

TALLER DE BLOCKCHAIN

TELECO RENTA

PLAN DE PROMOCIÓN DE LOS ESTUDIOS DE TELECOMUNICACIÓN

contacto de soporte: antoni.oller@upc.edu

Departament d'Enginyeria Telemàtica

EETAC - UPC - BAMPLA



Financiado por
la Unión Europea
NextGenerationEU



Plan de Recuperación,
Transformación y Resiliencia

Introducción a la Actividad

¡Bienvenido, Instructor!

Esta guía te ayudará a prepararte para este taller de TelecoRenta, donde los alumnos explorarán diversas tecnologías de Blockchain. Inicialmente, se situará a los estudiantes con conceptos básicos sobre blockchain y más adelante se realizará un par de ejercicios prácticos usando la plataforma de Ethereum. Asegúrate de seguir estos pasos para guiar adecuadamente a tus estudiantes.

Presentación:

La primera parte del taller consiste en una presentación de los conceptos básicos de blockchain, te hemos preparado una presentación PDF que puedes encontrar en el repositorio con el nombre:

[Presentacion_instructor.pdf]

Esta presentación te debe servir como soporte para presentar a los estudiantes la teoría necesaria para poder empezar con las dos actividades. Además de la presentación, en las siguientes páginas vas a encontrar definiciones más detalladas de cada concepto.

Conceptos y definiciones

Tecnología Blockchain

Blockchain es una tecnología revolucionaria que permite el mantenimiento de un registro público, distribuido y descentralizado. Nació como la infraestructura subyacente de Bitcoin, la primera criptomoneda, ideada por una persona o grupo bajo el pseudónimo de Satoshi Nakamoto en 2008. Su propósito original era solucionar el problema del doble gasto en monedas digitales sin necesidad de una autoridad central. Sin embargo, rápidamente se descubrió su potencial para otras aplicaciones, gracias a sus características de seguridad, transparencia y resistencia a la manipulación.

Blockchain es como un libro de registros digital: Imagina un libro donde se anotan todas las transacciones o intercambios de información. Cada página de este libro sería como un "bloque".

Cada bloque está conectado: Al igual que las páginas de un libro están encadenadas, cada bloque en blockchain está conectado al anterior y al siguiente, formando una "cadena de bloques".

Es muy seguro: Cada bloque está protegido con métodos especiales llamados criptografía, lo que hace que sea muy difícil alterar la información una vez escrita.

Uso en criptomonedas: Blockchain es conocido por ser la tecnología detrás de las criptomonedas como Bitcoin. Es como un registro público de todas las transacciones de Bitcoin.

Conceptos Principales

Bloques - Transacciones - Cadenas

Bloques: Un bloque es una unidad de almacenamiento que guarda un conjunto de transacciones validadas. Cada bloque tiene un identificador único, conocido como hash, y referencia el hash del bloque anterior, formando así una cadena.

Transacciones: Son las acciones realizadas por los usuarios, como transferencias de criptomonedas o datos. Cada transacción se verifica y se registra en un bloque.

Cadenas: La cadena de bloques, o blockchain, es la secuencia de bloques conectados. Esta estructura garantiza la integridad y la cronología de todas las transacciones realizadas.

Funciones de Hash - Criptografía - Seguridad

La seguridad en blockchain se logra mediante el uso de criptografía de clave pública, donde cada usuario tiene una clave privada única para acceder a sus activos y una clave pública que otros pueden usar para enviarle activos. Las funciones de hash criptográfico transforman los datos de los bloques en una cadena de caracteres alfanuméricos de longitud fija, lo que ayuda a proteger la integridad y la autenticidad de la información.

Contratos inteligentes

Un contrato inteligente es un acuerdo entre dos personas o entidades en forma de código informático programado para ejecutarse automáticamente. Los contratos inteligentes se ejecutan en blockchain, lo que implica que los términos se almacenan en una base de datos distribuida y no pueden modificarse. Las transacciones también son procesadas en blockchain, lo que automatiza pagos y contrapartidas.

