

Lab 1 – Explorando las *mainnet* de Bitcoin y Ethereum

La información almacenada en los sistemas de blockchain Bitcoin y Ethereum es pública y accesible para cualquiera que se conecte a sus redes. Existen múltiples sitios web en Internet que permiten explorar los bloques y las transacciones de criptomonedas públicas en tiempo real. En esta sesión veremos dos. El resultado de esta sesión debe ser un documento en formato pdf con las respuestas a los ejercicios que se incluyen en los siguientes apartados. En algunos casos es necesario que incluyáis capturas de pantalla, pero es importante resaltar la información relevante y las explicaciones que se solicitan. No olvidéis escribir vuestros nombres al principio del documento.

1. Bitcoin

Vamos a utilizar el explorador disponible en <https://www.blockchain.com>. Este explorador permite ver datos, estadísticas y algunas características de diversas criptomonedas, especialmente sobre Bitcoin.

Accede a la página <https://www.blockchain.com/explorer> para realizar los siguientes ejercicios.

1.1. Bloques

Los bloques son generados por los mineros y contienen el procesamiento de un conjunto de transacciones. Se identifican mediante un número consecutivo que se denomina **block height** (es el número de bloques que hay en la cadena desde el inicio de los tiempos, desde el primer bloque llamado *genesis block*).

Ejercicio 1. Busca el bloque de Bitcoin con el número 7754XX, donde XX es tu número de grupo. Puedes buscar un bloque de Bitcoin utilizando el campo de texto que aparece en la parte superior de la página y seleccionando la blockchain “BTC Block” de la lista que aparece al pulsar Intro.

Anota los siguientes datos (o una captura de pantalla resaltándolos) en la memoria del ejercicio:

- *Block Height*,
- *Timestamp*,
- *Difficulty*,

- *Number of confirmations,*
- *Number of transactions.*

Explica brevemente cómo se calcula la retribución total del minero y calcula cuánto ha ganado el minero minando este bloque.

1.2. *Difficulty*

Los bloques se minan con una **dificultad** que se va ajustando periódicamente cada cierto número de bloques. Consulta en las transparencias del tema 2 el significado de este concepto y la frecuencia con la que se ajusta en Bitcoin.

Ejercicio 2. *Encuentra un bloque anterior a este con una dificultad distinta. Incluye en el resultado del ejercicio el número de bloque encontrado y su dificultad (o una captura de pantalla que incluya esta información, resaltándola), y explica por qué es necesario modificar la dificultad periódicamente.*

1.3. *Retribución del minero*

El trabajo de cálculo de los mineros se retribuye con las comisiones de las transacciones incluidas en el bloque que se está minando, más una cantidad adicional (creada de la nada). Esta cantidad se denomina “block reward” y actualmente es de 6,25 Bitcoin por cada bloque.

Ejercicio 3. *Explora las transacciones incluidas en el bloque 7754XX y encuentra la transacción que corresponde a la retribución al minero. Incluye en el resultado una captura de pantalla resaltando esta transacción.*

La retribución de bloque de 6,25 Bitcoin cambia con el tiempo. Consulta en las transparencias cómo va cambiando y con qué frecuencia.

Ejercicio 4. *Encuentra un bloque anterior con una retribución que sea el cuádruple que la retribución actual. Incluye en el resultado del ejercicio una captura de la pantalla con la información del bloque resaltando el número de bloque encontrado y la fecha de minado de ese bloque.*

1.4. *Confirmaciones*

Una característica fundamental de los sistemas de criptomonedas similares a Bitcoin es que no existe una garantía absoluta de que una transacción haya sido incluida en la cadena de bloques de forma “definitiva”. Afortunadamente, la probabilidad de que el mecanismo de consenso (“la subcadena más larga”) descarte ese bloque decrece de forma exponencial con el número de bloques añadido con posterioridad. El **número de confirmaciones** de una transacción (o bloque) es el número de bloques que aparecen en la cadena después del bloque que contiene esa transacción. En Bitcoin, es habitual exigir que una transacción tenga **6 confirmaciones** para considerar que es definitiva, aunque si el importe de la transacción es muy alto, pueden ser necesarias más confirmaciones.

