educación IT
CODE YOUR FUTURE

Criptografía y Blockchain

Módulo 4

educación IT
CODE YOUR FUTURE

Bitcoin

Introducción

Un poco de historia

El 31/10/2008 se publica el célebre **artículo de Satoshi Nakamoto sobre Bitcoin.**

En enero de 2009, Nakamoto distribuye la **primera versión del *software* para crear un nodo de bitcoins** en código abierto (Génesis). Contenía 50 BTC que fueron asignados al propio Nakamoto como dueño del primer nodo Bitcoin.

En este primer bloque de bitcoins emitido venía encriptado el titular de una portada del diario The Times en la que se informaba de un nuevo rescate bancario en el Reino Unido.

THE TIMES

Saturday January 3 2009 timesonline.co.uk No 69523 £1.50

Eat Out from £5

More than 900 great restaurants, including four **Gordon Ramsay** favourites from £15

Start collecting tokens today Pullout inside

Israel prepares to send tanks and troops into Gaza

Israel allowed foreigners to flee the Gaza Strip as it prepared for a ground offensive. At least 420 Palestinians were killed in a week of airstrikes News, page 3

Michael Sheen Frost, Nixon and me

Magazine

Working mums So that's how she does it

Body&Soul

Detox in style The best spas on the planet

Travel

Salmon Rushdie I Won't Marry Again

Pages 21, 22

Giant Killing? Guide to the FA Cup Third Round

Sport

Chancellor on brink of second bailout for banks

Billions may be needed as lending squeeze tightens

99p

Hal Finney fue la primera persona en descargar el *software* **Bitcoin Core** creado por Nakamoto surgiendo de este modo el segundo nodo de Bitcoin.

Nakamoto envió 10 BTC de los 50 primeros a Finney, realizándose la **primera transferencia de moneda digital de forma totalmente segura y descentralizada de la historia**.

Luego, se fueron añadiendo más personas a la red, que descargaban el *software* y aparecían así nuevos nodos.

En mayo de 2010 **el bitcoin cotizó por primera vez en una bolsa de intercambio digital pública**.

El 22 de mayo de 2010 se realizó la primera compra en la cual se aceptaron **BTC como moneda de pago**: es el *Bitcoin Pizza day* (Laszlo Hanyecs compró 2 pizzas por U$S 25).

> No se sabe quién es Nakamoto. Tras la emisión del bloque Génesis se siguieron emitiendo más BTC de acuerdo con la política monetaria del Bitcoin, que dado que él es uno de los nodos originales, fueron a parar en su totalidad a su monedero, y que nunca después ha transferido ni gastado. Desde abril de 2011 desapareció casi por completo del mapa.

Bitcoin

Puede definirse como un **libro de contabilidad público y distribuido**, que almacena los registros de todas las transacciones de la red en forma ordenada e inmutable.

Las **transacciones** son seleccionadas por los mineros y añadidas a los bloques para ser minados. Cada bloque se identifica por su *hash* y está unido a la cadena mediante el *hash* del bloque previo, presente en su encabezado.

Minado

El minado es el proceso mediante el cual se **agregan nuevos bloques a la *blockchain*.**

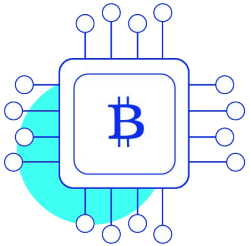
Los mineros se encargan de varias tareas, a saber:

- Mantienen copias de toda la *blockchain.*
- Validan las transacciones.
- Validan los bloques.
- Crean los bloques nuevos.
- Realizan la PoW.
- Distribuyen las recompensas.

Bitcoin como solución

El surgimiento de Bitcoin ha **resuelto varios problemas históricos** relacionados al dinero electrónico y los sistemas distribuidos, a saber:

- El problema de los Generales bizantinos.
- Los ataques Sybil.
- El problema del doble gasto.

