Guía didáctica

Blockchain avanzado

OBJETIVO GENERAL

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.

Objetivos específicos

- Aplicar las bases criptográficas como garantía para la integridad de los datos de la cadena y la propiedad de los activos digitales.
- Aplicar los protocolos de consenso y de resolución de conflictos en las cadenas públicas.

Módulos formativos

- Módulo 1 (25 horas) Fundamentos criptográficos de blockchain.
- Módulo 2 (25 horas) Mecanismos de consenso y resolución de conflictos en cadenas públicas

Contenidos

MODULO I. FUNDAMENTOS CRIPTOGRÁFICOS DEL BLOCKCHAIN (25 horas)	
MÓDULOS FORMATIVOS	**TEMAS**
Módulo I. Fundamentos Criptográficos del Blockchain (25 horas)	Tema 1. Distinción de las funciones flash criptográficas y sus aplicaciones. • Definición • Principales propiedades: unidireccionalidad, resistencia a colisiones y ocultación. • Aplicaciones prácticas de carácter general: integridad y comparación de documentos electrónicos.
	Tema 2. Identificación de las bases de la criptografía y sus aplicaciones

	• Introducción • Criptografía simétrica: definición y ejemplos (AES). • Criptografía asimétrica: definición y ejemplos (RSA, ECDSA). • Aplicaciones prácticas de carácter general: la firma digital y el cifrado de documentos o comunicaciones electrónicas.
	Tema 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.
	Tema 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.
Módulo II. Mecanismos de consenso y resolución de conflictos en cadenas públicas (25 horas)	Tema 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%.
	Tema 3. Aplicación del protocolo de prueba de trabajo en cadenas públicas • Uso de app para móviles sobre cadena de bloques de prueba.