Cómo funciona →

1. Un usuario inicia una transacción desde su monedero en la blockchain.
2. La transacción llega a la base de datos distribuida, donde se verifica la identidad del usuario.
3. Se aprueba la transacción, que puede consistir en una transferencia de fondos u otra acción específica.
4. La transacción incorpora un código que define la naturaleza de la acción a ejecutar.
5. Las transacciones se agregan como un bloque dentro de la cadena de bloques.
6. Cualquier modificación en el estado del contrato sigue el mismo proceso para actualizarse.

Aplicaciones de un Contrato Inteligente:

Los contratos inteligentes tienen una amplia gama de aplicaciones prácticas, incluyendo:

- Registros: Garantizar la integridad de los registros digitales.
- Comercio: Automatizar transacciones comerciales y pagos.
- Cadenas de Suministro: Rastrear la autenticidad y el origen de los productos.
- Hipotecas y Mercado Inmobiliario: Simplificar y asegurar las transacciones inmobiliarias.

- Recursos Humanos: Automatización de contratos de trabajo y pagos.
- Propiedad Intelectual: Gestionar derechos y licencias.
- Salud: Mantener registros médicos seguros y privados.
- Elecciones: Mejorar la seguridad y transparencia en los procesos electorales.
- Seguros: Agilizar y automatizar las reclamaciones y pagos.

Beneficios de un Contrato Inteligente:

Los contratos inteligentes ofrecen numerosas ventajas, como:

- Independencia: Minimiza la necesidad de intermediarios.
- Fiabilidad: Una vez desplegados, no pueden ser alterados.
- Seguridad: Protección contra fraudes y manipulaciones.
- Ahorro: Reducción de costos operativos y de transacción.
- Precisión: Eliminación de errores humanos en la ejecución de los acuerdos.
- Sostenibilidad: Reducción de papeleo y procesos burocráticos.

¿Para Qué se Usa Blockchain? Aplicaciones en la Vida Real

Criptomonedas como Bitcoin y Ethereum:

- Lo más conocido: Bitcoin, la primera criptomoneda, funciona gracias a blockchain.
- ¿Cómo se usa? La gente lo utiliza para enviar y recibir dinero digitalmente, sin la necesidad de bancos.
- Ethereum: Otra criptomoneda que permite algo más que solo transacciones: ejecutar contratos inteligentes.

Contratos Inteligentes:

- ¿Qué hacen? Automatizan acuerdos y transacciones. Por ejemplo, pueden usarse para ejecutar automáticamente un pago cuando se cumplen ciertas condiciones.
- Aplicaciones: Desde automatizar pagos en seguros hasta gestionar derechos de autor de música y libros.

Cadenas de Suministro y Logística:

- Seguimiento de productos: Blockchain puede usarse para rastrear el origen y el viaje de un producto, desde su fabricación hasta su entrega. Esto es útil para verificar la autenticidad de los productos y asegurar que se han transportado correctamente.

Votaciones y Elecciones:

- Más seguridad y transparencia: Blockchain podría ser usado para crear sistemas de votación digitales más seguros y transparentes, donde es más difícil manipular los resultados.

Identidad Digital:

- Manejo de identidades digitales: Blockchain puede proporcionar una manera segura de almacenar y gestionar identidades digitales, reduciendo el fraude y protegiendo la privacidad.

Registro de Propiedad y Bienes Raíces:

- Transacciones inmobiliarias: Simplifica y hace más seguras las transacciones inmobiliarias, registrando la propiedad de manera transparente y permanente.

Salud:

- Registros médicos seguros: Los registros médicos pueden ser almacenados de forma segura y accesible, permitiendo a los pacientes controlar quién tiene acceso a su información.

ACTIVIDAD 1. Hash

En la primera actividad, los alumnos van a entender el concepto de las funciones de Hash, cuál es su papel en una red blockchain y ver a través de dos simulaciones este concepto. Más concretamente, se van a utilizar dos páginas web que trasladan de manera muy clara conceptos importantes de las redes blockchain.

[<https://blockchaindemo.io/>]

[<https://simewu.com/blockchain-simulator/>]

Material necesario:

- Ordenadores con acceso a internet y con un navegador web.

