



MCR09. Blockchain avanzado



MCR09

Blockchain avanzado

El contenido formativo se adecúa a la unidad de competencia UC1214_3 del Catálogo Nacional de Cualificaciones Profesionales (CNCP).

Duración: 50 horas

Modalidad: 100% online

Requisitos y conocimientos previos: no se requiere nivel académico previo, pero al ser en modalidad online es necesario poseer conocimientos básicos de informática, así como habilidades básicas de comunicación lingüística que permitan el aprendizaje y el seguimiento de la formación.



Objetivos

Objetivos generales

- Aplicar las bases criptográficas que sustentan el funcionamiento de blockchain, así como los principales sistemas de consenso y los mecanismos de resolución de conflictos en las cadenas de bloques públicas.
 - Aplicar los protocolos de consenso y de resolución de conflictos en las cadenas públicas.
- 

Objetivos específicos

- Comprender el concepto de función matemática y, en particular, de funciones unidireccionales.
- Identificar las funciones hash criptográficas como funciones unidireccionales.
- Apreciar las propiedades de las funciones hash criptográficas.
- Valorar algunas aplicaciones de las funciones hash criptográficas
- Conocer algunos de los fundamentos de la criptografía moderna.
- Diferenciar entre criptografía simétrica y asimétrica.
- Enumerar algunas aplicaciones cotidianas de la criptografía.
- Relacionar la criptografía con la tecnología blockchain
- Valorar el papel de las funciones hash y de la criptografía asimétrica en Bitcoin.
- Establecer analogías y diferencias entre las transacciones de criptomonedas y transferencias bancarias.
- Diferenciar los distintos tipos de nodos y conocer cuál es su papel en la red.
- Comprender las fortalezas de una red descentralizada.
- Valorar la descentralización para la resolución de problemas como el doble gasto.
- Conocer los precedentes de la prueba de trabajo y comprender su funcionamiento como mecanismo de consenso.
- Identificar los mecanismos que intervienen en el proceso de «minería».
- Simular cómo se añade un nuevo bloque a la cadena.

• Contenidos

Unidad 1: Fundamentos criptográficos de blockchain.

1. Distinción de las funciones hash criptográficas y sus aplicaciones.
 - 1.1. Definición.
 - 1.2. Definición. Funciones.
 - 1.3. Definición. Funciones unidireccionales: definición informal.
 - 1.4. Definición. Funciones unidireccionales: suma de cifras y descomposición en factores primos.
 - 1.5. Definición. Funciones unidireccionales: algunas precisiones.
 - 1.6. Definición. Los orígenes de blockchain: Bitcoin.
 - 1.7. Principales propiedades: unidireccionalidad, resistencia a colisiones y ocultación I.
 - 1.8. Principales propiedades: unidireccionalidad, resistencia a colisiones y ocultación II.
 - 1.9. Principales propiedades: unidireccionalidad, resistencia a colisiones y ocultación III.
 - 1.10. Aplicaciones prácticas de carácter general: integridad y comparación de documentos electrónicos.
2. Identificación de las bases de la criptografía y sus aplicaciones.
 - 2.1. Introducción.
 - 2.2. Criptografía simétrica: definición y ejemplos (AES).
 - 2.3. Criptografía simétrica: definición y ejemplos (AES). Las funciones unidireccionales con trampa.
 - 2.4. Criptografía asimétrica: definición y ejemplos (RSA, ECDSA).

- 2.5. Criptografía asimétrica: definición y ejemplos (RSA, ECDSA):
Criptografía asimétrica. Algunas precisiones.
- 2.6. Criptografía asimétrica: definición y ejemplos (RSA, ECDSA):
principales algoritmos asimétricos y consideraciones adicionales.
- 2.7. Criptografía asimétrica: definición y ejemplos (RSA, ECDSA).
Conclusiones.
- 2.8. Aplicaciones prácticas de carácter general: la firma digital y el
cifrado de documentos o comunicaciones electrónicas.
- 2.9. Aplicaciones prácticas de carácter general: la firma digital y el
cifrado de documentos o comunicaciones electrónicas. Propiedades
de la criptografía.
- 2.10. Aplicaciones prácticas de carácter general: la firma digital y el
cifrado de documentos o comunicaciones electrónicas. Algunas
aplicaciones.
3. Aplicación de la criptografía y las funciones hash en blockchain.
 - 3.1. Funciones hash en blockchain: garantía de la integridad de los datos
de la cadena.
 - 3.2. Criptografía asimétrica en blockchain: acreditación de la propiedad
de activos digitales.
 - 3.3. Criptografía asimétrica en blockchain: acreditación de la propiedad
de activos digitales. Transferencias bancarias y transacciones
Bitcoin.
 - 3.4. Criptografía asimétrica en blockchain: acreditación de la propiedad
de activos digitales. Las diferencias.

Unidad 2: Mecanismos de consenso y resolución de conflictos en cadenas públicas.

1. Distinción de los principales mecanismos de consenso en blockchain.
 - 1.1. Necesidad de protocolos de consenso por la descentralización de la red.
 - 1.2. Necesidad de protocolos de consenso por la descentralización de la red: Tipos de nodos.
 - 1.3. Protocolo de prueba de trabajo: «minería» y nodos «mineros».
 - 1.4. Protocolo de prueba de trabajo: «minería» y nodos «mineros». Impedir el doble gasto.
 - 1.5. Protocolo de prueba de trabajo: «minería» y nodos «mineros». La honestidad de los mineros: Fijación del mecanismo de consenso.
 - 1.6. Protocolo de prueba de trabajo: «minería» y nodos «mineros». La honestidad de los mineros: Sistema de incentivo.
 - 1.7. Protocolo de prueba de trabajo: «minería» y nodos «mineros». La prueba de trabajo.
 - 1.8. Protocolo de prueba de trabajo: «minería» y nodos «mineros». El precedente: hashcash.
 - 1.9. Protocolo de prueba de trabajo: «minería» y nodos «mineros». La prueba de trabajo en Bitcoin.
 - 1.10. Detalle de una transacción con prueba de trabajo.
 - 1.11. Detalle de una transacción con prueba de trabajo. Los protagonistas: Alice, Bob y Eve.
 - 1.12. Emisión de activos digitales como recompensa a comportamientos honestos.

- 
- 
- 1.13. Emisión de activos digitales como recompensa a comportamientos honestos. Más sobre el nonce.
 - 2. Identificación de posibles conflictos y conocimientos de su resolución.
 - 2.1. Desdoblamientos de la cadena: descripción del fenómeno y protocolo de actuación previo.
 - 2.2. Doble gasto: definición del problema y maduración de la recompensa.
 - 2.3. Doble gasto: definición del problema y maduración de la recompensa. Otros intentos de doble gasto.
 - 2.4. Sostenibilidad: rentabilidad de la «minería» y ataque del 51%.
 - 2.5. Sostenibilidad: rentabilidad de la «minería» y ataque del 51%. Rentabilidad de la minería.
 - 2.6. Sostenibilidad: rentabilidad de la «minería» y ataque del 51%. El halving.
 - 2.7. Sostenibilidad: rentabilidad de la «minería» y ataque del 51%. ¿El final de la minería?
 - 2.8. Sostenibilidad: rentabilidad de la «minería» y ataque del 51%. El ataque del 51%.
 - 3. Aplicación del protocolo de prueba de trabajo en cadenas públicas.
 - 3.1. Uso de app para móviles sobre cadena de bloques de prueba.