Universidad de Alcalá
Escuela Politécnica Superior

Grado Ingeniería Informática

Trabajo Fin de Grado

Bitcoin y algoritmos. Variaciones y caso de uso Ravencoin.

Autor: Rubén Velasco Pérez

Tutor: José María Gutiérrez Martínez

2022

Resumen

Resumen en Español
En este proyecto, se verá y se analizará claramente todo el ecosistema Bitcoin. Veremos por qué surge, cómo surge, qué propósitos tiene, cómo funciona y sus principales vulnerabilidades. Además de sus implicaciones en la sociedad y en el mundo real.

Entenderemos, que Bitcoin, no trajo un sistema de pagos, trajo una nueva tecnología. Una tecnología capaz de crear ecosistemas descentralizados, construidos por los usuarios para los usuarios: La tecnología Blockchain.

Estudiaremos de cerca esta tecnología Blockchain, viendo cómo funciona y sobre qué principios se fundamenta. Conociendo así, qué es la Proof of Work (y sus derivados) y qué son los algoritmos hash de minado criptográfico que la soportan.
Con esto último, examinaremos varios ejemplos de algoritmos hash de minado criptográfico y comprenderemos por qué no dejan de aparecer nuevos. Y todo ello, tomando como caso de uso la red Ravencoin. Una Blockchain que presenta algunas características novedosas muy interesantes.

Resumen en Inglés
In this proyect, the Bitcoin ecosystem will get deeply seen and analyzed. We will see why and how it was created, what are its purpouses, how it works and its main vulnerabilities. Furthermore, we will see its implications in society and in the real world.

We will understand that Bitcoin did not bring just a payment system, it broguht a new technology. A technology capable of creating decentralized ecosystems, built by users for users: Blockchain techonology.

We will study this technology closely, analyzing how it works and on what principles it is based. Therefore, we will learn what the Proof of work (and its derivatives) is and what the cryptographic mining hash algorithms that support it are.
On the latter, we will see some examples of crypto mining hash algorithms and we will understand why new ones keep appearing. All of them, taking the Ravencoin as a use case. It is a Blockchain that presents some very interesting new features.

Palabras clave
Bitcoin, Criptomonedas, Blockchain, Algoritmo de consenso descentralizado, Algoritmo hash de minado criptográfico, ASICs

Tabla de Contenidos

Tabla de Ilustraciones

CAPITULO 1

Introducción

En este primer capítulo veremos por qué nace este proyecto de TFG (Trabajo de Final de Grado). Ya que todo proyecto en la vida tiene una finalidad en concreto. Y este, no es una excepción.

Veremos el enfoque que tomará con respecto al tema de investigación, los objetivos que persigue, y que salida como resultado se espera conseguir con la realización del mismo.

1. Contexto, planteamiento y objetivos del proyecto

Hoy en día no se deja de hablar del gran fenómeno de las criptomonedas y de los NFTs, y con ellos, de la tecnología que los sustenta: la Blockchain.
No dejan de aparecer en los periódicos, en las noticias, en los artículos, en los libros o en cualquier foro, página o red social de Internet.
Y no solo eso, parece que todo el mundo tiene conocimientos extensos sobre el tema. Da la sensación de que todo el mundo usa o ha usado alguna vez criptomonedas y NFTs. Que saben como utilizarlos, manipularlos y crearlos. Da igual con la persona que hables, da igual si tiene un perfil técnico, un perfil económico, un perfil más jurídico o ni siquiera ninguno de ellos, parece que sabe a la perfección todos los detalles que afectan a estos nuevos productos desde cualquiera de los ámbitos posibles.
Y es que, esta nueva tecnología, tan disruptiva, pero tan inmadura, se ha incrustado rápidamente en la sociedad, llegando a normalizarse incluso. Ahora, cualquier persona que no sepa o no utilice estos nuevos conceptos parece que está desconectado y anticuado. Pero…¿Cuánto se sabe realmente de todo este nuevo mundo?

Yo personalmente, autor de este TFG, no tengo ningún tipo de conocimiento al respecto. Lo poco que pueda saber, no es mayor que el conocimiento que pueda tener cualquier usuario al uso sobre cualquier producto.
Y esta, es la motivación principal del desarrollo de este trabajo. Considero primordial no dejarse llevar por la gran avalancha de desinformación sobre estos nuevos productos y con ellos de esta nueva tecnología tan innovadora. Considero que hay que pararse un segundo a sentar las bases y comprender todo el ecosistema, para después poder meterse de lleno y adecuadamente en él. Sabiendo así con qué trabajar y por qué, qué construir y qué beneficios económicos y sociales puede aportar. En definitiva, considero que primero es esencial conocer a la tecnología para después poder domarla.

Y eso es justo lo que se va a llevar a cabo con este proyecto. Se va a analizar de forma extensa el mayor campo de aplicación posible de este gran ecosistema. Obviamente todo ello desde un punto de vista técnico, en el que se vea claramente la arquitectura y estructura que hace posible todo esto. Entendiendo por qué se hacen las cosas que se hacen, por qué suceden las cosas que suceden y obviamente, comprendiendo y entendiendo por qué es necesaria toda la lógica que hay detrás ello.

Así pues, este proyecto será y tiene el objetivo de ser un resumen a modo de bitácora de todo lo descubierto y analizado en este proceso anteriormente descrito.
Para que así, cualquier persona que se adentre a leerlo, pueda navegar por toda la información recopilada, y que es totalmente necesaria, para que cuando acabe, tenga los conocimientos mínimos necesarios para entender de forma correcta esta nueva tecnología tan potente y todos aquellos proyectos que se están construyendo sobre ella. Y por tanto tenga una puerta de entrada a este nuevo mundo y pueda empezar a opinar con fundamento y critica.

Exactamente de la misma manera que espero acabar yo. Pretendo adquirir unos conocimientos bastante extensos sobre el tema de investigación dado, que me permitan complementar y completar mis aptitudes desarrolladas a lo largo de los cursos académicos. Haciendo que pueda conocer en esta nueva tecnología, que no he podido contemplar en la carrera como ingeniero informático, y que considero muy necesario por el gran potencial y revolución que presentan.

CAPITULO 2

Sistema Bitcoin

En este segundo capítulo haremos un análisis profundo y extenso sobre el sistema Bitcoin. Veremos cómo funciona cada uno de sus engranajes y por qué. Desde sus principios más básicos hasta los más avanzados.

Incluso, entraremos a discernir sobre las vulnerabilidades a las que está expuesto y como poder evitarlas poniéndonos en la piel de un usuario.

Para finalizar, cuando sepamos a la perfección como trabaja Bitcoin, entraremos a analizar si está preparado para funcionar como sistema de pago. Y las implicaciones que tiene en el mundo real.

1. Introducción

Nacimiento
En 2008, un misterioso usuario de Japón que se hacía llamar “Satoshi Nakamoto” compartió su proyecto con la comunidad de “The Cryptography Mailing List”. “The Cryptography Mailing List”, es una de las listas de correo más importantes sobre criptografía, en la que sus usuarios comparten ideas y dudas sobre el tema.

Satoshi, quería crear dinero digital, en el que no fuera necesario la existencia de un tercero de confianza, como por ejemplo los bancos o el gobierno. Para ello, publicó un artículo académico con el nombre de “Bitcoin P2P e-cash paper”. En el que se explicaba en detalle como funcionaba su sistema. Y meses más tarde, proporcionó el software necesario para implantarlo.

A diferencias de lo que muchos piensan, Satoshi, no inventó el dinero digital. Porque sí, aunque este proyecto trajo consigo varias de las innovaciones tecnológicas y sociales más importantes de nuestra era, el dinero digital ya existía. Y todos, aún a día de hoy seguimos utilizándolo.

Las cuentas bancarias, de las que prácticamente todo el mundo es propietario, son simplemente una anotación electrónica del dinero que hemos ido depositando a lo largo del tiempo en nuestra entidad bancaria. Tenemos tarjetas de crédito o débito, asociadas a estas cuentas y las usamos para hacer compras de todo tipo… y todo esto, sin que se mueva ni un solo billete o moneda.

En este sistema, sin entrar mucho en detalle, vemos, que la entidad bancaria tiene el control sobre absolutamente todas las transacciones que se realicen. Junto con la posesión del dinero, que se encargará de distribuirlo por nosotros cada vez que realicemos un movimiento.

Y esto es de lo que la moneda de Satoshi quiere desvincularse. No quería depender de ninguna entidad bancaria o gubernamental, y el control que ello supone, ya no solo sobre nosotros, sino sobre el propio dinero. Tampoco quería una trazabilidad de todos los movimientos. Quería anonimato… como pasa con el dinero físico. Todos los billetes y monedas son impersonales, si dispones de ellos, puedes comprar, sino no. Y cuando compras, nadie te pregunta tu nombre… a nadie le importa quien eres y que quieres… simplemente quieren el dinero.

Vista general del sistema de transacciones digitales tradicional (Banco)
Para explicarlo, usaremos un ejemplo sencillo, en el que Ana entra en la tienda de Juan y quiere comprarle una pantalla.

Ana dispone de una tarjeta de crédito asociada a su única cuenta bancaria en la que almacena todo su dinero. Y Juan, de un dispositivo de cobro, como por ejemplo un datafono, que estará asociado, al igual que Ana, a su única cuenta bancaria.

Entonces, Ana, pasa su tarjeta bancaria por el terminal de pago, para transferirle a Juan el capital correspondiente al valor de la pantalla.

En ese momento, como si de un recorrido de tren se tratara, van teniendo lugar de uno en uno diferente procesos para completar el pago. En los que se requerirá la intervención de varias partes, entre las cuales, estarán presente las entidades bancarias de cada uno de los implicados.

El terminal de pago enviará la información de la transacción tanto al banco del comprador (Ana) como al del vendedor (Juan). Una vez que llegue la información a la entidad bancaria de Ana, esta accederá a la información de la cuenta, con el objetivo de comprobar que dispone de dicho cantidad y que es quien dice ser.
Si la respuesta es afirmativa, se autorizará la tramitación del pago. Se enviarán los resultados de vuelta al terminal, para que Juan complete la venta. Y el banco de Ana enviará los fondos a la cuenta de Juan, cuyo banco ya fue advertido de dicha transacción.

En ese momento, Ana se puede marchar con la pantalla y Juan recibe el costo de la venta en su banco. Aunque, a modo de curiosidad, no puede acceder de forma inmediata a dichos fondos, ya que quedan retenidos de forma temporal en su cuenta.

Vista general del sistema de transacciones digitales de Satoshi (Bitcoin)
De igual manera que hemos hecho con el sistema tradicional, para explicar el sistema de Satoshi, usaremos un ejemplo sencillo, en el que María quiere comprarle a Roberto una gorra.

Pero antes de eso, aclararemos un par de términos relevantes para hablar con propiedad. Que en el ejemplo anterior, no ha hecho falta, por la familiaridad que tenemos con la jerga bancaria.

La moneda del sistema de Satoshi se llama Bitcoin, en contraposición al Euro o al Dólar. Las cuentas en las que almacenamos estos Bitcoins, se llaman Wallets. Y serían similares a las cuentas bancarias. Y la entidad bancaria, quedaría sustituida por el propio sistema, que recibe el nombre de Blockchain. Por lo que no interviene ningún agente externo, entidad u organización.

Ahora sí: María, dispone de una Wallet con una cierta cantidad de Bitcoins y quiere hacerle a Roberto un pago equivalente al valor de la gorra. Para ello, María accede a su Wallet, a la que solo ella tiene acceso, y por tanto se sobreentiende que es ella, y autoriza el traspaso monetario a Roberto. Esa transacción viajara al sistema Blockchain, que comprobará que se dispone de ese saldo. Y en caso de ser afirmativo, se enviarán los fondos a Roberto.

En este momento, María puede marcharse con su nueva gorra y Roberto tiene de forma inmediata sus Bitcoins.

Resumen de los sistemas de transacciones digitales
Para asimilar mejor estos dos sistemas y las diferencias entre ellos, no hay nada mejor que una imagen resumen de la vida de las transacciones. Así, podremos ver todas las partes involucradas y las diferencias sustanciales entre los dos sistemas… además, de entender porqué Satoshi creó este sistema y la finalidad que buscaba:

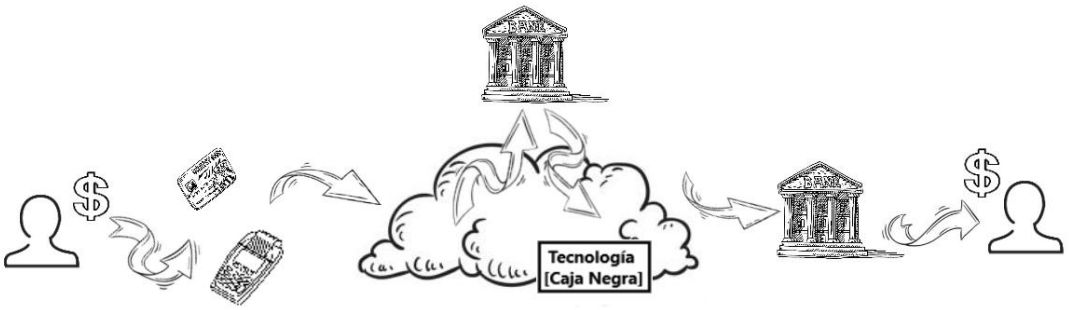

Ilustración 1: Transacción bancaria tradicional
Fuente: Elaboración Propia (elementos gráficos extraídos de Internet)

Ilustración 2: Transacción Bitcoin
Fuente: Elaboración Propia (elementos gráficos extraídos de Internet)

2. Sistema Bitcoin

Bien, ya que tenemos claro que es Bitcoin y los objetivos que persigue. Vamos a explicar en detalle como trabaja su sistema. Para ello, describiremos el recorrido por el que pasa una transacción, con el objetivo de ver que partes existen y como funcionan.

Transacción y Wallet
Si Esther quiere pagar a Fernando, deberá indicárselo al sistema. Para ello, enviará desde su Wallet, en la cual tiene almacenados todos sus Bitcoins, un mensaje como el siguiente: «Yo, Esther, transfiero a Fernando 10 Bitcoins».

Aunque, como podemos deducir, ese no puede ser el mensaje definitivo que se remita al sistema… ya que sabemos que las transacciones son anónimas y resulta completamente imposible hacer una trazabilidad hasta la persona.

Para tal fin, la Wallet, utiliza criptografía asimétrica. En el que asociamos nuestro saldo de Bitcoins a una clave pública, que funciona como número de cuenta. Y junto con la clave privada asociada, podemos enviar mensajes como el siguiente: «Yo, clave pública 008646BBFB7D, transfiero a clave pública 3FD8C0A9C6FF 10 Bitcoins. Firmado con la clave privada de la clave pública 008646BBFB7D».

Ahora sí, Esther y Fernando quedan totalmente en las sombras, ya que lo único que se comparte es la clave pública… que no está asociada su persona física. Como nota, mencionar, que al no ser necesario garantizar la identidad de la persona que está detrás de la generación de claves, no es necesario disponer de una entidad certificadora. Y se pueden generar tantos pares de claves (cuentas) como se desee.

Vemos también, que de forma indirecta, se ha inyectado una fuerte capa de seguridad en el sistema. Ya que al estar el mensaje cifrado con la clave privada de Esther, que solo ella conoce, al realizar el descifrado (con su clave pública) sabremos que ese mensaje es de ella, y nada más que de ella. Evitando los fraudes por corrupción de mensajes y suplantación de identidad (en este caso cuenta).

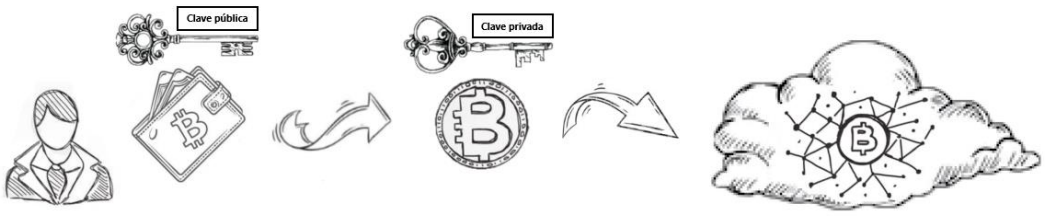

Ilustración 3: Resumen de una transacción en Bitcoin
Fuente: Elaboración Propia (elementos gráficos extraídos de Internet)

Sistema de validación de transacciones (parte 1 de 3)
Volviendo al ciclo de vida de la transacción. Tenemos que Esther a enviado el siguiente mensaje: «Yo, clave pública 008646BBFB7D, transfiero a clave pública 3FD8C0A9C6FF 10 Bitcoins. Firmado con la clave privada de la clave pública 008646BBFB7D».

Ahora, para que se haga efectiva la transferencia, deben existir como mínimo esos 10 Bitcoins en la Wallet de Esther. Por lo que el sistema, se encargará de acceder a su cuenta y comprobar que dispone de un saldo mayor o al menos igual al de la transacción.

Esto, como vemos y como hemos mencionado, elimina al tercero de confianza… pero de forma indirecta, el sistema, se convierte en el tercero de confianza. En el que tenemos que creer ciegamente de igual manera.

