FCOI04. Blockchain avanzado

Sku: PDFCOI04

Horas: 50

Formato: HTML

OBJETIVOS

Objetivo General

- 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.

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.
- Entender los motivos que producen desdoblamientos de la cadena y valorar cómo se resuelven en Bitcoin.

- Distinguir algunos factores de riesgo en la sostenibilidad de Bitcoin y comprender las soluciones.

CONTENIDOS

Unidad 1: Fundamentos criptográficos de blockchain. • Distinción de las funciones hash criptográficas y sus aplicaciones. o Definición. o Definición. Funciones. o Definición. Funciones unidireccionales: definición informal. o Definición. Funciones unidireccionales: suma de cifras y descomposición en factores primos. o Definición. Funciones unidireccionales: algunas precisiones. o Definición. Los orígenes de blockchain: Bitcoin. o Principales propiedades: unidireccionalidad, resistencia a colisiones y ocultación I. o Principales propiedades: unidireccionalidad, resistencia a colisiones y ocultación II. o Principales propiedades: unidireccionalidad, resistencia a colisiones y ocultación III. o Aplicaciones prácticas de carácter general: integridad y comparación de documentos electrónicos. **• Identificación de las bases de la criptografía y sus aplicaciones.** o Introducción. o Criptografía simétrica: definición y ejemplos (AES). o Criptografía simétrica: definición y ejemplos (AES). Las funciones unidireccionales con trampa. o Criptografía asimétrica: definición y ejemplos (RSA,ECDSA). o Criptografía asimétrica: definición y ejemplos (RSA,ECDSA): Criptografía asimétrica. Algunas precisiones. o Criptografía asimétrica: definición y ejemplos (RSA,ECDSA): principales algoritmos asimétricos y consideraciones adicionales. o Criptografía asimétrica: definición y ejemplos (RSA,ECDSA). Conclusiones. o Aplicaciones prácticas de carácter general: la firma digital y el cifrado de documentos o comunicaciones electrónicas. o Aplicaciones prácticas de carácter general: la firma digital y el cifrado de documentos o comunicaciones electrónicas. Propiedades de la criptografía. o Aplicaciones prácticas de carácter general: la firma digital y el cifrado de documentos o comunicaciones electrónicas. Algunas aplicaciones. **• Aplicación de la criptografía y las funciones hash en blockchain.** o Funciones hash en blockchain: garantía de la integridad de los datos de la cadena. o Criptografía asimétrica en blockchain: acreditación de la propiedad de activos digitales. o Criptografía asimétrica en blockchain: acreditación de la propiedad de activos digitales. Transferencias bancarias y transacciones Bitcoin. o 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. • Distinción de los principales mecanismos de consenso en blockchain** o Necesidad de protocolos de consenso por la descentralización de la red. o Necesidad de protocolos de consenso por la descentralización de la red: Tipos de nodos. o Protocolo de prueba de trabajo: «minería» y nodos «mineros». o Protocolo de prueba de trabajo: «minería» y nodos «mineros». Impedir el doble gasto. o Protocolo de prueba de trabajo: «minería» y nodos «mineros». La honestidad de los mineros: Fijación del mecanismo de consenso. o Protocolo de prueba de trabajo: «minería» y nodos «mineros». La honestidad de los mineros: Sistema d incentivo. o Protocolo de prueba de trabajo: «minería» y nodos «mineros». La prueba de trabajo. o Protocolo de prueba de trabajo: «minería» y nodos «mineros». El precedente: hashcash. o Protocolo de prueba de trabajo: «minería» y nodos «mineros». La prueba de trabajo en Bitcoin. o Detalle de una transacción con prueba de trabajo. o Detalle de una transacción con prueba de trabajo. Los protagonistas: Alice, Bob y Eve. o Emisión de activos digitales como recompensa a comportamientos honestos. o Emisión de activos digitales como recompensa a

comportamientos honestos. Más sobre el nonce. • **Identificación de posibles conflictos y conocimientos de su resolución.** o Desdoblamientos de la cadena: descripción del fenómeno y protocolo de actuación previo. o Doble gasto: definición del problema y maduración de la recompensa. o Doble gasto: definición del problema y maduración de la recompensa. Otros intentos de doble gasto. o Sostenibilidad: rentabilidad de la «minería» y ataque del 51%. o Sostenibilidad: rentabilidad de la «minería» y ataque del 51%. Rentabilidad de la minería. o Sostenibilidad: rentabilidad de la «minería» y ataque del 51%. El halving. o Sostenibilidad: rentabilidad de la «minería» y ataque del 51%. ¿El final de la minería? o Sostenibilidad: rentabilidad de la «minería» y ataque del 51%. El ataque del 51%. • **Aplicación del protocolo de prueba de trabajo en cadenas públicas.** o Uso de app para móviles sobre cadena de bloques de prueba.