ACTIVIDAD 2. Hello World Smart Contract

En esta actividad, los alumnos tendrán la oportunidad de sumergirse en el mundo del desarrollo de contratos inteligentes. Crearán su primer contrato inteligente, un simple "Hello World", utilizando la red Ethereum. Esta actividad tiene como objetivo introducir los conceptos básicos del desarrollo de contratos inteligentes y familiarizar a los estudiantes con herramientas de desarrollo en blockchain.

Material necesario:

- Ordenadores con Acceso a Internet: Para acceder a las plataformas de desarrollo y documentación online.
- IDE de Ethereum: Una plataforma de desarrollo web para escribir, desplegar y administrar contratos inteligentes en Ethereum. No se requiere instalación.
- Navegador Web Actualizado: Preferentemente Chrome o Firefox para compatibilidad con Remix.
- Documentación de Ethereum: Disponible en <https://ethereum.org/es> para referencia y guía.

Ethereum y su Relación con los Contratos Inteligentes

Ethereum: Es una plataforma blockchain avanzada que va más allá de la simple transferencia de criptomonedas. Su característica distintiva es la capacidad de ejecutar contratos inteligentes, que son programas que se autoejecutan cuando se cumplen ciertas condiciones, todo esto en un entorno descentralizado y seguro.

Contratos Inteligentes: Son acuerdos digitales codificados que se ejecutan automáticamente en la red de Ethereum. Estos contratos pueden realizar una variedad de tareas, desde la transferencia de fondos hasta la automatización de procesos complejos, sin necesidad de intermediarios.

Introducción a Alchemy como Herramienta de Desarrollo

Alchemy: Es una plataforma que facilita a los desarrolladores la conexión con la red Ethereum. Permite a los usuarios interactuar con la blockchain sin la necesidad de configurar y mantener sus propios nodos, simplificando así el proceso de desarrollo de aplicaciones basadas en blockchain.



Por Qué Usar Alchemy: Alchemy proporciona una interfaz accesible y herramientas de monitoreo que son fundamentales para entender y administrar aplicaciones en la red Ethereum, lo que lo hace una herramienta ideal para principiantes y desarrolladores experimentados.

Instalaciones necesarias

Instalación de MetaMask:

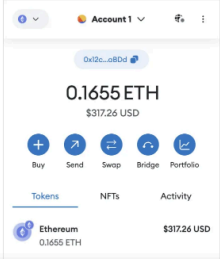
Accede a la página <https://metamask.io/download/> y descarga MetaMask para chrome en todos los ordenadores de los alumnos.

Discover MetaMask Portfolio today. Track and manage your web3 assets in one place! →

 **METAMASK** Features ▾ Build ▾ Resources ▾ Learn 






Chrome iOS Android



Install MetaMask for your browser




Install MetaMask for Chrome

Supported Browsers

 Chrome  Firefox  Brave  Edge  Opera

 **MetaMask** 

 metamask.io 3,1 ★ (3,5 k puntuacions)

Extensió Flux treball/plaificació 16.000.000 usuaris




Instalación de nodejs:

Accede a la página <https://nodejs.org/en/download/> y descarga la versión correspondiente al ordenador:

Downloads

Latest LTS Version: 20.11.0 (includes npm 10.2.4)

Download the Node.js source code or a pre-built installer for your platform, and start developing today.

LTS Recommended For Most Users	Current Latest Features	
 Windows Installer node-v20.11.0-x64.msi	 macOS Installer node-v20.11.0.pkg	 Source Code node-v20.11.0.tar.gz

Seguidamente sigue los pasos del instalador.




Instalación de VSCode:

Es necesario que los alumnos también dispongan de VSCode, instala la versión correspondiente de esta página:

<https://code.visualstudio.com/download>

Download Visual Studio Code

Free and built on open source. Integrated Git, debugging and extensions.

		
Windows Windows 10, 11	.deb Debian, Ubuntu	.rpm Red Hat, Fedora, SUSE
Mac macOS 10.15+		
User Installer System Installer .zip CLI	.deb .rpm .tar.gz Snap CLI	.zip CLI
x64 Arm64	x64 Arm32 Arm64	Intel chip Apple silicon Universal