Es por esto, que Satoshi propone una solución alternativa, en el que aunque se mantenga el tercero de confianza, este sea descentralizado. O dicho de otro modo, son los usuarios del propio sistema los que rechazan o aprueban de forma colectiva las transacciones.

Esto, deja, como no es de otra forma, que todas las cuentas de los usuarios sean publicas y de libre acceso.

Registro de transacciones
El acceso a la información de la cuenta de un usuario, y con ello la forma de validar transacciones, también adquiere un enfoque alternativo.

Existe un único registro de transacciones. En el que quedan apuntadas todas y cada una de las transferencias que han tenido lugar en el sistema, con independencia de que usuario las hayas realizado. Básicamente, el registro, es una lista ordenada de mensajes como el que quiere enviar Esther a Fernando. En el que habrá que realizar una trazabilidad entre los datos para calcular el saldo de cada una de las cuentas.

El registro, al igual que el sistema de validación de transacciones, es descentralizado. No hay ningún servidor central u organización que lo controle. Son los propios usuarios los que lo mantienen en funcionamiento.

Concretamente, sigue un modelo de sistema peer-to-peer (P2P). En el que el contenido integro del registro queda distribuido globalmente. Y cada uno de los usuarios, mantiene una copia en el dispositivo desde el que ha accedido al sistema.

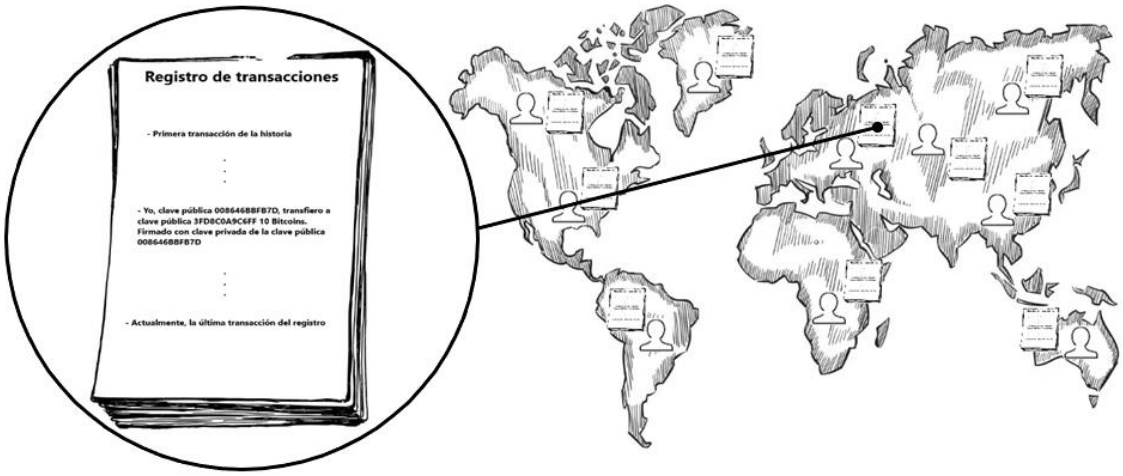

Ilustración 4: Resumen del funcionamiento del Registro Blockchain
Fuente: Elaboración Propia (elementos gráficos extraídos de Internet)

Una anotación importante, es que, la existencia del registro depende de si existen usuarios o no en la red. Por lo que, si todas las copias se corrompen o desaparecen de los dispositivos… Bitcoin dejaría de existir. Aunque la idea de estar distribuido en multitud de dispositivos a nivel mundial, es que esto no pase.

Formato del registro de transacciones

Desde un punto de vista más técnico, el registro de transacciones, es una secuencia de datos encadenados. Cada transacción que se añada al sistema, formará un nuevo eslabón y hará referencia a la transferencia anterior, formando así, esta estructura de cadena.

Esto no es nuevo, pero ya hemos especificado un poco mejor el sistema de ordenación que usa el registro. Con el que mantiene una correcta cronología de las transacciones.

Aunque esto no es del todo cierto. Con el objetivo de tener un registro manejable, que facilite el uso y explotación del sistema, los datos que lo conforman serán fraccionados en bloques. Estos, serán, los nuevos eslabones, y entre ellos, mediante una referencia al bloque anterior, formarán la nueva cadena del sistema. Por eso, este registro de transacciones se conoce como Blockchain… o cadena de bloques.

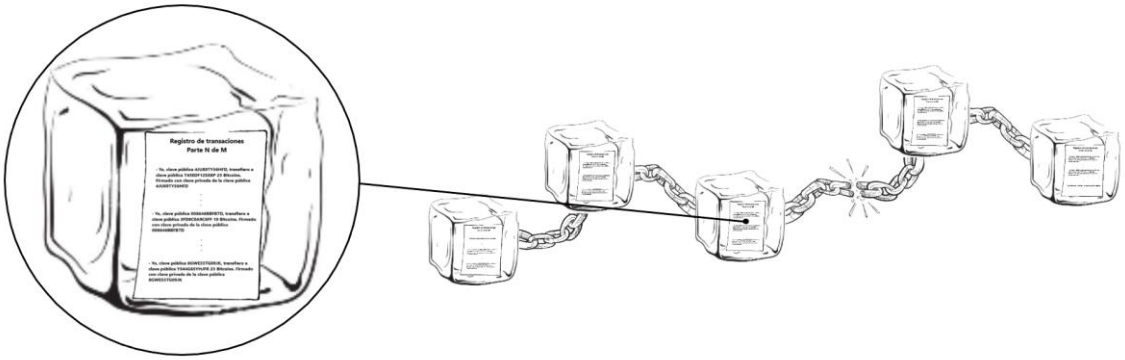

Ilustración 5: Resumen del formato del Registro Blockchain
Fuente: Elaboración Propia (elementos gráficos extraídos de Internet)

Contenido de un bloque de datos (parte 1 de 2)
Concretamente, cada bloque de datos tiene un tamaño máximo y aproximado de 1MB. Y almacena todas las transacciones en cola que quepan, que suelen ser unas 2.000 - 2.300.

Pero… ¿Cómo se mantienen las referencias entre bloques? Esto, en cierto punto, es simple. Veámoslo como si de una base de datos relacional se tratara:

Cada bloque tiene un identificador único asociado (o clave primaria), que lo identifica de manera inequívoca entre todos los demás. Y almacena, junto con sus respectivas transacciones, el identificador del bloque anterior (a modo de clave foránea)… lo que da como resultado, que sea posible esta estructura de bloques encadenados.

Como nota, aunque es de fácil deducción, el orden de los eslabones se consigue debido a que cada nuevo bloque que se añada al sistema, junto con sus transacciones, encapsula el identificador del último bloque vigente del registro… que es su respectivo bloque anterior. Y una vez dentro, este será el actual último bloque a la espera de nuevas entradas de datos.

El identificador de bloque, en principio, puede ser cualquier cosa. Podríamos implementar cualquier sistema generador de identificadores únicos, y en teoría, Bitcoin seguiría funcionando. Pero Satoshi se decantó por un sistema Hash, en el que el identificador de cada uno de los bloques de datos de la Blockchain es el Hash del propio contenido del bloque (Hash del bloque anterior y transacciones).

Pero… ¿Podemos asegurar que el Hash de los bloques de datos es único?

La respuesta es sí. El Hash se forma con el contenido del bloque, y, aunque un bloque tenga exactamente las mismas transacciones que otro, cosa que para empezar, se antoja bastante imposible, ya que, tendría que darse que las mismas personas, realicen las mismas transacciones, tanto al mismo destinatario como en la misma cantidad, en el mismo orden temporal, y sin que nadie se meta de por medio; jamás tendrán el mismo Hash como referencia al bloque anterior. Ya que cada uno de los Hashes, son en principio únicos. Y por tanto, nunca se va a generar un identificador de bloque igual a otro.

Pero esto, realmente no nos soluciona nada, simplemente nos dice, que para que los Hashes sean únicos, se tienen que construir sobre Hashes únicos. Pero ahí está en cierta medida la respuesta.

Pongamos por caso, que los Hashes no son únicos como norma universal. Y por tanto, que se pueda dar, que dos bloques, que tengan las mismas transacciones, tengan también el mismo identificador del bloque anterior. Y en consecuencia generen el mismo Hash.

Esto podría darse, si los bloques anteriores de los bloques del ejemplo, cumplen también la misma condición. Es decir, que tengan las mismas transacciones y la misma referencia al bloque anterior, para poder generar el Hash necesario.

Aunque de nuevo, se necesitaría, que estos bloques, tengan como bloques anteriores a dos bloques iguales. Y estos, últimos, igual. Y así sucesivamente.

Esta sucesión de referencias gemelas, no puede ser infinita, debe acabar en algún momento. Y precisamente eso es lo que sucede cuando una de estas llega al bloque inicial de la cadena. Que sin avanzar mucho al respecto, podemos adelantar, que es un bloque especial, totalmente diferente al resto de los bloques existentes en la cadena.

En ese momento, la sucesión de referencias que haya llegado al bloque inicial, tendrá como resultado inevitable un bloque anterior diferente. Lo que hará, que no coincida con su gemelo y se rompa la condición necesaria para que puedan llegar a existir dos Hashes iguales en todo el registro Blockchain.

Y sí, solo una sucesión de referencia podrá llegar al bloque inicial. La otra se quedará como mucho, a un bloque de diferencia. Ya que la Blockchain es una secuencia ordenada de bloques, uno detrás de otro. Y por tanto, para que dos bloques lleguen a la vez al bloque inicial, debe tratarse del mismo bloque.

Si vemos este ejemplo a la inversa, nos daremos cuenta, que el Hash del bloque inicial, influye en el resultado del Hash del siguiente bloque. Este, en el Hash de su siguiente. Y así hasta el último de ellos. Por lo que podríamos decir, que el Hash de un bloque, no solo es una referencia a dicho bloque, sino una referencia a todo el histórico de la Blockchain. Y por tanto, no se unen dos bloques entre si, sino el bloque con la cadena.

Por esto, usar un sistema Hash, aparte de solucionar el asunto de los identificadores de bloque, soluciona de forma indirecta, aunque seguramente buscada, la robustez y seguridad del registro. Ya que, como hemos visto, no tenemos una serie de transacciones encadenadas, sino, una cadena de transacciones… un ente único…una cadena. Siendo totalmente imposible modificar transacciones o bloques de la Blockchain. Ya que modificar alguna parte de la cadena, significaría, modificar toda la cadena.

En otras palabras, nos encontramos con que el cambio del contenido de un bloque, da como resultado una modificación de su Hash. Esto, a un conflicto directo con sus siguientes bloques, que pierden la referencia Hash que tienen almacenada. Y esto, a la necesidad de una resolución del conflicto, que acabará con el bloque invalidado y fuera de la cadena.

Y todo eso sin salir de nuestra copia de la Blockchain. Ya que si lo hiciéramos, el Hash del bloque también entraría en conflicto con el Hash del bloque válido que trata de sustituir, y el resto de usuarios, nos lo anularían.

Es por esto, que se dice, que la Blockchain es inmutable y completamente segura.

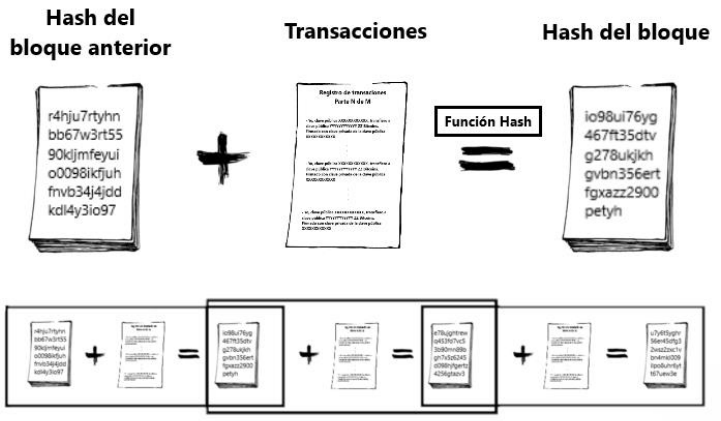

Ilustración 6: Resumen de un bloque de datos de Bitcoin
Fuente: Elaboración Propia (elementos gráficos extraídos de Internet)

Hash

Cabe destacar que, la función Hash que usa Bitcoin para operar es el algoritmo Hash SHA-256.

El SHA-256 es una variante del protocolo SHA, que vio la luz en 1993 de la mano de la Agencia de Seguridad Nacional de los Estados Unidos (NSA) y del National Institute of Standards and Technology (NIST). Cuyas siglas, SHA, significan Secure Hash Algorithm o es español Algoritmo de Hash Seguro. Y que usaban para asegurar documentos o datos informáticos frente a cualquier agente externo que desease modificarlos.

Realmente el SHA-256 es una versión del SHA-2, y este último, es la variante del SHA.

El SHA-2 tiene cuatro variantes según el número de bits: el SHA-224, el SHA-256, el SHA-384 y el SHA-512.

Así pues, la función SHA-256 genera cadenas de 64 caracteres alfanuméricos como Hashes, siguiendo una codificación de 256 bits (32 Bytes).

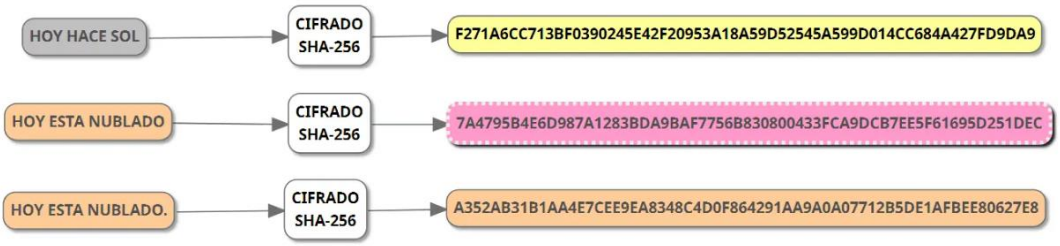

Ilustración 7: Ejemplo práctico del Algoritmo Hash SHA-256
Fuente: https://academy.bit2me.com/sha256-algoritmo-bitcoin/

Para finalizar mencionar que, el algoritmo SHA-256 es muy útil, ya que además de estar considerado actualmente como uno de los más seguros, el coste computacional que tiene asociado es muy eficiente para la alta resistencia de colisión que tiene.

Bloque Génesis

Habíamos terminado el punto anterior, haciendo mención al primer bloque de la cadena. Y es que efectivamente, como si de una cadena física se tratase, la Blockchain, tiene un eslabón inicial, al que se le han ido incrustando de forma ordenada, y de uno en uno, el resto de eslabones que la componen.

Un eslabón, completamente idéntico al resto, que simplemente fue designado como el inicio para poder construir la cadena, pero que tiene la misma forma y funcionalidad que todos los demás. Es decir, el de un bloque de datos que sirve para almacenar las transacciones del sistema.

Pero… si dijimos que el bloque inicial de la cadena, era completamente diferente al resto. ¿Cómo es posible que tenga sentido esto que estamos diciendo?

Y es que, el bloque inicial al que nos estamos refiriendo es el segundo bloque de la cadena Bitcoin. El primero, jamás podrá ser igual que el resto. Ya que como sabemos, un bloque, guarda una serie de transacciones y una referencia al bloque anterior. Y este, como mínimo, no contendrá el Hash del bloque anterior, ya que no existe ningún bloque predecesor al que pueda referenciar. Por lo que debe ser de forma obligatoria un bloque especial, con alguna modificación que otra, para que esto pueda llegar a ocurrir.

A este bloque se le conoce como Bloque Génesis y fue creado el 3 de enero de 2009, aparentemente por Satoshi Nakamoto.

En el momento de la creación no había Bitcoins en circulación… y con ellos, transacciones que anotar en el registro, por lo que este primer bloque está completamente vacío. Lo único que contiene, y a modo de curiosidad, es el titular del periódico The Times del 3 de enero de 2009, el día de su creación, cuyo titulo es: “El Canciller (británico) está considerando un segundo programa de rescate a la banca”.

Su única función es el de ser los cimientos de la cadena que se va a crear. Aportando al primer bloque no oficial de la cadena una referencia Hash para que pueda construirse.

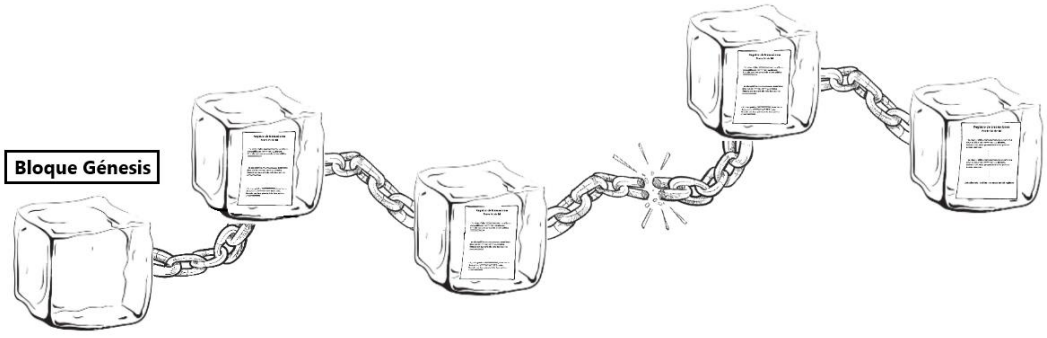

Ilustración 8: Resumen del bloque Génesis de Bitcoin
Fuente: Elaboración Propia (elementos gráficos extraídos de Internet)

Sistema de validación de transacciones (parte 2 de 3)
Si recapitulamos un poco, recordaremos, que el mensaje enviado por Esther a Fernando: «Yo, clave pública 008646BBFB7D, transfiero a clave pública 3FD8C0A9C6FF 10 Bitcoins. Firmado con la clave privada de la clave pública 008646BBFB7D» llegaba al sistema Bitcoin. Y entre todos los usuarios de la red, se encargaban de validar la transacción, comprobando, mediante el registro, que existía efectivamente el saldo necesario. Y luego, una vez validada, la almacenaban para siempre en la Blockchain.