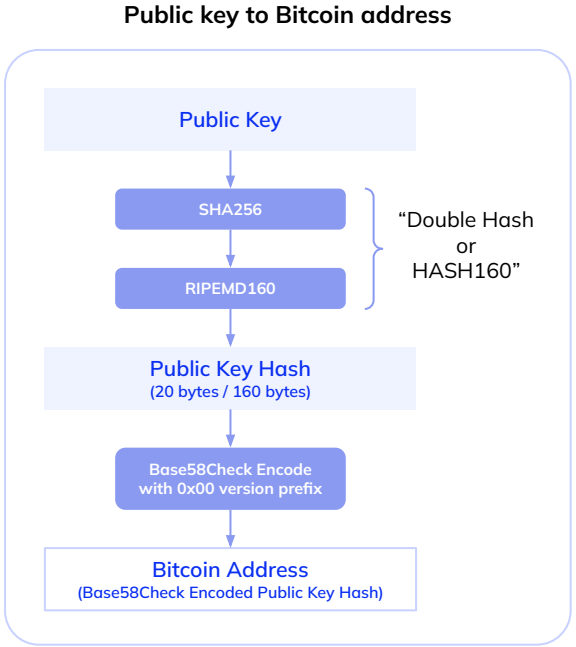


- Un **ataque Sybil** consiste en atacar un sistema distribuido creando un gran número de identidades que aparenten ser independientes y usarlas para obtener una influencia desproporcionada, alterar rutas o modificar contenido almacenado de forma redundante. De esta forma ciertos nodos legítimos pueden sufrir una usurpación de identidad al estar solo conectados a los del atacante.
- El **problema del doble gasto** consiste en un usuario que envía el mismo dinero electrónico a dos usuarios diferentes al mismo tiempo y se verifican independientemente como transacciones válidas.

Direcciones en Bitcoin

Las **direcciones en Bitcoin** suelen ser codificadas en **códigos QR** para su fácil distribución.

Los ***wallets*** (monederos) almacenan una clave privada. Pueden implementarse mediante *software* o por *hardware*. Los monederos físicos cuentan con un chip seguro que hace que no podamos usarlos sin autenticarnos con nuestra clave privada. Si se rompen o los perdemos, es posible restaurarlos y recuperar el acceso a las criptomonedas con una combinación de palabras o semilla de recuperación que se incluye con ellos cuando los compramos.



Algoritmo de consenso en Bitcoin

Todos los nodos poseen el libro de contabilidad en el que se registran irreversiblemente todas las transacciones que se realizan.

Cada vez que se lleva a cabo **una nueva transacción se agrega a un bloque** (no se verifica cada transacción, sino los bloques en los que son agregadas). Cada diez minutos es emitido un bloque nuevo con las transacciones que se hayan realizado en ese espacio de tiempo.

En el momento en que es emitido un bloque, cada **nodo compite por descifrar la información** que contiene y agregarla al libro de contabilidad (minado).

En cuanto uno de los nodos resuelve el problema, **la información es registrada, agregada a la cadena de bloques y todos los demás nodos la replican, y queda fijada en el libro de contabilidad de forma inmutable,** sin que sea posible modificarla.

Política monetaria en Bitcoin

Durante el minado, lo que **los mineros de Bitcoin hacen es computar una función de *hash*** en la única dirección que pueden hasta que uno de ellos **encuentre cuál era la entrada correcta y ese mismo es el que valida el bloque y recibe como premio los nuevos bitcoins** que se están emitiendo.

En el famoso artículo de Nakamoto en 2008 también se explica una política de emisión de bitcoins, que en absoluto es arbitraria, sino que sigue, no las directrices de un banco central, sino un algoritmo perfectamente establecido.

El número de bitcoins que se emitirán en total es un número finito y prefijado (21 millones). Se comenzó emitiendo 50 BTC cada diez minutos (cada vez que se añade un bloque nuevo con transacciones a la *blockchain* de Bitcoin).

