

Blockchain Avanzado

Duración: 60 horas

Modalidad: Online

Coste Bonificable: 420 €

Objetivos

El presente curso FCOI04 Blockchain Avanzado es una especialidad formativa de la Familia Profesional de la Formación Complementaria. El curso FCOI04 Blockchain Avanzado tiene como objetivo que el alumno sea capaz de emplear las bases criptográficas que sostienen el blockchain, conociendo para ello los sistemas y mecanismos más importantes en la resolución de conflictos de las cadenas de bloques públicas.

Temario

UNIDAD DIDÁCTICA 1. FUNDAMENTOS CRIPTOGRÁFICOS DE BLOCKCHAIN

1. Distinción de las funciones hash criptográficas y sus aplicaciones
 - Definición
 - Principales propiedades: unidireccionalidad, resistencia a colisiones y ocultación.
 - Aplicaciones prácticas de carácter general: integridad y comparación de documentos electrónicos.
2. Identificación de las bases de la criptografía y sus aplicaciones
 - Introducción
 - Criptografía simétrica: definición y ejemplos (AES).

MATRICÚLESE



- Criptografía asimétrica: definición y ejemplos (RSA, ECDSA).
- Aplicaciones prácticas de carácter general: la firma digital y el cifrado de documentos o comunicaciones electrónicas.

3. Aplicación de la criptografía y las funciones hash en blockchain

- Funciones hash en blockchain: garantía de la integridad de los datos de la cadena.
- Criptografía asimétrica en blockchain: acreditación de la propiedad de activos digitales.

UNIDAD DIDÁCTICA 2. MECANISMOS DE CONSENSO Y RESOLUCIÓN DE CONFLICTOS EN CADENAS PÚBLICAS

1. Distinción de los principales mecanismos de consenso en blockchain

- Necesidad de protocolos de consenso por la descentralización de la red.
- Protocolo de prueba de trabajo: «minería» y nodos «mineros».
- Detalle de una transacción con prueba de trabajo.
- Emisión de activos digitales como recompensa a comportamientos honestos.

2. Identificación de posibles conflictos y conocimiento de su resolución

- Desdoblamientos de la cadena: descripción del fenómeno y protocolo de actuación previsto.
- Doble gasto: definición del problema y maduración de la recompensa.
- Sostenibilidad: rentabilidad de la «minería» y ataque del 51%.

3. Aplicación del protocolo de prueba de trabajo en cadenas públicas

- Uso de app para móviles sobre cadena de bloques de prueba.