Bien, pues ahora que conocemos como funciona el sistema Bitcoin por dentro, vamos a especificar un poco mejor el proceso.

Existen dos tipos de usuarios en la red Bitcoin. Los Usuarios y los Mineros.

Los primeros, los Usuarios, son, como su propio nombre indica, los usuarios de Bitcoin. Son los que mueven los Bitcoins. Son los que usan la moneda de Satoshi para comprar, pagar deudas, invertir o cualquier otra practica que se pueda llegar a hacer con una moneda. En definitiva, son los que crean las transacciones que luego entran al sistema. Y los segundos, los Mineros, son los usuarios que se encargan de validar esas transacciones. Son los que se encargan de velar porque solo entren transacciones reales al sistema y que ningún Usuario introduzca alguna transacción corrupta para beneficio propio.

Ya nos es conocido que es lo que tienen que hacer para validar y añadir cada transacción. Pero… ¿Yo como Minero, cómo sé que transacción es la que debo, o al menos puedo, validar?

Bien, esto es sencillo, como si de una subasta se tratase, cada Minero, se encargará de validar por su cuenta cada transacción, y el primero que lo logre, será el que avise al resto de Mineros, para que comprueben que efectivamente es válida. Y una vez tenga luz verde por parte de la mayoría de Mineros, se encargará de incorporarla al registro Blockchain. Es decir, es una competición de todos los Mineros contra todos los Mineros por ver quien es el que puede validar una transacción.

Pero tenemos que tener en cuenta una cosa, y es que, no se validan y se añaden las transacciones de forma individual al registro, sino que se añaden mediante bloques. Como ya sabemos. Siendo así, una competición de Mineros contra Mineros, por ver quien es capaz de validar un bloque de transacciones.

Sistema de validación de transacciones (parte 3 de 3)
Entonces, a modo de resumen general, tenemos que:

Todas las transacciones de los Usuarios, como la que desea realizar Esther, llegan al sistema de forma cronológica. Y se publican para todos los participantes por igual, es decir, para los Mineros.

Estos, mediante el acceso al registro Blockchain, se encargan de validar todas y cada una de las transacciones. Para comprobar que sean coherentes tanto con las transacciones pasadas del registro, como con el resto de transacciones del bloque. Es decir, miran que los emisores tengan los fondos necesarios para realizar la transferencia

y no los hayan gastado, así como que la propia transferencia, sea compatible. Y no se intente hacer un doble gasto, por ejemplo. Que no consiste en otra cosa, que en intentar gastar los mismos fondos en varios destinos de forma simultanea, con el objetivo de engañar al sistema y solapar varias transacciones en una (y con el gasto de una sola).

Y una vez que se tiene eso asegurado. Un bloque repleto de transacciones válidas. Se añade el Hash del último bloque de la cadena, a modo de Hash del bloque anterior, para enlazarlo con la cadena. Se realiza el Hash identificador del bloque. Y se envía al resto de mineros para que lo comprueben.

Si se recibe el visto bueno de la mayoría, y hemos sido los primeros en subirlo, el sistema podrá almacenarlo para siempre en el registro Blockchain. Sino, deberemos probar suerte con alguno de los siguientes bloques.

Sistema de recompensas

Realmente, los Mineros, ¿Por qué validan bloques de transacciones? Simple. Cada vez que se verifique un bloque, el sistema recompensará al Minero en cuestión con Bitcoins. Lo que incentiva, por su parte, a que exista una competición real entre Mineros.

Estos Bitcoins, que se otorgan como recompensa, serán Bitcoins frescos. Serán totalmente nuevos, como si acabásemos de imprimir o acuñar Euros o Dólares. Aunque, a diferencia de estas monedas, el Euro y el Dólar, Bitcoin, tiene un máximo de unidades que puede emitir. Fijado en los 21.000.000 de Bitcoins en circulación.

A modo de curiosidad, se estima que para el año 2140, se hayan emito los 21.000.000 de Bitcoins. Basándose en la cadencia actual de generación de nuevas monedas.

Volviendo a la recompensa en Bitcoins que recibe el Minero. Esta, está prefijada, aunque se reajusta de forma dinámica cada 210.000 bloques confirmados, mediante un evento en el sistema que recibe el nombre de Halving.

Las recompensas empezaron con un valor de 50 Bitcoins por bloque. Y en cada actualización, se reduce a la mitad. Lo que nos deja, a día de hoy, con unos 745.000 bloques validados, una recompensa de 6,25 Bitcoins por bloque.

Ahora, estos Bitcoins que recibe el Minero, ¿Cómo quedan registrados en el sistema? Ya que, si la recompensa no se queda materializada en el registro, los usuarios, jamás le dejarán gastarse la recompensa que ha conseguido.

Bien, existe una transacción especial, llamada Coinbase, que se almacena junto el resto de transacciones, y sirve para anotar la Wallet del minero y la recompensa que recibe por minar el bloque en ese momento. Esta transacción, ocupará el primer puesto de la lista de transacción del bloque. Y deberá ser validada, al igual que el resto de transacciones, por la mayoría de mineros de la red.

Proof-of-work

La forma en la que se validan los bloques de transacciones, como sabemos, es por votación. Si un bloque, cuenta con el apoyo de la mayoría de Mineros, se incorpora para siempre en la Blockchain. Por lo que si juntamos, que un atacante, puede intentar, una

y otra vez, crear un bloque corrupto para someterlo a votación. Y que es relativamente fácil inundar la red de identidades falsas, que nos hagan valido el bloque. Nos encontramos con que la Blockchain, deja de ser segura.

Es por esto, que el sistema Bitcoin, incorpora una pequeña modificación en el sistema de minado, para desincentivar estas prácticas. Y hacer, que para un atacante, salga más rentable minar un bloque y llevarse la recompensa, que intentar engañar a toda la red.

Esta modificación, consiste en incorporar una prueba de trabajo o Proof of Work en el proceso de minado.

El concepto de Proof of Work surge a finales de los 90. Cuando unos científicos informáticos crean un sistema para reducir el número de Spam en los correos electrónicos.

Este sistema, se instalaba en los servidores de correo electrónico. Y cuando un usuario enviaba un correo, el servidor, antes de recogerlo y reenviarlo al destinatario, solicitaba resolver un problema matemático. El resultado del problema matemático, no tenía ninguna utilidad en concreto, simplemente era para gastar el tiempo y los recursos de la máquina del usuario. Para que no pudiera enviar miles de correos al instante. Y que en el caso de que pudiese, ni se le pasara por la cabeza, debido al gran gasto de recursos que eso supondría.

Entonces, volviendo a Bitcoin, el Minero, como el usuario de correo electrónico, para poder subir y compartir con los demás un bloque de transacciones, debe resolver una pequeña traba computacional, que gaste sus recursos y su tiempo.

Esta traba, consiste en jugar con el Hash del bloque minado, que obliga a que empiece por una cantidad de ceros específicos.

Obviamente, esto obligará a modificar el contenido del bloque. Porque de no ser así, un bloque, con unas transacciones fijas y una referencia al bloque anterior fija, siempre generará el mismo Hash. Que seguramente, no cumplirá con la exigencia de ceros al comienzo del mismo.

Este nuevo campo del bloque recibe el nombre de Nonce. Y básicamente, es un campo para guardar datos aleatorios. Sin ninguna utilidad. Nada más que para modificar el contenido del bloque y conseguir un Hash que respete la norma de generación.

Así pues, el proceso de minado, consistirá en validar todas las transacciones, añadir la referencia al bloque anterior, completar de forma aleatoria el Nonce y ver si el Hash generado coincide con la regla de los ceros. Para poder subir el bloque a la red, someterlo a revisión y reclamar la recompensa.

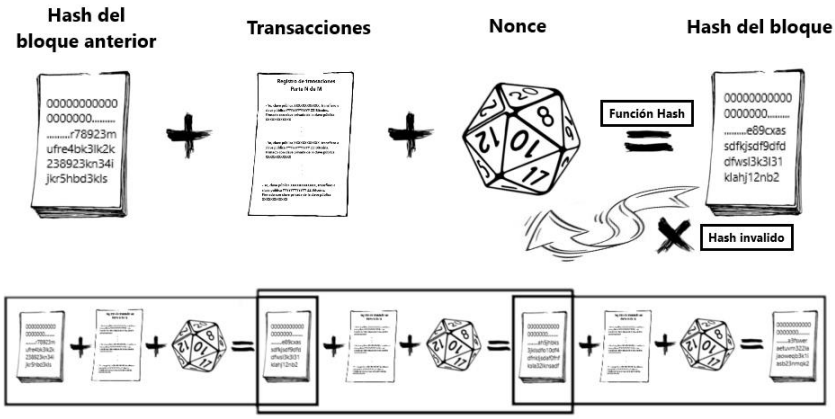

Ilustración 9: Resumen de la Proof of Work en Bitcoin
Fuente: Elaboración Propia (elementos gráficos extraídos de Internet)

La expresión de “aleatoriedad en el Nonce” no está descuidada. Y es que, el resultado de la Función Hash del bloque, no es predecible. Lo que implica realizar una resolución por fuerza bruta. Probando combinaciones de Nonce una y otra vez, hasta obtener un Hash de bloque valido.

Todo este trabajo computacional, se traduce a un gasto real de Hardware y electricidad. Y que como hemos mencionado, es un desincentivo para los atacantes. Ya que nadie en su sano juicio querrá realizar un gasto ingente de recursos para crear y subir un bloque corrupto, para que luego nos lo echen para atrás y nos quedemos con las manos vacías.

Aunque si que es cierto, que la posibilidad existe. Y está ahí para cualquier que quiera intentarlo.

Nivel de dificultad y los 10 minutos

Cuando se genera un nuevo bloque de datos y se sube a la red, no llega de forma inmediata a todos los usuarios. Tarda aproximadamente 1 minuto en hacerlo. O al menos, es lo que asumió Satoshi cuando desarrollo el sistema.

Esto significa, que después de que un Minero haya resuelto un bloque, durante 1 minuto, el resto de usuarios van a estar trabajando y gastando recursos para encontrar una solución que ya ha sido encontrada. Esto es un desperdicio de recursos. Y Satoshi, decidió, de forma arbitraria, que gastar más de un 10% de los recursos de la red en balde no se puede tolerar. Por eso, implantó una medida de tiempo de 10 minutos, como el tiempo necesario y obligatorio para resolver el Hash de un bloque de datos.

El problema está, en que la cantidad de Mineros en la red es dinámico, al igual que la potencia de calculo que estos aportan. Así que, el tiempo que se tarda en resolver la Proof of Work, y con ello en validar un bloque, es dinámico también.

La solución, para mantener un tiempo constante de resolución de 10 minutos, pasa entonces por hacer dinámica la Proof of Work. Aumentando su dificultad cuando más potencia de calculo haya repartida por toda la red. Y reduciéndola cuando menos haya. Para ello, lo único que hay que hacer, es variar el numero de ceros que se exige que tenga un Hash. Cuanto más ceros, más difícil será generar un Hash que cumpla la

condición. Y cuanto menos ceros, más fácil será. A esto se le conoce como Nivel de Dificultad. Y se revisa cada 2.016 bloques validados.

Ilustración 10: Nivel de Dificultad de la red Bitcoin
Fuente: https://www.blockchain.com/es/charts

La gráfica anterior, calculada directamente con el número de bloques que se confirman en la red Bitcoin, representa el Nivel de Dificultad del que estamos hablando. Si la analizamos, podemos observar, que se ha hecho más difícil la tarea de minar un bloque de transacciones con el tiempo. Esto es, porque conforme Bitcoin se ha hecho más famoso, más usuarios se han sumado al proceso de minado. Incrementando inevitablemente la potencia de calculo total de la red. Además de que la revolución tecnológica en la que nos encontramos, ha hecho, que independientemente de los usuarios que haya en la red, haya mayor potencia de cálculo por la mejora en los equipos de los usuarios.

Esto, en un principio podría parecer malo, ya que un nivel alto del Nivel de Dificultad, representa la necesidad de un mayor poder computacional para minar un mismo bloque. Y que cada usuario, gaste más recursos. Pero realmente es todo lo contrario. Representa que la red Bitcoin es más segura con el paso del tiempo. Que es lo que realmente Satoshi quiere. Y es que, como sabemos, a mayor gasto computacional, mayor desincentivo hay para cualquier atacante que pretenda subir bloques corruptos a la red.

A modo de curiosidad, podemos observar en la siguiente gráfica, la cantidad de Hashes, en TH/s (Tera Hashes por segundo), que de media son necesarios computar para generar un bloque valido.

Ilustración 11: Poder de Hashing en la red Bitcoin
Fuente: https://www.blockchain.com/es/charts

Se ha calculado a partir del número de bloques que han sido minados en las últimas 24 horas y la complejidad del bloque actual, cuyo valor se saca de la gráfica anterior.

Si nos fijamos bien, y la comparamos con la gráfica de la complejidad de la red, observamos que son bastante semejante. Y es que, realmente, son dos gráficas correlacionadas. A mayor Nivel de Dificultad, mayor cantidad de Hashes hay que generar para poder dar con el resultado correcto.

UTXOs

En cualquiera de las monedas de curso legal que existen, hay una serie de montos predefinidos. Que vienen a representar, por así decirlo, a la propia moneda. Y se usan para facilitar los intercambios.

Veamos esta idea con un poco más de detenimiento, usando una moneda en concreto, como por ejemplo, el Euro. Pero antes de eso, aclarar, que es un monto.
Un monto, es una agrupación de monedas, que representa un determinado valor dentro del sistema. Basado, obviamente, en la cantidad de monedas que reúna. Coloquialmente, se le conoce como billete o moneda, dependiendo de su valor.

Ahora sí, de vuelta al análisis extenso de la idea. El Euro, realmente, no existe. Existen una serie de billetes y monedas, que representan la idea abstracta del Euro. Por lo que, si yo como usuario del sistema, tengo unos fondos de 100 Euros, como tal, no tengo esos 100 euros, tengo un conjunto de montos, en billetes y monedas, que representan esos 100 Euros. Y por tanto, lo que recibo o gasto en las diferentes transacciones, son montos, no monedas.

Es por eso, que se dice que, más bien que monedas, los sistemas de monedas tradicionales, son un sistema de montos.

En Bitcoin, con una idea similar, pasa exactamente lo mismo.
La diferencia principal se encuentra, en que el valor de los montos, no está prefijado, como pasa con el sistema de montos de las monedas en curso legal. Los montos de

Bitcoin, pueden tomar cualquier valor. Que será, concretamente, el valor de la transacción que lo creó. Esto último se refiere, a que cuando un Usuario, recibe una transacción, con ella, recibe uno o varios montos. Como si de billetes se tratasen. E independientemente del valor que estos tengan, se fundirán, como por así decirlo, en un nuevo monto. En otras palabras, es como si cada vez que alguien nos pagase en Euros, reuniese todos los billetes que necesitase para llegar a la cantidad acordada y crease con ellos un nuevo billete explícitamente para nosotros y con el valor de la transacción.

Este monto de Bitcoin, recibe el nombre de UTXO. Que significa, Transacción Pendiente de Gasto, o en inglés, Unspent Transaction Output. Y realmente, representa esta idea. Ya que un usuario, cuando recibe una transacción, con ella, recibe un monto único y completo. Que le da de forma indirecta a la transacción el estatus imaginario de monto.

Para finalizar, veamos todo esto con un ejemplo.

Pongamos por caso, que somos Usuarios de Bitcoin. Con una dirección de cartera A.
Lo primero a tener en cuenta, es que no podemos crear liquidez de la nada. Los fondos de los que dispongamos, habrán de haber llegado a nosotros mediante transacciones. Ya sea por parte del sistema, cuando minemos bloques, o por parte del resto de usuarios, mediante transferencias. Así que vamos a suponer, que nos llega una transacción t1, con un saldo de 4 Bitcoins, una transacción t2, con un saldo de 0’5 Bitcoins y una transacción t3 y t4, con un saldo de 6 y 1’2 Bitcoins respectivamente.
Bien, pues esto hace que disponga de 4 UTXOs, con los valores respectivos a cada transacción, para poder gastar. Y que aportan a la cuenta un saldo total de 11’7 Bitcoins.

Vamos a suponer también, que decido gastar 8 de esos Bitcoins. Mediante una transferencia a otro Usuario, con una dirección de cartera B. Deberé entonces, hacer un grupo de UTXOs, que igualen o superen dicha cantidad y mandar el mensaje al sistema. Como si de un pago en billetes se tratase. El mensaje, llamémoslo t5, podría formarse con las transacciones t1 y t3. Ya que hacen un saldo de 10 Bitcoins de los 8 necesarios.