Cada cuatro años la cifra se divide por dos: desde 2009 se emitían 50 BTC cada diez minutos, en el cuatrienio siguiente 25 BTC, en el 2018, se emitieron 12,5 BTC cada diez minutos, y así sucesivamente. En 2024 la recompensa será 3,125 BTC.

Árbol de Merkle

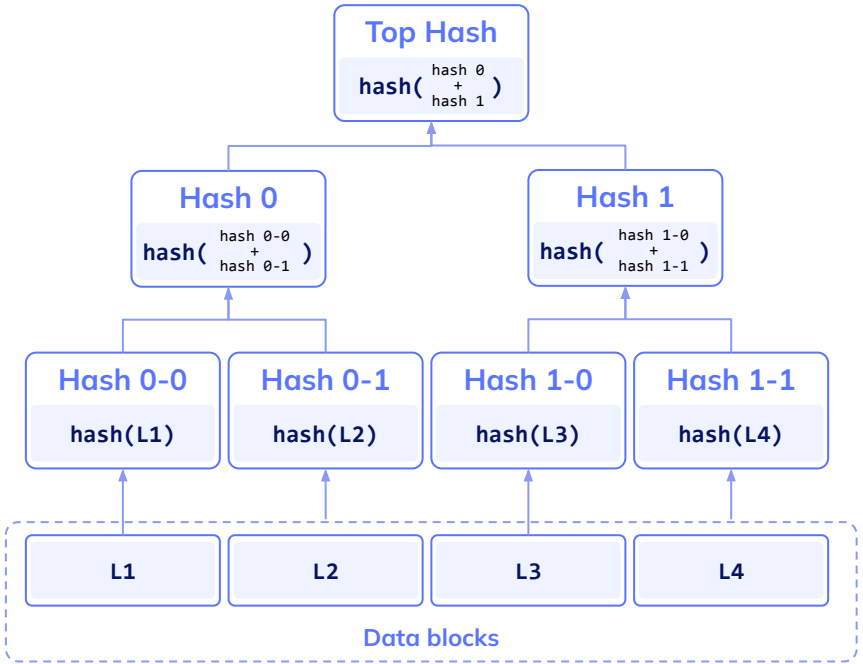
La raíz del árbol de Merkle **resume todos los datos de los bloques**, y por eso:

- Mantiene la **integridad de los datos.**
- Permite una prueba rápida y sencilla para saber si un bloque de datos está incluido realmente dentro del árbol.
- No es necesario descargar todo el conjunto de datos para verificar la integridad de la información.

Ejemplo

Los hashes 0-0 y 0-1 son los valores de los hash de los bloques de datos 1 y 2 respectivamente, y 0 es el hash de la concatenación de hashes 0-0 y 0-1.

Árbol de Merkle



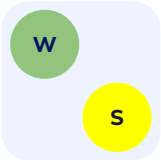
Tipos de nodos

Reference Client (Bitcoin Core)

Contiene un *wallet*, un minero, una base de datos Blockchain completa y un nodo de enrutamiento de red con la red bitcoin P2P.

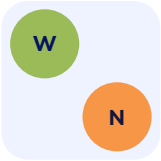
Full Blockchain Node

Tiene una base de datos Blockchain completa y un nodo de enrutamiento de red con la red bitcoin P2P.



Lightweight (SPV) Stratum wallet

Contiene un *wallet* y un nodo de red en el protocolo Stratum, sin *blockchain.*

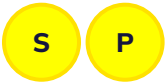


Lightweight (SPV) wallet

Contiene un *wallet* y un nodo de red en el protocolo bitcoin P2P, sin *blockchain.*

Solo Miner

Contiene una función de minería con una copia completa de la cadena de bloques y un nodo de enrutamiento de red bitcoin P2P.