Ejercicio 5. *Accede de nuevo al explorador de <https://www.blockchain.com/explorer> para que se muestren los últimos bloques minados hoy en tiempo real. Busca el bloque más reciente que tenga al menos 6 confirmaciones. Anota en el resultado de este ejercicio el número de ese bloque, y el tiempo que ha pasado para que se hayan producido las 6 confirmaciones.*

2. Ethereum


El explorador de www.blockchain.com que acabamos de ver permite explorar múltiples redes de blockchain, incluida Ethereum. Sin embargo, para explorar la información de la red principal de Ethereum utilizaremos un explorador específico: <https://etherscan.io>. La ventaja de este explorador es que permite visualizar información exclusiva de un blockchain programable como Ethereum: *smart contracts*, consumo de *gas*, *tokens*, *NFT*, etc.

2.1. Transacciones por segundo

Un indicador relevante de un sistema de blockchain es el número de transacciones procesadas por segundo. Esta es bastante baja actualmente si se compara con redes mundiales como Paypal o Visa (con alrededor de 2000 transacciones por segundo) y constituye una de las críticas que se hacen a los sistemas de blockchain actuales. Esta velocidad se debe fundamentalmente al sistema de proof-of-work. La propuesta de la próxima versión de Ethereum (proof-of-stake, sharding) promete una velocidad teórica de 100.000 transacciones por segundo.¹

Ejercicio 6. *En la página principal de <https://etherscan.io> puedes ver el número medio de transacciones por segundo (TPS) de los últimos bloques minados en Ethereum. Incluye en el resultado de este ejercicio este valor.*

2.2. Cuentas de contratos

En Ethereum existe el concepto de *cuenta* con un saldo asociado. Las cuentas pueden ser EOA (*externally owned accounts*) o estar controladas por un contrato. Todas las cuentas están identificadas por una dirección (*address*). Cuando se consultan las transacciones en Etherscan, es fácil identificar las cuentas de contrato porque tienen el símbolo . Además en Etherscan se pueden buscar los contratos a partir de su address.

Ejercicio 7. *Busca en <https://etherscan.io> el contrato con address `0xdAC17F958D2ee523a2206206994597C13D831ec7`.*

Este contrato corresponde a Tether², una criptomoneda implementada sobre Ethereum mediante un contrato que sigue el estándar de tokens ERC20 que veremos más adelante. En Etherscan se puede consultar información muy detallada sobre este contrato. Por ejemplo, se pueden consultar las transacciones realizadas a este contrato (pestaña Transactions), e

¹<https://ethereum.org/en/upgrades/shard-chains/>

²<https://tether.to/en/>

incluso el código fuente en el lenguaje Solidity del contrato que implementa esta criptomoneda (pulsando en la pestaña Contract).

Incluye como resultado de este ejercicio la captura de pantalla de Etherscan en la que aparece la información básica de este contrato y resaltando el número de transacciones que se han realizado a este contrato (pestaña Transactions).

2.3. Estimación del precio del *gas*

Cuando se realiza una transacción en Ethereum se debe indicar un precio del gas que se utilizará para retribuir al minero. Como las comisiones en Bitcoin, un precio de gas demasiado bajo puede hacer que la transacción tarde mucho en realizarse. existen herramientas para estimar el precio de gas necesario para que la transacción sea procesada en un tiempo razonable.

Ejercicio 8. *Utiliza la opción de menú More / Gas Tracker de <https://etherscan.io> para ver el precio del gas utilizado en las últimas transacciones recibidas en la red. Incluye en el resultado de este ejercicio una captura de esta página donde aparece el precio medio del gas.*

Considerando el precio medio del gas, calcula cuánto costaría el gas de una transferencia simple que gasta 21000 unidades de gas. Proporciona el importe total de gas tanto en ether como en dólares al cambio que aparece en la esquina superior izquierda de la página.