Aunque como vemos, esto sobre pasa por 2 Bitcoins el saldo necesario.
Esto supondría en el sistema del Euro, que es usuario con la dirección de cartera B, nos devuelva la diferencia. Pero en Bitcoin no hace falta, nosotros mismos nos damos las vueltas. Básicamente, cuando creemos el mensaje, de los montos t1 y t3, crearemos una salida de 8 Bitcoins para el Usuario de la Wallet B y otra salida de 2 Bitcoins para nuestra Wallet. Entrando, al igual que para el usuario de la cartera B, como nuevos OTXOs en cada una de las respectivas carteras.

Así que como resumen final, yo acabaría con los UTXOs t2, t4 y t5, que tienen un saldo de 0’5, 1,2 y 2 respectivamente y que me dan un saldo total de 3’7 Bitcoins. Y el Usuario de la Wallet B, acabaría con el UTXO t5, que tiene un saldo de 8 Bitcoins, y que le deja con un saldo total de 8 Bitcoins.

Para finalizar, con todo esto visto, podemos deducir con facilidad, que los mensajes que se envían al sistema, como el que pusimos de ejemplo de Esther y Fernando deben modificarse, para adaptarse a los nuevos requerimientos.

Si recordamos dicho ejemplo, tenía la siguiente estructura: «Yo, clave pública 008646BBFB7D, transfiero a clave pública 3FD8C0A9C6FF 10 Bitcoins. Firmado con la clave privada de la clave pública 008646BBFB7D».
Y, con la nueva modificación, podría quedar de la siguiente manera: «Yo, clave pública 008646BBFB7D, transfiero los UTXOs t1 y t3, que forman un saldo de 10 Bitcoins, a clave pública 3FD8C0A9C6FF en un saldo de 8 Bitcoins y a clave pública 008646BBFB7D con un saldo de 2 Bitcoins. Firmado con la clave privada de la clave pública 008646BBFB7D».

Formato de una transacción (parte 1 de 2)
Ahora que ya sabemos como se producen realmente los pagos en el sistema Bitcoin, y que son los UTXOs, vamos a profundizar de una forma más técnica en todo esto, viendo la estructura y formato exacto de una transacción

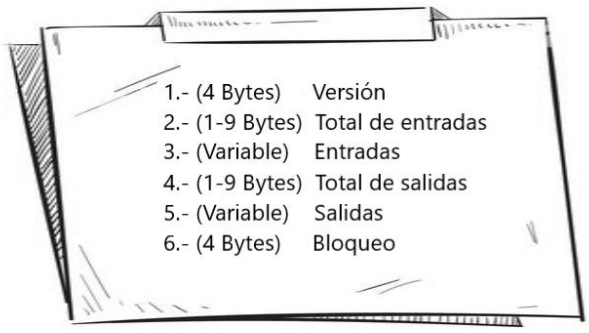

Ilustración 12: Formato general de una transacción en Bitcoin.
Fuente: Elaboración Propia (elementos gráficos extraídos de Internet)

La Versión, indica la versión del software que los Mineros de forma obligatoria deben usar para validar la transacción.

El Bloqueo, indica una condición de tiempo para que se pueda proceder a verificar la transacción por parte de los Mineros. Y que se rige por los siguientes códigos: 0, se puede validar directamente; >0-500 millones, no se puede validar hasta antes de ese número de bloque; >500 millones, que se interpreta como una fecha en formato UNIX, y que al igual que el código anterior, no se puede validar hasta pasado dicho sello de tiempo.

El Total de entradas y el Total de salidas, que como sus nombres indican, referencian el total de entradas y salidas que van a componer a la transacción.

Y las entradas y salidas. Son respectivamente, como hablamos en el punto anterior, los UTXOs que el Usuario va a gastar, y el nuevo UTXO que se genera para el Usuario receptor, o UTXOs en caso de que haya más de una salida.

Cada una de las Salidas de la transacción, tiene el siguiente formato:

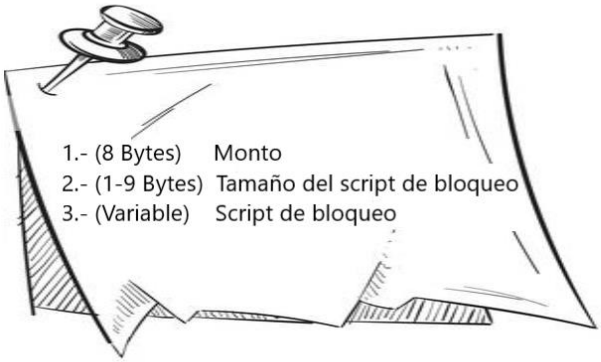

Ilustración 13: Formato específico de una salida de una transacción Bitcoin
Fuente: Elaboración Propia (elementos gráficos extraídos de Internet)

Compuestas, por el Monto, que referencia la cantidad de Bitcoins que va a percibir el Usuario receptor de la transacción y por ende, el valor de la UTXO generada; y por un Script de Bloqueo.

Ahora bien, ¿Qué es el Script de Bloqueo?

El script de bloqueo, es simplemente un seguro, en formato script, para que esta UTXO de salida solo pueda ser gastada por el Usuario correspondiente. Es decir, es un pequeño programa, que retiene los fondos, mediante una condición de bloqueo. Que será la dirección de Wallet, o clave pública, del Usuario destinatario. Para que solo este pueda gastar los Bitcoins asociados.

Como máximo, en cada transacción, habrá dos salidas. Una salida de fondos, destinados al usuario receptor de la transferencia. Y otra salida con el cambio de vuelta, en caso de que se produjese.

Y cada una de las Entradas de la transacción, tiene el siguiente formato:

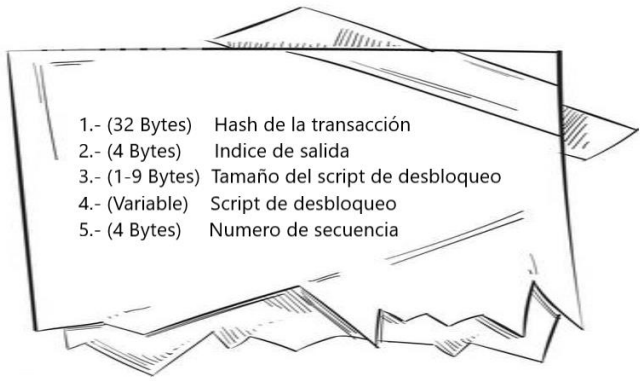

Ilustración 14: Formato específico de una entrada de una transacción Bitcoin
Fuente: Elaboración Propia (elementos gráficos extraídos de Internet)

Antes de nada, recordar que, un usuario no puede crear liquidez de la nada, por lo que las UTXOs que gaste, previamente han debido llegarle a través de una transacción. Y por tanto, estas UTXOs se han debido de crear, como acabamos de ver, en una salida de transacción.

Pues los campos de Hash de transacción e índice de salida, sirven para referenciar esas salidas y poder usar las UTXOs como entradas en esta nueva transacción.
El campo de Hash de transacción, es la referencia Hash, que identifica a la transacción del UTXO de salida que estamos buscando dentro de la Blockchain.
Y una vez que la tengamos localizada la transacción, el campo de índice de salida, sirve para concretar cual UTXO de salida, de todas las que componen dicha transacción, es a la que estamos referenciando.

Y con el campo de script de desbloqueo, podremos acceder a los fondos. Ya que es el inverso del campo script de bloqueo que tiene la UTXO de salida a la que estamos accediendo. Y sirve precisamente para eso, para desbloquear.
Obviamente, si el script de bloqueo tenía la clava pública, para restringir el acceso, este nuevo script, contendrá la clave privada. Que es la llave del candado que genera la pública.

Para finalizar con el formato de las entradas de una transacción. Nos queda hablar del campo número de secuencia. Este actualmente está en desuso y se completa con el siguiente valor: 0xFFFFFFFF.

Comisiones
La Mempool, es una base de datos compartida, que funciona como memoria temporal para almacenar de forma momentánea todas las transacciones que vayan llegando al sistema y aún no hayan sido confirmadas por parte de los Mineros.
Es un concepto simple, y que permite que todo el sistema de Bitcoin funcione. Pero tiene una curiosidad. Y es que, no funciona como una cola FIFO, como podríamos llegar a pensar. Para que así, las primeras transacciones que lleguen, sean las primeras en salir. Y se mantenga un correcto orden temporal en las transacciones.
Es una simple memoria, en la que el Minero, puede elegir que transacciones añade en su bloque y cuales no.

Ahora, la cuestión está en, ¿Por qué un Minero querría elegir unas transacciones por encima de otras? ¿Por qué no simplemente seguir un orden FIFO?

Y es que hay un concepto muy interesante, que no hemos hablado en los puntos relacionados con las transacciones y los UTXOs. Que es, que los usuarios, pueden añadir donaciones, a modo de comisiones, para aquel Minero que valide su transacción. Estas comisiones, reciben el nombre de Fee.

Esto, realmente es muy interesante. Ya que como hablamos en el punto de las recompensas. Hay un máximo de Bitcoins que pueden llegar a estar en circulación. Y que se estima que se alcance en el año 2140. Lo que produciría que ya no se pueda seguir recompensando a los Mineros por hacer su trabajo. Y por ende, que ya no exista ningún incentivo para seguir realizándose… y más como el poder computacional necesario para minar un bloque siga a este ritmo.
Así pues, que exista un sistema de comisiones, es una solución para incentivar a que un Minero siga realizando su trabajo. Independientemente de si recibe la recompensa por parte del sistema o no.

Claro está, que si esta recompensa desaparece, las comisiones que tenemos actualmente, incrementarán su costo, hasta posiblemente igualar la recompensa que debería seguir dando el sistema.

Pero como eso, de momento queda lejano. Vamos a centrarnos en las comisiones de hoy en día y en el papel que desempeñan.

Lo primero a tener en cuenta, es que, no es obligatorio realizar una “donación” por transacción. Cada usuario es libre de añadirla o no. Al igual que en decidir en la cantidad que la conformará. Eso sí, al igual que nosotros somos libres para decidir que comisión adjuntar con nuestra transacción. El Minero, es libre para seleccionar que transacción validará y cual no.

Lo que hace, que se pueda dar el caso, de que una transacción no siga su orden natural. Y pueda tardar horas o días en validarse. E incluso semanas y meses.

Es por todo esto, que se habla, de forma abstracta, de que hay niveles de prioridad en la Mempool. Con los niveles de bajo, medio y alto. Y que se basan, en cuanto de rápido se quiere que una transacción se valide y se añada a la Blockchain.

Si se quiere validar en el siguiente bloque, o en el peor de los casos, en algunos de sus siguientes. Esta transacción deberá tener una prioridad alta dentro de la cola.
Para lo cual, simplemente se deberá acompañar a la transacción con una comisión sustancial. Así pues, los mineros, se interesaran en la transacción y la añadirán al registro rápidamente. La misma idea, siguen los niveles de prioridad medio y bajo.

Aclarar que, aunque nuestra transacción tenga una prioridad alta, no nos asegura que se valide rápidamente. Puede tardar cualquier periodo de tiempo. Ya que este concepto de prioridad, de cara al minero no existe. Él, podrá seguir eligiendo las transacciones que quiera, aunque tengan una supuesta prioridad media o baja.
Y, aunque existirá, no nos salva del mismo resultado. Puede haber congestiones en la red que retrasen la validación de la transacción. Puede haber multitud de transacciones con la misma prioridad y que haga que nuestra transacción deje de resaltar por encima del resto. E incluso, que empiecen a llegar transacciones, con mayor comisión y que acaben convirtiendo a la transacción en una transacción de prioridad media.

Otro concepto a tener en cuenta en todo esto de la selección de transacciones. Es que, como hemos visto en el punto del formato de las transacciones. Una transacción tiene un tamaño variable. Puede haber transacciones muy pequeñas y transacciones muy grandes. Y que va en función de la cantidad de entradas y salidas que la compongan.

Una transacción grande, es menos interesante para almacenar en un bloque. Ya que, obviamente, ocupa más, y deja menos espacio para almacenar otras transacciones. Y con ello, la perdida de más comisiones.
Así pues, una transacción pequeña y con una comisión alta, es ideal para ser seleccionada por los Mineros.

Por otro lado, esto último, significa también, que las comisiones, no son universales. Una transacción grande, deberá pagar más comisión que una pequeña para obtener el mismo grado de prioridad en el Mempool.

Para finalizar, mencionar, que este sistema de comisiones, es beneficioso para la red al largo plazo. Ya que desincentiva a los usuarios a realizar transferencias de poco valor.
Que en principio, pueden parecer inofensivas. Pero la Blockchain está distribuida y cada usuario tiene una copia en su dispositivo. No conviene saturar el espacio de los dispositivos con transacciones ridículas.
Obviamente, se podrán seguir haciendo. Pero pagar una comisión elevada, por el traspaso de unos Bitcoins con un valor minúsculo. No es lo más apetecible para nadie.
Al igual, que tardar días o semanas en que se valide, por pagar una comisión muy baja, o incluso nula, como solución al primer problema de pagar una comisión muy por encima del valor de los Bitcoins traspasados.

Formato de una transacción (parte 2 de 2)
Las comisiones, son las únicas salidas de Bitcoins que no generan UTXOs. Así pues, si un Usuario, quiere incluir en su transacción una comisión, esta se reflejará como la diferencia entre las entradas y las salidas.

Veamos esto un poco más de cerca.

En el ejemplo del punto de las UTXOs, generábamos una transacción, t5, con dos UTXOs de entrada, que formaban un saldo de 10 Bitcoins; y dos UTXOs de salida, una de 8 Bitcoins a pagar y otra de 2 Bitcoins como vuelta de cambio.
Bien, pues si se quiere realizar una comisión de, pongamos, 0’5 Bitcoins. Esta se verá reflejada en la UTXO de vuelta de cambio. Que cambiará su valor de 2 Bitcoins a 1’5 Bitcoins.
Así, si hacemos el sumatorio de las entradas y salidas, tenemos lo siguiente: 10 (4+6) Bitcoins en las entradas y 9’5 (8+1’5) Bitcoins en las salidas.
Quedando reflejada la comisión de 0’5 Bitcoins para el Minero y sin necesidad de crear ninguna salida extra.

Obviamente, la diferencia siempre se reflejará en la UTXO de vuelta de cambio, ya que es el Usuario emisor el que realiza tanto el pago como la comisión, y por tanto, sus vueltas, tendrán que ser respecto al valor de ambos.

Ahora bien, ¿Cómo se queda reflejado en el sistema que el Minero recibe esa comisión si jamás se crea una UTXO?

Resolvamos esta cuestión viendo la estructura concreta de una transacción Coinbase.

Realmente sigue el formato normal de cualquier transacción, pero sus estradas y salidas tienen algunas particularidades.
Empezando por las entradas. La transacción Coinbase, tiene únicamente una entrada. Esta, no está asociada a ninguna UTXO. Simplemente, sirve, para reflejar, la creación de nuevas monedas por parte del sistema. Así pues, se podría decir, que la entrada en vez de apuntar a una UTXO, crear una nueva UTXO. Así pues, realmente, no existe entrada.
Y continuando por las salidas, tenemos también, que la transacción Coinbase, tiene una única salida. Esta salida, será la UTXO que reciba el minero como recompensa por minar el bloque, y por tanto, la que deba reflejar la recompensa del sistema y las comisiones.

Y precisamente así es como se forma. El script de bloqueo, asociará la UTXO a la dirección del minero, para que solo él pueda acceder a los fondos. Y el monto, tomará el valor del Halving junto con el sumatorio total de todas las comisiones que existan entre las transacciones que se hayan añadido al bloque.

Esta transacción, será creada por el propio minero. Cosa, que no es de sorprender, ya que cada usuario, crea sus propias transacciones. La única diferencia, que es la única transacción creada por el receptor, en vez por el emisor. Pero no es por eso por lo que se menciona. Es porque, como sabemos, una transacción es un conjunto de datos. Ordenados en diferente campos como hemos visto en el punto del formato de las transacciones. Pero como la Coinbase es una transacción especial. El sistema y el resto de usuarios, permiten que los mineros, puedan añadir algunos datos extras a la transacción.

Y es precisamente lo que hacen. Adjuntan unos pequeños datos extra al final de la transacción, a modo de texto, para personalizar su bloque.
Así es como, Satoshi, en el bloque Génesis incluyó el titular del The Times. Como comentamos en el punto del bloque Génesis.

Bifurcaciones

Como sabemos, cada bloque de transacciones además de pasar por la Proof of Work. Debe pasar por un proceso de votación, por parte de todos los usuarios de la red, para decidir, si el sistema puede almacenarlo de forma definitiva o no. ¿Ahora, cómo se lleva a cabo esta votación?

Cuando un Minero, consigue resolver la Proof of Work de su bloque de transacciones. Este, lo subirá a la red, dando por hecho que es válido. Y conforme se vaya propagando de usuario en usuario, estos, decidirán si es válido realmente o no.
Si es válido, lo aceptarán en su copia de la Blockchain, y sino, lo ignorarán como si nunca se lo hubiesen compartido.
Obviamente, si es de verdad válido, acabará en todas las copias de la Blockchain. Y si no lo es, caerá en el olvido, como si nunca hubiese existido.

