Introducción a la Tecnología Blockchain y Smart Contracts

2024-2025

Presentación 10 de abril de 2024

Jesús Correas – jcorreas@ucm.es (despacho 412)

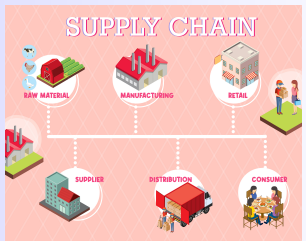
Departamento de Sistemas Informáticos y Computación
Universidad Complutense de Madrid

La tecnología blockchain

- La tecnología blockchain surgió como una forma de representar una moneda digital.
  - Sin existencia física.
  - Resistente a la falsificación y al fraude.
  - Fuertemente basada en técnicas de criptografía y en sistemas distribuidos.
- Idea básica: un **registro descentralizado** de transacciones.
  - El **estado** del sistema se guarda en una **cadena de bloques.**
  - **La infraestructura informática garantiza por construcción el funcionamiento correcto del sistema.**
  - Procesamiento de transacciones en múltiples nodos (*mineros*).
  - Eliminación de un nodo central.
  - Utilización de **algoritmos de consenso** para evitar fraudes.

La tecnología blockchain: mucho más que criptomonedas

- Pero es una tecnología mucho más general: es una forma de garantizar **transacciones confiables** entre organizaciones que no confían entre sí.
- No está necesariamente relacionada con aplicaciones financieras: *Enterprise blockchains.*
- **Ejemplos:**
  - Cadena de suministros:
    - alimentación, vehículos, etc.
    - `https://www.ibm.com/products/supply-chain-intelligence-suite/food-trust`
  - Trazabilidad:
    - Diamantes de sangre, minerales críticos, reciclado de baterías.
    - `https://everledger.io`
  - Identidad digital, gobernanza:
    - `https://www.dock.io`
    - `https://aragon.org`




Images by Freepik, Everledger, Freepik

Blockchain 2.0: Smart Contracts

- La tecnología blockchain ha evolucionado y algunas plataformas incluyen una **máquina virtual.**

> *Smart Contracts*
>
> Son programas que se ejecutan en la MV del blockchain.
>
> Permiten implementar un **contrato** (financiero o de otro tipo) de forma que el propio sistema garantiza su cumplimiento.

- La plataforma más relevante es **Ethereum.**
- Los smart contracts proporcionan una potencia mucho mayor a los sistemas de blockchain.
- Durante el curso estudiaremos cómo se programan contratos en el lenguaje **Solidity** y se ejecutan en la **máquina virtual.**
- La **seguridad de las aplicaciones** es fundamental:
  - Evitar vulnerabilidades.
  - Conocer buenas prácticas de programación.
  - Detalles de implementación de bajo nivel.

Programa de la asignatura

1. Introducción a los sistemas descentralizados.
2. Mecánica de un sistema de blockchain.
3. Smart contracts: un blockchain programable.
4. El lenguaje de programación Solidity.
5. Seguridad de contratos inteligentes. Análisis de vulnerabilidades.
6. Casos de uso y temas avanzados.

¿Qué se aprende?

- Conceptos básicos de la tecnología blockchain.
- Los conceptos de blockchain programable y smart contract.
- El funcionamiento de la plataforma **Ethereum.**
- Programación con el lenguaje **Solidity.**
- Conceptos avanzados de programación y de la *Ethereum Virtual Machine*.
- **Vulnerabilidades** de un blockchain programable y **buenas prácticas** de programación.

La asignatura se imparte en español, pero todos los materiales disponibles están en inglés. **Los estudiantes internacionales pueden recibir tutorías y ser evaluados en inglés.**

Información de la asignatura: Clases y Evaluación

- TBC está disponible en **todos los grados.**
- Asignatura de **segundo cuatrimestre: X, J: 12:00-14:00**
- **Convocatoria ordinaria (curso 2021-2022):**
  - **20 %:** Participación y realización de ejercicios en clase.
  - **60 %:** Proyecto de la asignatura.
  - **20 %:** Examen.

  No hay notas mínimas en ningún apartado.
- **Convocatoria extraordinaria (curso 2021-2022):**
  - **50 %:** Trabajos prácticos.
  - **50 %:** Examen.
- Ejercicios y proyecto de la asignatura en **grupos de dos alumnos.**
- Estas transparencias están en `http://costa.fdi.ucm.es/~jcorreas/TBCinfo.pdf`

Lee la ficha docente en la Web de la Facultad.

Bibliografía

- Esta tecnología cambia muy rápidamente. Durante el curso proporcionaremos la bibliografía más relevante que vayamos a utilizar.
- Algunas referencias:


W.-M. Lee, *Beginning Ethereum Smart Contract Programming*. Apress, 2019.


C. Dannen, *Introducing Ethereum and Solidity: Foundations of Cryptocurrency and Blockchain Programming for Beginners*. Apress, 2017.


M. Mukhopadhyay, *Ethereum Smart Contract Development*. Packt publishing, 2018.


A. Antonopoulos and G. Wood, *Mastering Ethereum: Building Smart Contracts and DApps*. O'Reilly Media, Inc., 2018. [Online]. Available: https://github.com/ethereumbook/ethereumbook


A. M. Antonopoulos, *Mastering Bitcoin: Programming the Open Blockchain*, 2nd ed. O'Reilly Media, Inc., 2017. [Online]. Available: https://github.com/bitcoinbook/bitcoinbook

Enlaces de interés

- Introducciones breves a la tecnología blockchain:
  https://www.geeksforgeeks.org/blockchain-technology-introduction

  https://solidity.readthedocs.io/en/v0.7.0/introduction-to-smart-contracts.html
- Etherscan Explorer and Analytics:
  https://etherscan.io/
- Ethereum White Paper:
  https://ethereum.org/en/whitepaper/
- Solidity language documentation:
  https://docs.soliditylang.org/en/develop/
- Ethereum developers documentation:
  https://ethereum.org/en/developers/docs/
- Remix – Solidity web-based IDE:
  https://remix.ethereum.org