cumple con las normas y reglamentos internos de seguridad, así como con los requisitos de certificaciones como ISO 27001 o PCI-DSS.

- **Medir la sensibilización del personal:**
Evalúan el conocimiento y la capacidad de los empleados para identificar y responder a incidentes de seguridad.

- **Fortalecer la capacidad de respuesta ante incidentes:**
Ayudan a la organización a mejorar su capacidad para detectar, contener y mitigar los ataques cibernéticos.

En un proceso integral, durante las evaluaciones de seguridad, se siguen la siguiente serie de pasos:

1. Detección de vulnerabilidades:
Se utilizan diferentes técnicas para identificar las brechas de seguridad en los sistemas informáticos de la organización.

2. Reporte de vulnerabilidades:
Se informa a los administradores del sistema sobre las vulnerabilidades detectadas, con el fin de que puedan implementar las medidas correctivas necesarias.

3. Implementación de correcciones:
Los administradores del sistema aplican las medidas necesarias para mitigar las brechas de seguridad.

4. Retesting:
Se realizan nuevas pruebas para verificar que las correcciones hayan sido efectivas y que las vulnerabilidades hayan sido remediadas.

Beneficios de las evaluaciones de seguridad:

Uno de los principales beneficios de las evaluaciones de seguridad es la identificación proactiva de vulnerabilidades y debilidades en los sistemas y aplicaciones de una organización. Al analizar minuciosamente la infraestructura y las configuraciones de seguridad, las evaluaciones pueden detectar problemas potenciales antes de que sean aprovechados por atacantes, lo que permite a la organización tomar medidas preventivas para mitigar los riesgos.

Además de identificar vulnerabilidades, las evaluaciones de seguridad también ayudan a priorizar y remediar las amenazas de manera efectiva. Al proporcionar una evaluación detallada de los riesgos y sus impactos potenciales, las organizaciones pueden asignar recursos y esfuerzos de manera más eficiente para abordar las vulnerabilidades más críticas y urgentes, reduciendo así la exposición a posibles ataques.

Otro beneficio importante de las evaluaciones de seguridad es el cumplimiento normativo y regulatorio. Muchas industrias están sujetas a regulaciones estrictas en cuanto a la protección de datos y la seguridad de la información, y las evaluaciones de seguridad ayudan a garantizar el cumplimiento de estas normativas al identificar y abordar posibles violaciones.

Además, las evaluaciones de seguridad también pueden mejorar la confianza y la credibilidad de una organización ante sus clientes, socios comerciales y otras partes interesadas. Al demostrar un compromiso con la protección de los datos y la seguridad de la información a través de evaluaciones regulares, las organizaciones pueden construir y mantener la confianza con sus partes interesadas, lo que puede ser crucial para el éxito a largo plazo.

A continuación se definen algunos de los beneficios de realizar la pruebas de seguridad pertinentes:

Reducción del riesgo de ataques cibernéticos:
Al identificar y corregir las vulnerabilidades, se reduce la probabilidad de que un atacante pueda explotarlas para obtener acceso a la información o los sistemas de la organización.

Mejora de la postura de seguridad:
Las evaluaciones de seguridad ayudan a la organización a mejorar su postura de seguridad general y a estar mejor preparada para enfrentar los ataques cibernéticos.

Cumplimiento normativo:
Las evaluaciones de seguridad pueden ayudar a la organización a cumplir con las normas y reglamentos de seguridad, así como con los requisitos de certificaciones como ISO 27001 o PCI-DSS.