Pero este proceso, permite que se produzca la siguiente casuística:

Como vimos en el punto del nivel de dificultad de un bloque y los 10 minutos. El bloque no se transmite de forma inmediata. Es un proceso gradual. Es decir, que puede que mientras se transmita este supuesto bloque válido, otro Minero, haya conseguido resolver también la Proof of Work de su bloque y por ende lo haya empezado a transmitir. Ya que al no llegarle el bloque que se está transmitiendo, no sabrá que ya se ha encontrado una solución. Que deja invalido al resto de bloques que estaban luchando por esa posición.

Así pues, según el proceso de votación, conforme vayan llegando ambos bloques a los usuarios, cada uno de estos, aceptará el primer bloque que le llegue e invalidará el segundo. Ya que lo considerará como un intento de modificación de su Blockchain.
Es decir, habremos roto la Blockchain. Una parte de los usuarios tendrá una versión de la Blockchain y otros otra. A este concepto, de tener más de una versión de la Blockchain, se le conoce como bifurcación.

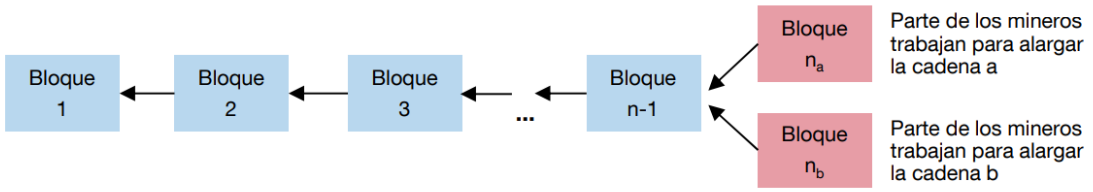

Ilustración 15: Bifurcación de la Blockchain
Fuente:https://www.bde.es/f/webbde/SES/Secciones/Publicaciones/PublicacionesSeriadas/DocumentosOcasionales/19/Fich/do1901.pdf

El problema se resuelve con la llamada regla de la Cadena Lineal más Larga. Que determina que la copia de Blockchain con más bloques validados, y con ello que más poder computacional incorpora, constituye la versión correcta del registro de transacciones.

En el caso del ejemplo, tenemos dos bifurcaciones. Ambas del mismo tamaño. Ya que unos usuarios tiene una copia de la Blockchain con el bloque, llamémoslo n_a; y otros con el bloque n_b. Y el conflicto se resolverá, cuando uno de los usuarios de ambos bandos, consiga minar un nuevo bloque y añadirlo a la Blockchain. Ya que supondrá que la copia de dicho bando, tendrá más bloques validados. Concretamente en uno más.

Si ponemos de ejemplo, que lo consiguen validar los usuarios de la bifurcación del bloque n_a. Tendremos que estos usuarios dispondrán de una copia con los bloques anteriores al n_a/n_b, el n_a y el bloque n_{a+1}. Mientras que los otros, dispondrán de una copia con los bloques anteriores al n_a/n_b y el n_b. Es decir, de un bloque más. Y cuando este se vaya propagando. Los usuarios de la cadena n_b, en vez de rechazar el bloque (ya que no coincidiría la referencia al bloque anterior), corroborarían que hay una copia más larga que referencia a ese bloque, y se cambiarían de bifurcación.

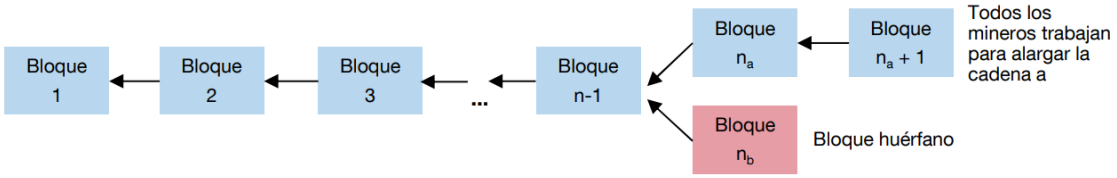

Ilustración 16: Resolución de bifurcación de la Blockchain
Fuente:
https://www.bde.es/f/webbde/SES/Secciones/Publicaciones/PublicacionesSeriadas/DocumentosOcasionales/19/Fich/do1901.pdf

Como nota, mencionar que, este proceso de bifurcación podría darse de nuevo en una rama ya bifurcada. Pero no tiene importancia que se de o no, y ni si quiera en cuantas veces. Al final, va a llegar un momento, en el que un usuario consiga validar y transmitir un bloque antes que ningún otro, y todas las bifurcaciones se unificarán en dicha rama. Es más, es poco probable que se repitan muchas bifurcaciones seguidas. Es muy difícil encontrar un bloque valido, para que se de el caso, de que varias personas lo encuentren de forma simultanea.

Realmente, la solución de aplicar la regla de Cadena Lineal más Larga. Trae consigo otro problema. Y es que, el bloque de la rama que se desestima, el bloque n_b, queda completamente invalidado. Y se le conoce como bloque Huérfano.

Todas las transacciones del bloque Huérfano vuelven al Mempool como si nunca se hubiesen validado. Aunque haya aparecido alguna vez como tal. Y el Minero, pierde la recompensa que una vez ganó.

Es por esto, que se aconseja, que los Usuarios, tanto si son receptores como emisores, para confirmar que se a realizado la transacción en la que están involucrados, esperen a que el bloque que la contiene esté bajo la validación de un par de bloques más. Recomiendan que el bloque esté bajo 2 o 3 bloques más. Incluso se oye hablar de 5.

La solución de eliminar el bloque Huérfano, trae consigo de nuevo otro problema. Y no es que le hayamos dado una “buena” noticia al Minero que ha perdido sus recompensas. Tiene que ver, pero no es. Básicamente, nos encontramos con que en el trascurso de la bifurcación los mineros que han generado los dos bloques paralelos, pueden gastar sus recompensas. Y cuando se vuelva a una versión unificada de la Blockchain. Uno de ellos, habrá realizado una transferencia que no debería de haber realizado.

Esto se soluciona con un concepto denominado Coinbase Maturity. Y que viene a representar, que para que se pueda gastar una UTXO asociada a una Coinbase, el bloque contenedor de la misma debe haber recibido 100 confirmaciones. O dicho de otro modo. Para que el Minero pueda acceder y gastar sus recompensas, ha de esperar que el bloque que las ha generado, esté bajo el minado de 100 bloques más.
Hasta entonces, si realiza una transacción usando como entrada esta UTXO, el resto de usuarios la invalidarán.
Pero no tiene que esperar mucho. 100 bloques a 10 minutos, dan 1.000 minutos. A 60 minutos por hora. Da, que de media, para que un Minero pueda reclamar de forma oficial su recompensa, debe esperar 16 horas y media.

Árbol de Merkle

El Árbol de Merkle es un concepto muy interesante que incorpora Bitcoin. Fue propuesto a principios de los 80 por Ralph Merkle, como una estructura de datos que permite verificar de manera eficiente la integridad de un gran conjunto de datos.

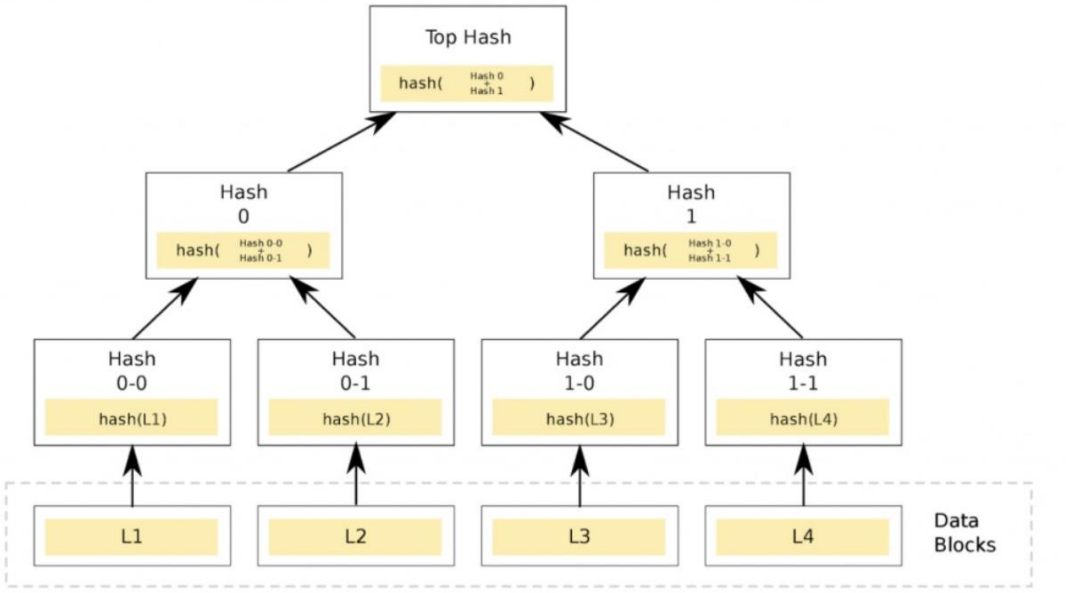

Ilustración 17: Estructura de un Árbol de Merkle
Fuente: https://observatorioblockchain.com/

Como podemos observar en la *ilustración*, el Árbol de Merkle consiste en reducir, mediante funciones Hash, los datos a validar en una sola función Hash. Que se conoce como Merkle Root.

Esta Merkle Root, al formarse mediante funciones Hash, coincidirá con el valor de otra Merkle Root, si ambas se han construido con los mismos datos. Y por tanto, le confiere al Árbol de Merkle dicha propiedad de validador de conjuntos de datos.

El Árbol de Merkle en Bitcoin se construirá con todas las transacciones de cada bloque de datos. Así pues, ahora, cada bloque de transacciones contendrá los siguientes campos: las transacciones, la referencia Hash del bloque anterior, el Nonce y la Merkle Root, formada con todas y cada una de las transacciones anteriores.

Entrando en el por que de todo esto. En el por que Bitcoin usa los Árboles de Merkle. Podemos decir que, Satoshi quería una correcta optimización en el uso y creación de bloques. Ya que tratar con estos, significa tratar con 2.000 - 2.300 transacciones como sabemos. ¿Y por qué hacer esto, si se puede tratar simplemente con un valor Hash que me las resume?

Esto es muy útil en el proceso de minado. Y realmente, no es que suponga ningún inconveniente a día de hoy tratar con tal cantidad de transacciones. Ni desde el punto de vista del procesador, ni de la RAM. Pero si tengo que realizar una y otra vez una función Hash con los campos del bloque, para ver si consigo obtener un Hash que respete las normas de creación. Es interesante, realizarlo solo con unos pocos datos, que no con todo el bloque completo.

Además, Bitcoin, siguiendo el mismo objetivo de eficiencia, también usará esta Merkle Root como se diseño. Es decir, como validador de datos. Cuando se realicen traspasos de bloques entre usuarios, estos deben de asegurarse que no sean corruptos,

comparándolos con otros bloques de la Blockchain. Y usar el protocolo del Árbol de Merkle, ahorra bastante tiempo en ese sentido.

Otra propiedad interesante de las Merkle Root, es la relativa a los Nodos Ligeros. Que no son más que aquellos usuarios que no tienen una copia completa de la Blockchain. Solo una parte. Ya que, si un usuario está ejecutando el protocolo de Bitcoin en un dispositivo de bajos recursos, no desea descargar y Hashear todas las transacciones de un bloque. Como puede darse, en los usuarios de dispositivos móviles y tablets.

Normalmente, estos nodos, tendrán una copia completa de la Blockchain, pero sin las transacciones. Los bloques, solo contendrán los campos: del Hash del bloque anterior, el Nonce que lo formó, y el resumen de las transacciones como una Merkle Root.

Y aunque estos Nodos Ligeros no puedan acceder ni a las transacciones ni a su contenido. Si pueden estar interesados en comprobar que una transacción en concreto está incluida en un bloque de datos.
Por ejemplo, para que un usuario de dispositivo móvil, corroboré que la transacción que ha realizado, con independencia de si es el emisor o receptor, se ha validado correctamente en el sistema.

Para ello, hay un proceso, denominado Verificación de Pago Simplificado (SPV). Y que consiste, en que dicho Nodo ligero, solicita una Prueba de Merkle a un usuario que tenga la Blockchain completa.

Esta Prueba de Merkle consiste en pasarle al usuario del Nodo Ligero, la secuencia de Hashes necesaria para que este forme la Merkle Root. Y pueda comprobar con la suya si coincide. Si coincide, es que la transacción se encuentra en ese nodo. Sino no se encuentra en ese nodo. Y no hay posibilidad de fallo o falsificación. Ya que la única manera de conseguir la misma Merkle Root, es con los mismos Hashes de los mismos datos, sino, es imposible.
Concretando más sobre qué y cuales son estos Hashes necesarios para generar el Merkle Root. Pongamos de ejemplo, que queremos validar la transacción L3 de la *ilustración* anterior. El nodo completo, ha de remitirnos de vuelta, el valor, del Hash1-1 y el del Hash 0. Para que así el nodo ligero, con el Hash de la transacción L3, que es el valor Hash1-0, y con el valor del Hash1-1, remitido por el nodo completo; forme el valor de Hash 1. Y junto con el valor del Hash 0 (del nodo completo) forme el Top Hash.
Este Top Hash, es la Merkle Root, y ya podrá compararla con la que el dispone en su copia.

Obviamente, este proceso, se realiza con bloques que tienen entre 2.000 - 2.300 transacciones, no 4. Pero seguiría la misma filosofía.

Contenido de un bloque de datos (parte 2 de 2)
Ahora que conocemos de una forma más concreta el sistema Bitcoin y hemos analizado los campos más importantes que conforman a un bloque de transacciones. Vamos a estudiar el contenido integro de estos bloques de la Blockchain.

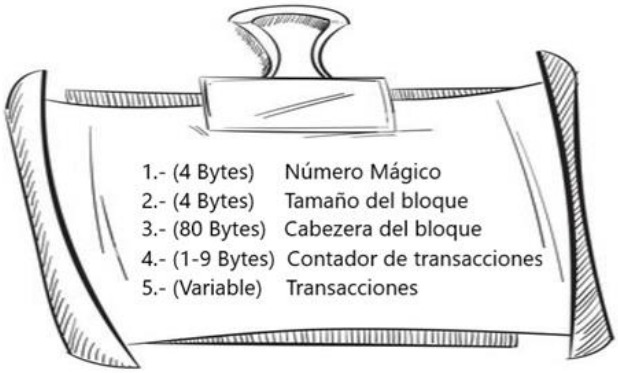

Ilustración 18: Contenido de un bloque de transacciones en la Blockchain
Fuente: Elaboración Propia (elementos gráficos extraídos de Internet)

El Número Mágico, en programación, se trata de un número constante que se utiliza para identificar el formato de un archivo o protocolo. En el caso de Bitcoin, este número sirve para identificar cuándo empieza y cuando termina un bloque de transacciones. Y siempre tendrá el mismo valor: 0xD9B4BEF9.

El tamaño del bloque, se define así mismo. Al igual que el contador de transacciones y las transacciones.

Así pues, solo nos queda examinar la Cabezera del bloque. En la que como mínimo tiene que estar el Hash del bloque anterior, el Merkle Root y el Nonce. Veamos su estructura:

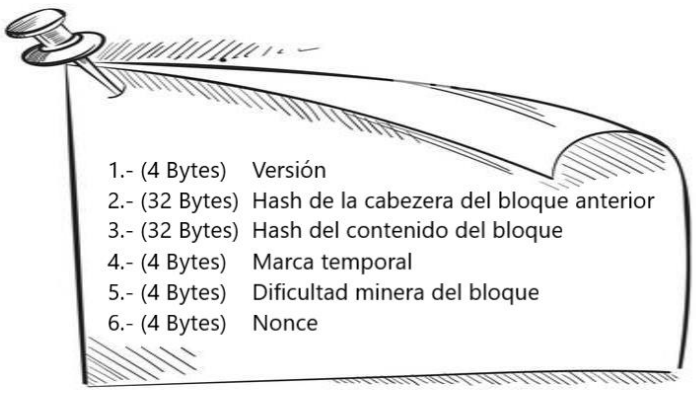

Ilustración 19: Contenido de la cabezera de un bloque de transacciones en la Blockchain
Fuente: Elaboración Propia (elementos gráficos extraídos de Internet)

La versión, indica la versión del software de Bitcoin que se ha usado por parte del Minero para generar el bloque de transacciones.

El Hash de la cabecera del bloque anterior, es obviamente el Hash del bloque anterior.

Y el Hash del contenido del bloque, es la Merkle Root.

La marca temporal, es una marca de tiempo estilo UNIX, que indica el momento exacto en el que fue minado el bloque de transacciones. Esta, es un número que equivale a los segundos pasados desde enero de 1970.

La dificultad minera del bloque, indica el Nivel de Dificultad en el momento de minar el bloque de transacciones.

Y el Nonce, se define a sí mismo.

