UNIVERSIDAD DE GRANADA

FACULTAD DE CIENCIAS

Propuesta TFG. Curso 2025/2026

GRADO: Grado en Matemáticas

CÓDIGO DEL TFG: 270-009-2025/2026

1. DATOS BÁSICOS DEL TFG:

Título: Bases matemáticas de la cadena de bloques.

Descripción general (resumen y metodología):

En 2008 se presentó bajo el seudónimo Satoshi Nakamoto un manuscrito conteniendo la descripción de la criptomoneda Bitcoin. Esta divisa funciona como un algoritmo de consenso implementado mediante varias herramientas criptográficas entre las que destacamos las funciones hash que garantizan la integridad de la información y sirven para estrablecer la prueba de trabajo, y el algoritmo de firma ECDSA utilizado para garantizar la identidad y autenticidad de la información tratada. Una cadena de bloques puede modelarse mediante un grafo acíclico, por lo que el estudio y conocimiento de dicho tipo de grafos debe ayudar a entender y mejorar el funcionamiento de una cadena de bloques.
En este Trabajo de Fin de Grado se pretende estudiar los fundamentos matemáticos detrás de la construcción de una cadena de bloques. Entre los mismos destacamos las funciones hash, los algoritmos de firma digital y los grafos acíclicos.

Tipología: Estudio de casos, teóricos o prácticos, relacionados con la temática del Grado.

Objetivos planteados:

1. Funciones hash: resistencia a colisiones y técnicas de construcción.
2. Firma digital: algoritmos clásicos.
3. Estudio de los árboles de Merkle.
4. Descripción del concepto de prueba de trabajo y su uso.

Bibliografía básica:

- Satoshi Nakamoto. "Bitcoin: A Peer-to-Peer Electronic Cash System" (PDF). bitcoin.org.
- Hans Delfs, Helmut Knebl. Introduction to Cryptograp Springer Berlin, Heide 2015. https://doi.org/10.1007/978-3-662-47974-2
- Nigel P. Smart, Cryptography Made Simple, Springer Cham, 2016. https://doi.org/10.1007/978-3-319-21936-3

Recomendaciones y orientaciones para el estudiante:

Plazas: 1

2. DATOS DEL TUTOR/A:

Nombre y apellidos: FRANCISCO JAVIER LOBILLO BORRERO

Ámbito de conocimiento/Departamento: ÁLGEBRA

Correo electrónico: jlobillo@ugr.es

3. COTUTOR/A DE LA UGR (en su caso):

Nombre y apellidos:

Ámbito de conocimiento/Departamento:

Correo electrónico:

4. COTUTOR/A EXTERNO/A (en su caso):

Nombre y apellidos:

Correo electrónico:

Nombre de la empresa o institución:

Dirección postal:

Puesto del tutor en la empresa o institución:

Centro de convenio Externo:

5. DATOS DEL ESTUDIANTE:

Nombre y apellidos: JOSE MARIA CASTRO PASTILLA

Correo electrónico: josemariacp19@correo.ugr.es