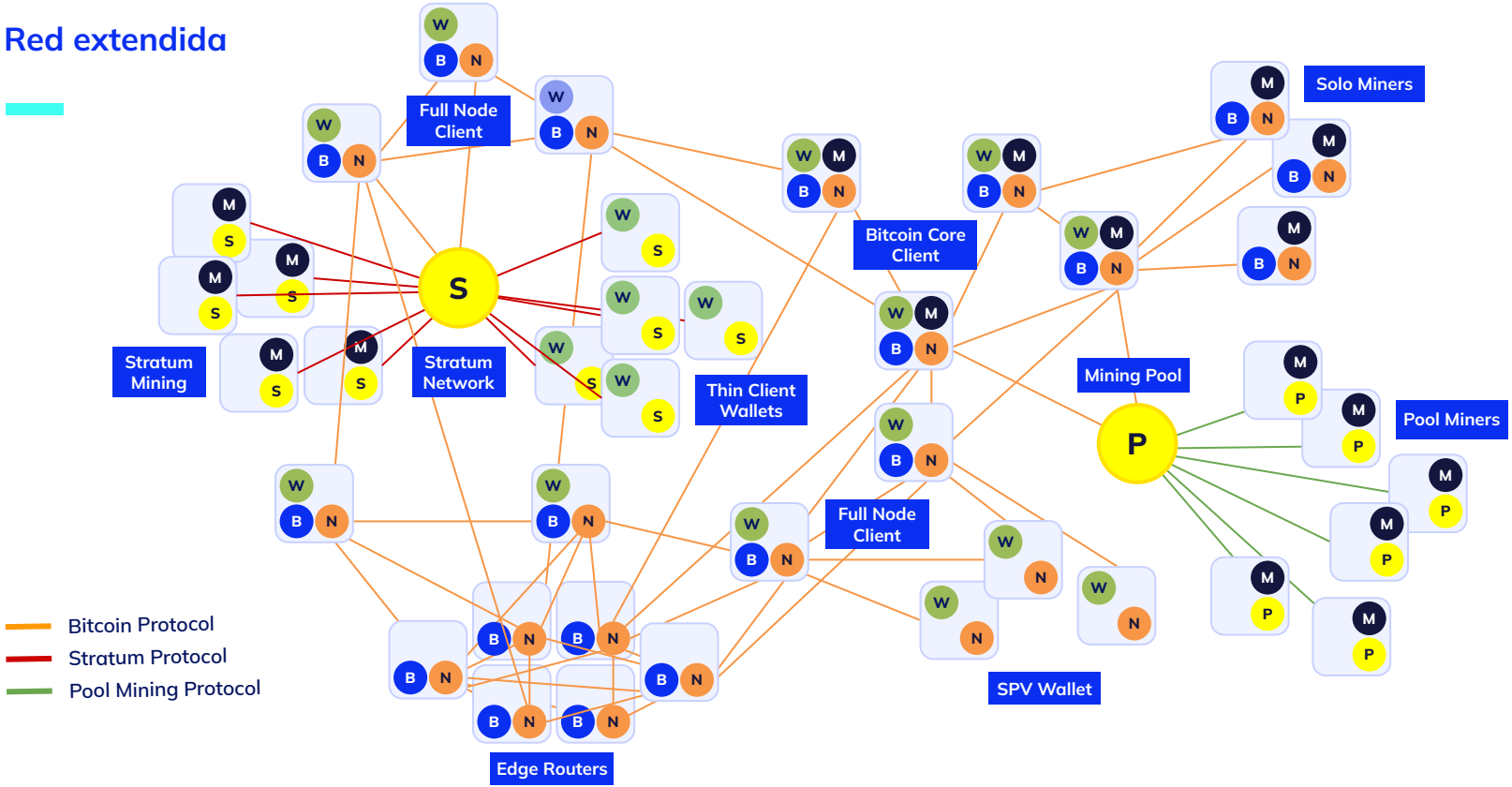
Pool Protocol Servers

Routers de puerta de enlace que conectan la red bitcoin P2P a nodos que ejecutan otros protocolos, como nodos de minería de *pool* o nodos Stratum.

Mining Nodes

Contienen una función de minado, sin *blockchain,* con los nodos de protocolo Stratum (S) u otro protocolo de minería de *pool* (P).

Red extendida



¡Sigamos trabajando!