3. Seguridad en el sistema Bitcoin

Día tras día, se escucha hablar de que Bitcoin es completamente seguro. Totalmente hermético. Totalmente impenetrable. Pero realmente no es así.
Hay dos puntos débiles en el sistema. Ambos de construcción. Ambos permitidos por las reglas que rigen Bitcoin. Ambos, una excepción para la completa seguridad del sistema.

Primera vulnerabilidad
El propio Satoshi Nakamoto, en su Paper, deja claro que, “El sistema es seguro mientras los nodos honestos controlen colectivamente más potencia CPU que cualquier grupo cooperante de nodos atacantes” [1].
Si de momento la Blockchain sigue intacta, es porque dicha norma se cumple, nada más. El día que un grupo de atacantes, logre reunir más potencia de calculo que el resto de la red, aunque sea durante escasos minutos, Bitcoin, quedará a su merced.

Sabemos, que para subir un nodo a la red, hay que completar una Proof of Work. Que consume una cantidad ingente de potencia de calculo. Y después, hay que someterlo a un proceso de votación.
Si conseguimos suficiente potencia de calculo, podemos intentar amañar el proceso de votación. Se puede conseguir minar un bloque, subir dicho bloque corrupto a la red, y aceptarlo por un ejercito de identidades falsas.
Pero, esta solución, es igual de fácil como absurda. (Fácil, quitando la parte de conseguir el Nonce válido, claro está).

¿Qué significa aceptar un bloque de transacciones? Significa añadir el bloque a cada una de las copias privadas de la Blockchain, y seguir minando bloques a partir de el.

Así pues, el problema de esta solución reside, en que los nodos honestos, jamás aceptarán el bloque. Se crearán dos ramas de la Blockchain. Y por tanto, cuando estos, vayan añadiendo bloques, como tiene más potencia de calculo, rápidamente, añadirán más bloques y por la regla de la Cadena Lineal más Larga, harán de su bifurcación, la bifurcación válida para toda la red. Y el bloque supuestamente validado, quedará invalidado.

Esto no es nuevo, y realmente ya se habló en el apartado anterior. Solo era para recordar y poner un poco en contexto todo esto de la potencia de cálculo.

Ahora si, entrando en materia. Para poder falsificar el contenido de uno o varios bloques de la Blockchain, debemos crear una bifurcación, con el suficiente procesamiento en CPU, que nos permita crear una cadena suficientemente larga de bloques, que por la regla de la Cadena Lineal más Larga, sea aceptada en la red de forma unánime.

Así pues, esto significa, que vamos a necesitar minar bloques de transacciones más rápido que el resto de la red. Para conseguir superar cualquiera de las bifurcaciones que se generen a partir del bloque corrupto.

Suena simple en papel. Pero en la práctica, todo esto se vuelve más complejo.

Lo primero a tener en cuenta, que la cadena corrupta, en el momento de su creación va a partir de como mínimo un bloque de desventaja.
Esto es, que si queremos añadir un bloque, sin modificar ninguno del pasado. Tenemos que crear, junto con nuestro bloque corrupto, un bloque adicional. Que nos de la ventaja, con respecto a la bifurcación honesta, en la cual, solo hay que añadir un bloque más.
Y si queremos modificar un bloque del pasado, debemos modificar el bloque del pasado, arreglar toda la cadena de referencias perdidas y añadir dos bloques adicionales más, que nos den de nuevo, la ventaja con respecto a la bifurcación honesta en la que solo hay que añadir un bloque más.

Es decir, no solo debemos tener exactamente el mismo procesamiento de cálculo que toda la red en conjunto, sino, superarla. Para que así, podamos minar este bloque adicional que necesitamos para cumplir la regla de la Cadena Lineal más Larga. Y eso, contando que estamos intentando el mejor caso de éxito, que es el de añadir un bloque corrupto sin modificar nada de lo anterior.

Y todo esto sin contar, que cada bloque que avancen los nodos honestos, deben avanzarlo los nodos atacantes para encontrarse en la misma situación que la inicial. Sino, irán perdiendo terreno.

Si tomamos números, la probabilidad de que un atacante alcance a la cadena honesta, se ve como un paseo aleatorio binomial como sigue:

p = probabilidad de que un nodo honesto encuentre el siguiente bloque
q = probabilidad de que el atacante encuentre el siguiente bloque
q_z = probabilidad de que el atacante alcance [la cadena honesta] desde z bloques atrás

$$q_z = \begin{cases} 1 & \text{if } p \leq q \\ (q/p)^z & \text{if } p > q \end{cases}$$

Ilustración 20: Probabilidad de que un nodo atacante alcance a los nodos honestos en Bitcoin
Fuente: https://bitcoin.org/files/bitcoin-paper/bitcoin_es.pdf

Si se asume que p > q, es decir, que la mayor potencia de calculo la posen los nodos honestos, la probabilidad cae de forma exponencial a medida que aumenta el número de bloques que el nodo atacante quiere alcanzar.

Así pues, con las probabilidades en su contra, si desde el principio no tienen un golpe de suerte que los hagan avanzar, sus oportunidades se irán desvaneciendo a medida que se vayan quedando atrás.

En resumen, cualquier grupo de atacantes puede intentar y conseguir minar una cadena de bloques corrupta y subirla como correcta a la Blockchain, ya que no es imposible. Eso sí, las probabilidades de éxito son muy bajas.

En caso de que lograran conseguirlo, tampoco sería el fin de Bitcoin. No pueden hacer lo que quieran. El propio sistema por construcción, fija una normas para la construcción de bloques y transacciones. Y aunque el bloque se corrompa, no puede convertirse en otra cosa que no es.

Cada bloque, contiene única y exclusivamente transacciones. Y estas, tienen un formato. Así pues, lo que pueden corromper, son algunos datos de las transacciones. Y sí, algunos datos, porque no pueden modificar lo que quieran.
No pueden crear Bitcoins de la nada, cada transacción, debe hacer referencia a las respectivas UTXOs de entrada y estas, deben existir. Tampoco pueden acceder a las UTXOs de entrada que quieran, cada una de estas, tendrá asociado un script de bloqueo, que los atacantes no disponen, ni dispondrán nunca. Tampoco pueden modificar la Coinbase, que obviamente estará destinada a ellos, debe crearse con el Halving pertinente y con el total de las comisiones que tengan las transacciones. Y tampoco se pueden crear transacciones invalidas.

Lo único que se puede corromper es una de sus propias transacciones para recuperar el dinero que se ha gastado en ella. Remitiéndose el monto de entrada a una dirección de cartera controlada por ellos, en vez de a la Wallet original.

Así pues, y resumiendo todo lo redactado en este apartado, un usuario honesto, puede ser engañado por un grupo de atacantes de la siguiente manera:

Tener una transacción validada en la Blockchain por un bloque de transacciones, e incluso que este bloque esté asegurado bajo la validación de varios bloques más y que acabe modificándose la transacción en un futuro para que los saldos que le pertenecían acaben en la dirección de Wallet del atacante.

Volviendo a resumir, todo esto, se puede llevar a cabo de la siguiente manera:

Los atacantes pueden modificar bloques pasados o añadir nuevos bloques corruptos. La practica que se puede realizar con la primera posibilidad se auto explica sola. Pero la segunda, merece mención. Cuando un atacante suba una transacción, este, puede empezar a trabajar en una cadena paralela de bloques, en el que dicha transacción no exista. Así, el usuario victima creerá en todo momento que su transacción es valida, y cuando los atacantes logren alcanzar a la cadena honesta, la transacción se revertirá.

Realmente, las dos practicas son exactamente iguales. La única diferencia es que una empieza en algún bloque del pasado, y la otra en el mismo momento que tiene lugar la transacción y por tanto en el bloque actual.

Satoshi, hizo algunos cálculos para precisamente esto. Para tener un aproximado de cuanto tiempo debe esperar el receptor de una transacción para tener la suficiente seguridad de que el emisor no puede cambiarla. Y se resumen en lo siguiente:

```
P < 0.001
q=0.10   z=5
q=0.15   z=8
q=0.20   z=11
q=0.25   z=15
q=0.30   z=24
q=0.35   z=41
q=0.40   z=89
q=0.45   z=340
```

Ilustración 21: Número de bloques que aseguran que una transacción no se puede modificar
Fuente: https://bitcoin.org/files/bitcoin-paper/bitcoin_es.pdf

Los cálculos completos se pueden consultar en el Paper de Satoshi, estos son simplemente los resultados finales.

Segunda vulnerabilidad

Esta vulnerabilidad, realmente no es una vulnerabilidad en el sistema como la anterior. Es simplemente una practica, que Bitcoin permite, para que se pueda engañar a los usuarios que quieran ser engañados.

Se sustenta en el método de verificaciones de transacciones. Y en la confianza que deposite la gente en el sistema. Si recordamos, cuando un usuario realiza una transacción a otro usuario, esta, llega al Mempool. Y se queda ahí, hasta que un Minero, decida recogerla en su bloque de transacciones y validarla. Momento en el cual, quedará visible para todo el mundo, incluidos ambos usuarios, y se habrá realizado el pago.

Pues en todo ese proceso, si el usuario victima, no toma cartas en el asunto, y se asegura que su transacción está correctamente validada y serializada en la Blockchain, puede ser engañado.

Veámoslo mejor con un ejemplo:

Vamos a suponer, que un usuario emisor, quiere realizar una transacción a otro usuario, para comprarle una prenda de ropa. Pues si el usuario receptor, el usuario victima, le entrega al usuario emisor dicha prenda de ropa, simplemente porque se realice la transferencia de Bitcoins, está cometiendo un error. El usuario emisor, inmediatamente después de pagar y recibir la prenda. Puede realizar una transferencia, por ejemplo a otra cuenta de su propiedad, con los mismos fondos y con una comisión más elevada a la que se haya asociado al pago.
Esto hace, que ambas transacciones tengan un nivel de prioridad diferente en la Mempool. Y con un poco de suerte, si hay muchas transacciones entre medias. Puede darse el caso de que cuando los Mineros, recojan las transacciones para validarlas, cada una, caiga en un bloque diferente. Quedando, obviamente, el pago al usuario victima por debajo del pago falso.
El sistema, validará el primer pago. Y el segundo lo invalidará. Ya que supondrá una violación de las normas de Bitcoin. Al estar gastando un saldo que ya ha sido gastado.
Y el usuario victima, habrá sido estafado. Por eso es esencial asegurarse que el pago se ha realizado antes de hacer nada.

Pero esto no es todo, si el usuario victima, no se asegura tampoco que el bloque que valida su transacción está confirmado bajo un par de bloques más. Como comentamos en el punto de las Bifurcaciones. Es posible, que pueda darse el caso de que dicho bloque, sea un bloque bifurcado. Y que acabe convirtiéndose en un bloque Huérfano.

Esto hará, que la transacción vuelva al Mempool, como si nunca se hubiese validado. Y si el usuario emisor, de nuevo, envía al sistema una transacción falsa con los mismos fondos. Ambas quedarán en el Mempool con la situación antes descrita.

Y sin contar, que cabe la posibilidad, de que ya haya sido validada en alguno de los bloques de la otra rama. Y por tanto, cuando la transacción real vuelva al Mempool, la falsa, ya esté validada en el sistema.

Obviamente, el caso de éxito de está opción, es menos probable que la anterior. Ya que tiene que darse que el bloque que haya validado la transacción real, caiga en una bifurcación. Y encima, que la rama de la bifurcación a la que pertenece, sea rechazada. Aun así, es probable, y se puede dar. Por lo que de nuevo, es esencial asegurarse que el pago, se ha realizado y que está confirmado bajo varios bloques.

4. Bitcoin como medio de pago

Transacciones por segundo

Recuperando cifras de los apartados anteriores, tenemos que Bitcoin procesa bloques de transacciones cada 10 minutos. Esto es unos 144 bloques al día. Si cada uno de los bloques contine, unas 2.000 - 2.300 transacciones. Nos encontramos, con que Bitcoin puede soportar unas 331.200 transacciones al día. O lo que es lo mismo 3’83 transacciones por segundo.

Y eso teniendo en cuenta los valores teóricos. En la practica, todos estos valores son dinámicos y varían con el tiempo. Concretamente, a día de hoy, agosto de 2022, podemos encontrarnos con los siguientes valores:

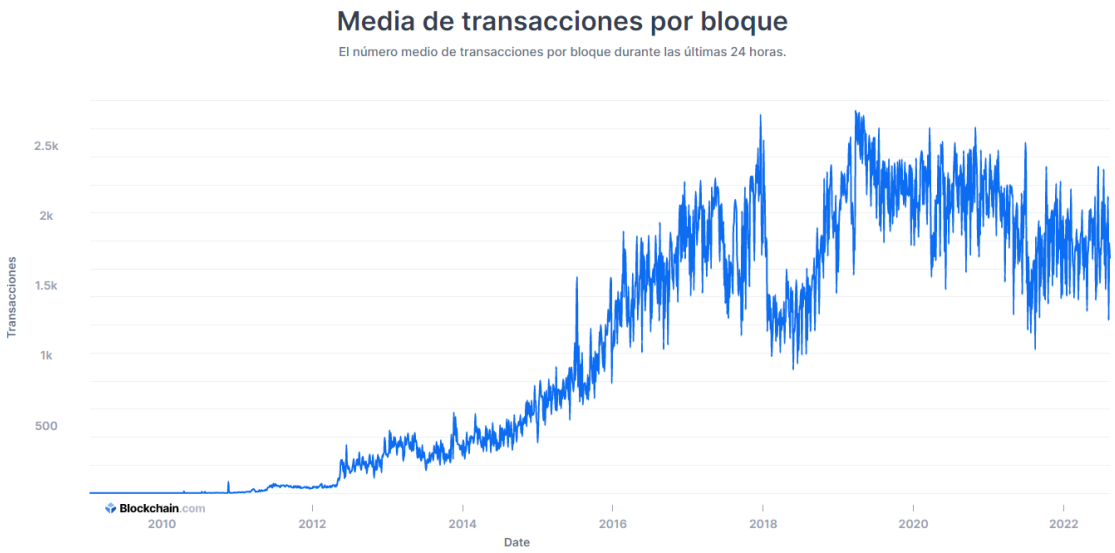

Ilustración 22: Número de transacciones por bloque en Bitcoin
Fuente: https://www.blockchain.com/es/charts

A una red Bitcoin soportando 1.678 transacciones por bloque, en comparación a las 2.300 teóricas que se llevaban hablando varios años atrás.

Ilustración 23: Número de transacciones por día en Bitcoin
Fuente: https://www.blockchain.com/es/charts

A unas 233.308 transacciones por día, en comparación de las 331.200 transacciones que nos habían salido anteriormente.

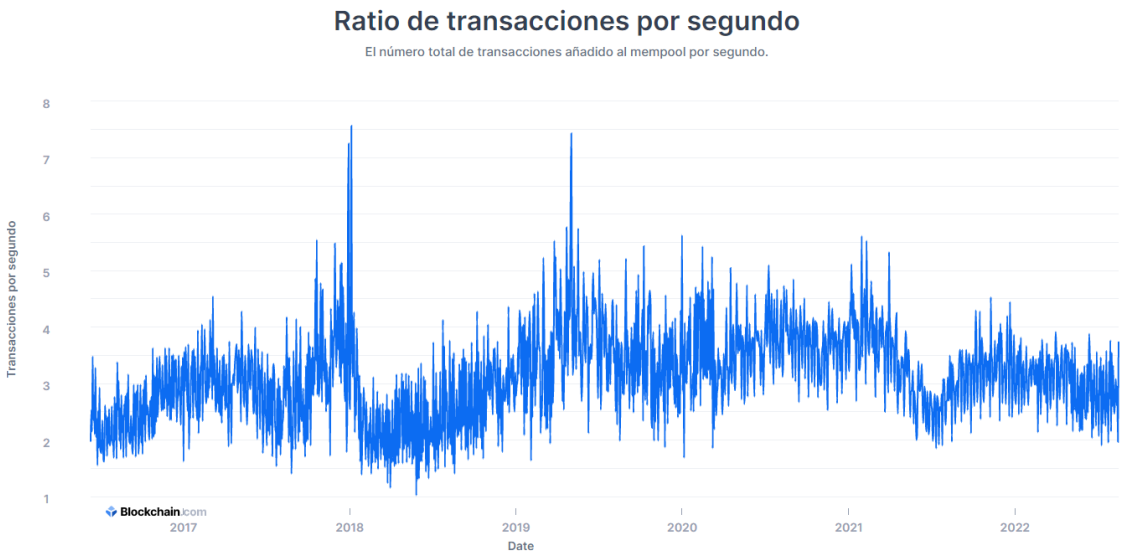

Ilustración 24: Número de transacciones por segundo en Bitcoin
Fuente: https://www.blockchain.com/es/charts

Y a unas 2’95 transacciones por segundo, en comparación de las 3’83 transacciones por segundo teóricas.

Esto, sin tomar perspectiva no representa nada. Pero si lo comparamos con sistemas de pago tradicionales, como VISA o Mastercard, que tienen 24.000 y 5.000 transacciones por segundo respectivamente. Vemos que Bitcoin se queda bastante en la cola.

Cosa que realmente no supondría ningún problema, si no pretendiese ser una alternativa a los medio de pago tradicionales. O al menos, lo que pretende o quieren que pretenda actualmente.
Es decir, el tener un valor de transacciones por segundo tan bajo puede producir un cuello de botella enorme si se pretende abarcar todas las transacciones que se lleven a cabo en el día a día en todo el mundo.

Comisiones
A día de hoy, las comisiones por transacción se han vuelto obligatorias si se quiere incluir dicha transacción en la Blockchain en un lapso de tiempo aceptable.

Incluso se está dando el caso de que las transacciones sin comisión o con una comisión muy baja se queden de forma indefinida en la red. Ya que van llegando de forma constante nuevas transacciones al sistema, con una comisión asociada mayor, que van dejando siempre a estas al final de la cola.

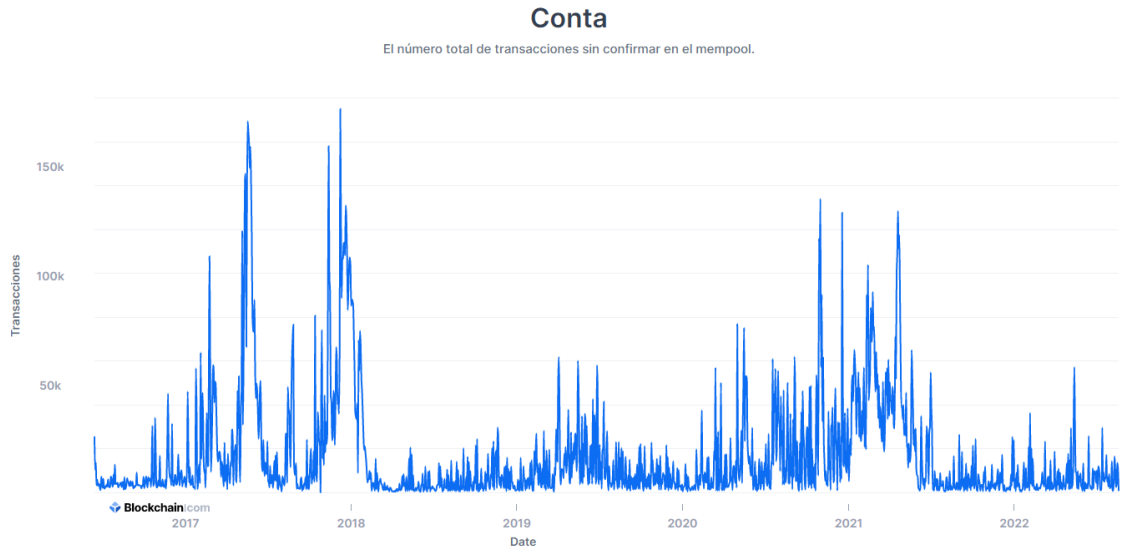

Ilustración 25: Número de transacciones sin confirmar en el Mempool
Fuente: https://www.blockchain.com/es/charts

Como resultado tenemos a día de hoy que, para que se llegue a validar una transacción hay que pagar de media una comisión 1’216 $.

Ilustración 26: Comisiones en USD en Bitcoin
Fuente: https://www.blockchain.com/es/charts

Por lo que realizar pagos pequeños y micro pagos, dejan de ser tan atractivos. Aunque si que es cierto, que para pagos medios o grandes, no es un gran inconveniente.

Pero si al igual que antes, Bitcoin pretende sustituir a los medios de pago tradicionales y con ello abarcar absolutamente todas las transacciones del día a día, puede llegar a ser un problema de cara al usuario. Transferencia tras transferencia, los usuarios van a ir acumulando una carga monetaria en comisiones demasiado grandes para que usar Bitcoin sea atractivo.

Rapidez
Lo más rápido que el sistema puede validarnos una transacción, es en un lapso de tiempo de 10 minutos. Verificando el pago de forma inmediata con el siguiente bloque de transacciones disponible desde el momento en el que tiene lugar la transferencia.

Pero realmente esto no es así. Como sabemos, es recomendable, por no decir obligatorio, que el receptor de una transacción espere a que se añadan una media de 5 bloques más al registro, para asegurar que sus fondos son inmutables.

Esto hace, que para que un pago se verifique de forma correcta, han de verificarse 6 bloques, uno que la contenga y cinco que la validen. A una media de 10 minutos cada uno, hace que, para cada pago, se tarde como mínimo 60 minutos en ser verificado.

Y sí, como mínimo, ya que la transacción solo será incorporada en el siguiente bloque si tiene consigo una comisión sustancial… si no, quedará en la cola hasta nuevo aviso.

Esto hace, que de nuevo Bitcoin sea incompatible como media de pago diario. Los comerciantes, o cualquier otro tipo de receptor de la transacción, no pueden esperar una hora o más a que se confirme el pago con cada uno de los cliente.

Utilidad como medio de pago
Bitcoin, a día de hoy, no puede soportar la carga que supondría convertirse en uno de los medios de pago principales a nivel diario y global.

Como hemos visto en este apartado, el procesamiento de transacciones es un cuello de botella para este objetivo. Y de cara a los usuarios, tanto emisores como receptores, las comisiones y el tiempo de verificación asociado a cada transacción, de forma respectiva a cada uno de ellos, no es para nada viable. Y más aún cuando convertir a Bitcoin en un sistema de pagos a gran escala solo haría que empeorarlo.

Si que es cierto que a día de hoy pretende serlo. O al menos, muchos usuarios y partidarios del sistema pretenden que así sea. Pero de momento no lo es.

Y sí, de momento no… porque el objetivo realmente es alcanzable. Bitcoin no es un sistema cerrado. Bitcoin es un sistema de código abierto. Y aunque a día de hoy Bitcoin no tenga capacidad para ser uno de los sistema de pagos principal, la comunidad que lo conforma tiene la posibilidad de modificar e incluso añadir todo lo que necesiten al software para lograrlo.

Es un objetivo a largo plazo, sí, pero al fin y al cabo, es un objetivo que se puede lograr.

Pero volviendo al presente, Bitcoin, a día de hoy, solo es un medio de pago alternativo a los tradiciones. Y es que es normal que esto suceda. Bitcoin y los sistemas de pago tradicionales no tienen los mismos objetivos.

Los medios de pago tradicionales tienen de objetivo facilitar el envío de dinero entre dos actores, de una forma rápida, sencilla, considerablemente segura y al menor precio posible. Mientras que Bitcoin, tiene de objetivo ser un sistema de pagos en el que no haya autoridades centrales que gobiernen el sistema y por tanto puedan controlarnos e

incluso censurarnos, entendiendo como tal a la posibilidad de detener o revertir transacciones

Objetivos distintos, sistemas distintos. No nos podemos sorprender porque Bitcoin no funcione de forma satisfactoria como sistema de pago tradicional.

Pero si funciona como el sistema que es. Un sistema que se puede usar para pagos ocasionales, sobre todo en aquellos que no queramos dejar rastro ni identificarnos. Como por ejemplo en los pagos realizados por Internet, en los que no haya confianza entre los usuarios, y por tanto, no se desee compartir información personal, como el número de la tarjeta o el nombre.

O simplemente porque queramos un sistema de pagos que no esté controlado por las entidades bancarias y el gobiernos. Y que nuestros pagos sean nuestros. Y con ellos, que toda la información asociada sea nuestra.

5. Bitcoin en el mundo real

Valor

Una disección importante es: ¿Qué utilidad tiene realmente Bitcoin en la sociedad? Hemos estado hablando en los apartados anteriores de que es un sistema de pago. Pero ¿Qué es un sistema de pago?

Antes de responder estas preguntas, es necesario tener claro un concepto base. Ya que sin el, no llegaremos a entender la resolución de la disección.
Valor ¿Qué entendemos por valor?

Según la Real Academia Española (RAE) el termino valor se puede corresponder con alguna de las siguientes definiciones:

1 “Grado de utilidad o aptitud de las cosas para satisfacer las necesidades o proporcionar bienestar o deleite” [18].
2 “Cualidad de las cosas, en virtud de la cual se da por poseerlas cierta suma de dinero o equivalente” [18].

Así pues, un recurso, ya sea bien o servicio, tiene asociado un valor positivo, aunque fluctuante en el tiempo, siempre que alcance un cierto grado de utilidad o aptitud que satisfaga las necesidades de una persona. Lo que hace que esta esté dispuesta a realizar un intercambio monetario o equivalente por poseerlo.

Ahí, y ya respondiendo a la disección, es donde entran los sistemas de pago como Bitcoin. Permiten facilitar la tarea de compra/venta de recursos. Cualquier usuario puede vender sus recursos por una cierta cantidad monetaria que equivalga a su valor y comprar otros con el proceso inverso.

Y esto es posible, porque al igual que los productos o servicios tienen un valor asociado, el dinero también lo tiene. No deja de ser un recurso más, susceptible a ser objeto de valor, y por la definición segunda de la RAE, a ser deseado por otras personas.

Por lo tanto, podemos decir que, la compra/venta es un proceso de intercambio entre recursos del mismo valor, en el que siempre un elemento de los mismos va a ser dinero.

En el tiempo y en la sociedad en la que vivimos, cualquier recurso tiene asociado un precio, basado en el mercado globalizado que existe y siguiendo la ley de la oferta y la demanda. Ese precio realmente no variará (con respecto a las diferentes monedas, el valor en sí siempre va a estar sujeto a fluctuaciones), variará la moneda en la que se oferta. Es decir, y poniendo de ejemplo un ordenador, es posible que ese ordenador en Estados Unidos valga 500$ y en España valga 495€.

A eso se le conoce como el poder adquisitivo que tiene cada moneda.

Bitcoin, como moneda y sistema de pago que es, también tendrá un poder adquisitivo dado en el mundo real. La manera más fácil de verlo, es comparado con alguna de las monedas de curso legal, como por ejemplo el Dólar. Ya que son sistemas muy implementados en la sociedad, y aunque no sabremos que podemos comprar con 1 Bitcoin, si sabremos que podemos comprar con 23.194$.

Ese es el valor a día de hoy, agosto de 2022, de Bitcoin. 1 Bitcoin equivale a 23.194$.

Pero al igual que el propio dólar y como hemos dicho más arriba, todos los recursos sin excepción tiene un valor fluctuante en el tiempo. El valor de Bitcoin a lo largo del tiempo se puede ver reflejada en la siguiente gráfica:

Ilustración 27: Valor de Bitcoin a lo largo del tiempo
Fuente: https://www.blockchain.com/es/charts

De los 21.000.000 de Bitcoins disponibles, actualmente se han producido 19.123.000 (agosto de 2022). Esto deja con el valor a día de hoy de Bitcoin un volumen de negoción total de 461.000.000.000$.

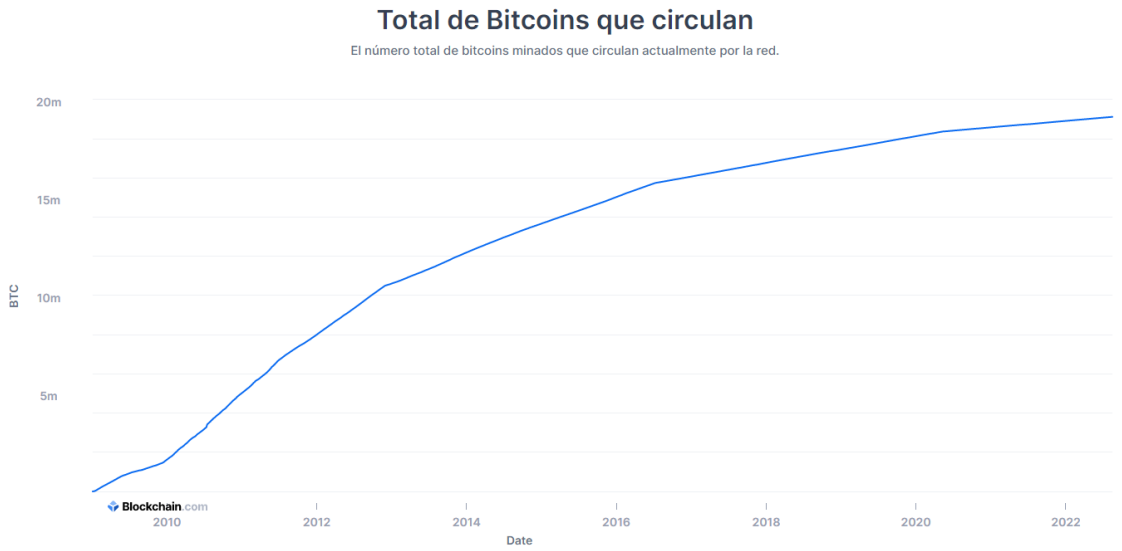

Ilustración 28: Bitcoins en circulación
Fuente: https://www.blockchain.com/es/charts

Ilustración 29: Volumen de negocio total de Bitcoin
Fuente: https://www.blockchain.com/es/charts

Actividades ilícitas

El anonimato y privacidad de Bitcoin han causado gran estrago en la sociedad. Gran número de malhechores han visto una oportunidad de oro para realizar cualquier actividad ilícita que se pueda imaginar de forma fácil y segura.

Como por ejemplo, comprar y vender todo tipo de objetos, sustancias o servicios sin necesidad de que se den a conocer quien está detrás de la compra por ambas partes. Y no solo entre ellos, sino de cara a todo el mundo.

Las transacciones no contienen ningún dato identificativo, ni de la persona ni de la compra, solo una dirección y un pago. Nadie sabe de donde sale ni a donde va. Y mucho menos por y para que se realiza.

Un lujo para mantener en la sombra lo que se quiere mantener en la sombra.

El inicio de todo esto se puede asociar a la famosa plataforma Silk Road. Un portal de venta de sustancias y servicios ilegales alojado en la Internet Profunda, que usaba el Bitcoin como medio de pago entre sus usuarios.
Afortunadamente, fue desalojada en octubre de 2013 por el FBI. Pero el tiempo que estuvo operativa fue más que suficiente para implantar una nueva metodología de pagos. Que aún se mantiene a día de hoy.
Y se puede ver en cualquier momento, solo es necesario contar con los medios necesarios, como por ejemplo con el más que conocido navegador Tor, acceder a la Internet Oscura o Dark Web, y navegar por la multitud de portales ilegales que existen. En donde podremos comprar cualquier cosa que se pueda imaginar mediante Bitcoins.

Se calcula que el 98% de las transacciones de la Darknet se realiza en Bitcoins.

Los Bitcoins no solo son un medio excepcional para la compra/venta. Es el sistema de pagos perfecto para financiar el terrorismo o blanquear dinero. Y es que volvemos a las mismas, Bitcoin permite mantener en las sombras lo que se quiere mantener en las sombras. Nadie gobierna o controla Bitcoin, y por tanto, nadie sabe que se mueve con cada transacción y por qué. Los emisores y receptores de dichas transferencias de dinero, pueden actuar impunemente, y peor aún, pueden hacerlo con total sosiego. Nadie puede bloquear sus transacciones al igual que nadie puede saber que es lo que están haciendo.

Ilustración 30: Resumen de Bitcoin y las actividades ilícitas
Fuente: Elaboración Propia (elementos gráficos extraídos de Internet)

Anonimato y privacidad
Realmente Bitcoin no es del todo anónimo. Se podría decir, que es más bien pseudoanónimo. Ya que en los pagos se refleja siempre una dirección de cartera emisora y otra receptora. Y aunque estas no estén asociadas a ninguna persona física, si representan a estas. Y por tanto, con las herramientas y metodologías adecuadas, se

podría llevar a cabo una buena labor de recopilación y posterior tratamiento de datos, que nos lleve directos a la persona física que posee la Wallet.

De igual manera pasa con la privacidad de las transacciones. Aunque las transacciones en sí no contengan información alguna sobre el pago. Con el historial público de Blockchain y los procesos adecuados de análisis de datos, se puede presuponer el fin de la transferencia.

Así, podemos concluir que, la tecnología Blockchain sin la ausencia de otras tecnologías no proporciona un servicio de anonimato y privacidad totalmente fiable.

Wallets, Exchangers y Cajeros

Con el notable crecimiento de la popularidad de Bitcoin más y más usuarios se han ido sumando al sistema. Usuarios de todo tipo, usuarios que saben como funciona Bitcoin y usuarios que no tienen idea en absoluto, usuarios que saben manejarse correctamente con las nuevas tecnologías, totalmente necesarias para poder operar con Bitcoin; y de nuevo, usuarios que no saben tanto.

Y es que a fin de cuentas, Bitcoin, no deja de ser un medio de pago. Un medio de pago abierto a todo el público.

Es por eso, que han salido al mercado herramienta que facilitan la vida a los usuarios promedio. Les ofrecen la posibilidad de operar con Bitcoin de la forma más fácil posible. No necesitan conocer en absoluto el sistema y tampoco tener conocimientos avanzados de informática para poder interaccionar con Bitcoin.

Las famosas Wallets o Monederos son un ejemplo de ello. Las Wallets, cuyo termino se ha usado en los apartados anteriores como sinónimo del término: cuenta o dirección de cuenta, es una herramienta muy útil para los usuarios promedio.

Una Wallet, es una herramienta software o hardware diseña para almacenar y gestionar las claves públicas y privadas de Bitcoin. Con ellas, los usuarios no tiene que preocuparse de saber qué es y cómo se usa la criptografía asimétrica. Con ellas, los usuarios realizarán sus transacciones con la única preocupación de indicar a quién se quiere realizar la transferencia y en qué cantidad, y la Wallet se encargará de firmar la transacción y enviarla al sistema.

Obviamente, son una herramienta auxiliar a Bitcoin. Si el usuario saber manejar Bitcoin no es obligatorio que acuda a ellas para poder operar, podrá custodiar el mismo sus propias claves y operar de forma directa con Bitcoin.
Otro ejemplo de estas tecnologías son los Exchangers o Casas de Cambio. Que son precisamente eso, una casa de cambio en donde poder realizar intercambios de Bitcoins a dinero FIAT y viceversa.

Son muy útiles para permitir a nuevos usuarios acceder al sistema Bitcoin y disponer de fondos con los que operar. Se habla incluso de que si no hubiese sido por ellos, no hubiese sido posible dinamizar la vida económica y financiera de Bitcoin hasta tal punto.

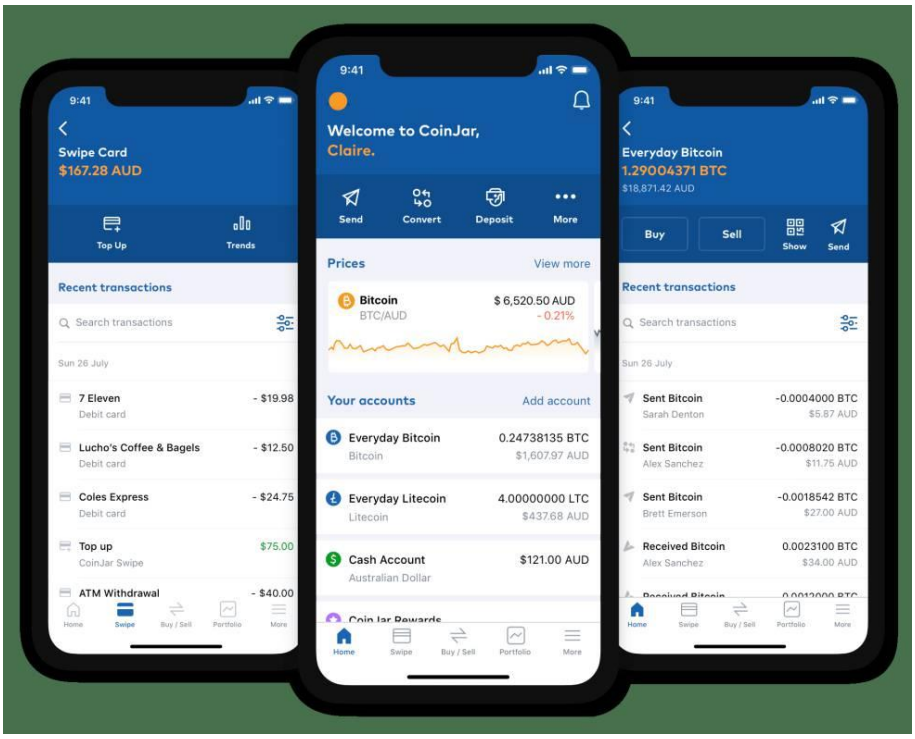

Ilustración 31: Aplicaciones de Wallets y Exchangers en Bitcoin
Fuente: Internet

De la mano de estos, surgen los también conocidos Cajeros de Bitcoins. Que son los hermanos de los Exchangers pero en el mundo físico.
Y es que, aunque no se haya mencionado, los Exchangers son espacios virtuales, en donde se realizan intercambios entre FIAT digital y Bitcoin.
Mientras que los Cajeros, dan la posibilidad de hacer exactamente lo mismo, pero con el FIAT físico.

Ilustración 32: Cajeros en Bitcoin
Fuente: Internet

Seguridad
Aunque el sistema de Bitcoin es completamente seguro (entre comillas como sabemos) no dejan de salir noticias sobre robos de Bitcoins. ¿Cómo es esto posible?

Y es que hay que diferenciar entre la seguridad del núcleo del sistema y la seguridad del sistema en general.

La propiedad de los fondos de cada cuenta Bitcoin se demuestra con la posesión de la clave privada asociada a la dirección de cartera que almacene dichos Bitcoins. Por lo que si un usuario, pierde la clave privada pierde la posesión de los Bitcoins.

En esto se basan los robos. Hay multitud de usuarios que no custodian bien sus claves y dejan una puerta abierta a cualquier atacante para que se las robe. Y con ellas, los Bitcoins que posea.

Cabe destacar, que la mayoría de robos que han tenido lugar, vienen de la mano de la falta de seguridad de los sistemas de Monederos y Exchangers, en los que miles de usuarios confían para custodiar sus claves de Bitcoin.

Ilustración 33: Robos de Bitcoins (parte 1 de 2)
Fuente: Internet

Ilustración 34: Robos de Bitcoins (parte 2 de 2)
Fuente: Internet

Pools de minería

De nuevo, el notable crecimiento de la popularidad de Bitcoin, ha hecho que no solo se vayan uniendo más y más usuarios, sino que, cada vez haya más mineros en el sistema, y cada vez con más potencia de calculo.

Por lo que actualmente es casi imposible minar un bloque de datos si se trabaja de forma aislada. Situación que se revierte si se trabaja de forma conjunta, uniendo fuerzas entre varios mineros. Estos, tendrán más posibilidades de minar un bloque de datos y reclamar la recompensa asociada.

Y precisamente eso son los Pools de minería. Son agrupaciones de mineros que cooperan con el objetivo de incrementar sus posibilidades en la tarea de minar un bloque de datos. Cada usuario que lo componga aportará toda la potencia de calculo de la que disponga. Y en el momento en el que se consiga minar un bloque de datos, se repartirá de forma equitativa la recompensa generada.

Aunque no es todo tan bonito. La agrupación en Pools de mineros está provocando un proceso de centralización de la potencia de cálculo general de toda la red.

En la actualidad, los cinco principales Pools de minería reúnen más del 50% de poder de computación de toda la red.

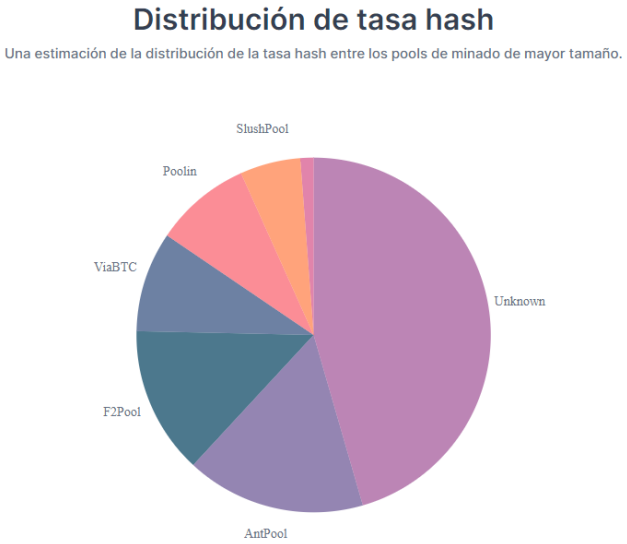

Ilustración 35: Poder de cálculo estimado de cada uno de los Pools de Minería
Fuente: https://www.blockchain.com/es/charts

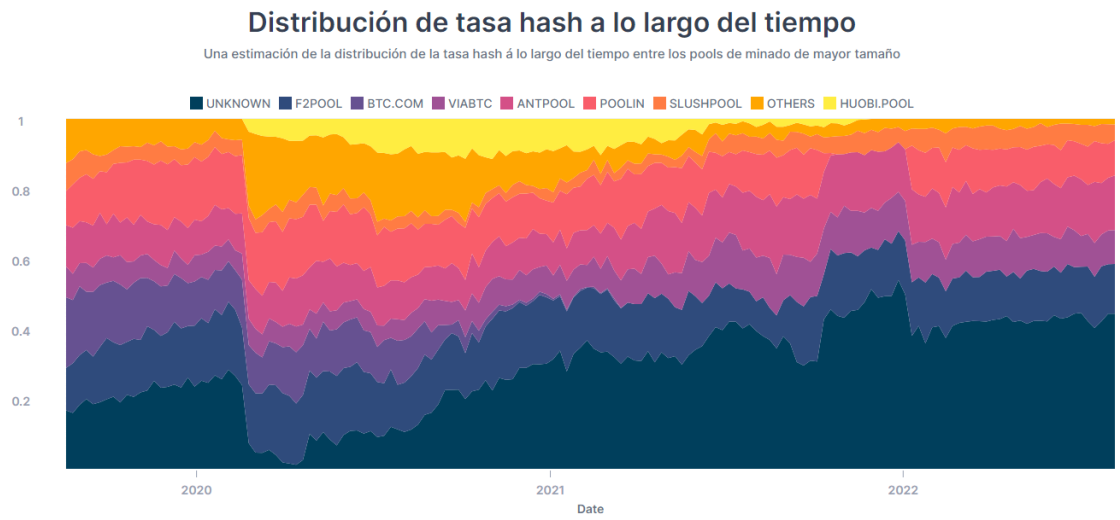

Ilustración 36: Poder de cálculo estimado de cada uno de los Pools de Minería a lo largo del tiempo
Fuente: https://www.blockchain.com/es/charts

Esto nos está llevando a un mercado oligopolista, en el que si no estás dentro de un Pool de mineros no podrás competir para generar bloques de datos.

Y peor aún, nos está acercando cada día más a la inestabilidad de la seguridad del sistema. Como se mencionaba en la disección anterior, más usuarios se están uniendo a los Pools de minería por miedo a no poder sacar rentabilidad. Lo que está haciendo que poco a poco, pero peligrosamente, los Pools vayan reuniendo mayor potencia de calculo, acercándoles a que alguno de ellos logre reunir la mayoría de la potencia de calculo.

Huella de carbono

La Proof of Work asociada a la validación de cada uno de los bloques de transacciones, como sabemos, consume una cantidad ingente de recursos para que lleve asociado un gasto desincentivador para subir bloques corruptos a la red.

Esto favorece al sistema y a sus usuarios, y perjudica a los atacantes que pueda llegar a tener. Pero de forma indirecta, está perjudicando al medio ambiente.

Según un post de National Geographic, se estima que el consumo de energía necesaria para llevar a cabo de forma satisfactoria este proceso de validación alcance su pico para 2024, consumiendo alrededor de 297 teravatios por hora, y generando aproximadamente 130 millones de toneladas métricas de emisiones de carbono.

Esto sin tomar perspectiva no nos transmite nada. Pero esta cantidad de emisión de carbono supera la producción anual total de emisiones de gases de efecto invernadero de países de tamaño medio en Europa, como Italia o la República Checa.

CAPITULO 3

Legado de Bitcoin

En este tercer capítulo veremos que Bitcoin no solo trajo un sistema de pagos e intercambios descentralizado altamente seguro, sino la tecnología necesaria para crear cualquier tipo de espacio descentralizado altamente seguro.

Así pues, analizaremos como reutilizar esta tecnología para implantarla en nuestros proyectos.

Y una vez asentada esta información, en definitiva, obtendremos una visión general de que aportaciones a la sociedad ha generado esta nueva tecnología y los proyectos que la han implementado.

Para lo cual, entraremos a analizar algunos de dichos proyectos. Como por ejemplo, el proyecto Ethereum y el proyecto Web3.0, muy importantes en la actualidad y que han traído consigo innumerables innovaciones tecnológicas y sociales.

1. Introducción

El lanzamiento del sistema Bitcoin, además de cambiar de forma radical la manera de ver los sistema de pago e intercambio, trajo consigo varias de las innovaciones tecnológicas y sociales más importantes de nuestra era.

Y es que se llevaba años esperando un sistema de consenso descentralizado altamente seguro para el desarrollo de diferentes conceptos y proyectos.

Uno de ellos, obviamente, era el desarrollo de una moneda digital descentralizada. Lográndose directamente con el lanzamiento de dicho tecnología, pero que ya desde los años 80 se llevaba intentando.
Como pincelada de historia, mencionar que, se realizaron múltiples intentos, pero todos ellos fallaron. Quizás, el que más cerca se quedó de conseguirlo fue el proyecto b-money, lanzado en 1988. Pero que al igual que sus hermanos, acabó quedose por debajo del ideal al depender en exceso de un intermediario centralizado y delegar la computación de confianza en un Back End.

Así pues, después del 2009, una vez desarrollado el sistema de consenso descentralizado, todos estos conceptos y proyectos comenzaron a tomar forma rápidamente.

De entre los que podemos destacar el concepto de desarrollar un sistema de registros de propiedad descentralizado, por el largo recorrido que llevaba detrás al igual que el concepto de una moneda descentralizada.
Ya en 1988, de la mano de Nick Szabo se publicó un articulo al respecto, denominado: “Títulos de propiedad seguros con autoridad de propietario”, en el que se hablaba de como poder implementar un registro de quien es propietario de que terreno, incluyendo conceptos tales como la propiedad familiar, la posesión adversa y el impuesto sobre la tierra.

Ahora, la cuestión está en cómo todos estos conceptos y proyectos, como los ya descritos, pueden usar esta tecnología de consenso descentralizado.

Bien, hay dos formas. La primera de ellas, es usar el sistema de consenso de Bitcoin tal cual, es decir, su Blockchain; superponiendo la nueva tecnología a desarrollar. Y la segunda, es desarrollar un sistema de consenso independiente, es decir, desarrollar e iniciar otra Blockchain que sirva como base del proyecto.

Obviamente, ambas opciones tienen sus ventajes e inconvenientes.

Construir sobre Bitcoin, supone que hay que seguir las reglas que rigen el funcionamiento de su Blockchain, lo que limita en exceso la elaboración de nuevos proyectos. Pero a cambio, el proyecto parte de una cadena de bloques completamente funcional y altamente segura.
Y desarrollar una Blockchain independiente, como si fuera el inverso de lo anterior, supone partir de una cadena de bloques que se adapte perfectamente a las necesidades del proyecto. Pero a cambio, habrá que llevar a cabo un desarrollo bastante exigente de la nueva cadena de bloques, y no tendremos la seguridad de que acabe resultando plenamente funcional y segura.

2. Criptomonedas

Aunque el concepto de desarrollar una moneda digital descentralizada ya se lograse con el proyecto Bitcoin, no significa que no pueda haber otros proyectos independientes que le hagan competencia. Es, ha sido y será siempre así; cualquier producto o servicio que salga al mercado o aparezca en la sociedad esta sujeto a que puedan salir competidores.
Y así ha sucedido. Numerosos proyectos han ido saliendo paulatinamente al mercado, cada uno con sus características, operaciones y propósitos específicos, pero todos ellos representando el mismo concepto de monedas digitales descentralizadas.

A estos nuevos productos, es decir, a las monedas digitales descentralizadas, se les conoce comúnmente como criptomonedas. Y actualmente hay multitud de ellas en el mercado.

Ilustración 37: Resumen de algunas criptomonedas en el mercado
Fuente: Internet

Muchas de ellas, y haciendo mención al apartado anterior, se han construido sobre el sistema Bitcoin y su sistema de consenso, otras, han desarrollado su propia Blockchain, y otras, siguiendo el concepto de las primeras, se han desarrollado sobre las Blockchains de otras criptomonedas.

Stablecoins
Uno de los muchos subconceptos de criptomonedas que podemos destacar, por ser quizás el más disruptivo y diferente con el funcionamiento tradicional, es el conocido como Stablecoins. Pudiéndose resumir como: una criptomoneda creada con la finalidad de que su valor permanezca estable (que no invariable) en el tiempo. Evitando así la gran variabilidad en el precio de mercado que sufren todas las criptomonedas. Como pudimos observar por su parte en el tema de Bitcoin, en el punto de valor, viendo su precio en Dólares a lo largo del tiempo.

Para mantener la estabilidad de su valor, las Stablecoins, necesitan un backup de respaldo. Que normalmente se hace con otros activos financieros, como: monedas

FIAT, materias primas como el oro, la plata, el diamante o el petróleo; u otros criptoactivos.

La más común es la primera de las opción, mantener la estabilidad mediante monedas fiduciarias. Respaldando cada una de las monedas de la Stablecoin con una moneda de la moneda FIAT elegida, que suele ser el dólar. Así pues, se mantiene una relación de monedas 1:1. 1 Stablecoin, vale 1$.

Cabe destacar que, las dos primeras opciones tienen la ventaja de garantizar una mayor estabilidad en el precio de la criptomoneda. Pero a cambio, incorpora un gran inconveniente, que es depender de un ente centralizado de emisión.
En cambio, la tercera opción, que si mantiene el concepto fundamental de las criptomonedas de mantenerse descentralizadas, tiene el inconveniente de estar a expensas de como se comporta el criptoactivo de backup, ya que una gran variación del mismo puede repercutir negativamente en el valor de la Stablecoin.

3. Ethereum

El proyecto Ethereum, ha marcado otro de los grandes hitos de esta era. Gracias al sistema de consenso descentralizado que trajo consigo Bitcoin, los desarrolladores de Ethereum fueron capaces de traer al mundo un nuevo concepto en el que se modificaba por completo el paradigma de la programación. Fueron capaces de desarrollar un sistema de aplicaciones descentralizadas (DApps).

El proyecto Ethereum fue fundado e iniciado por Vitalik Buterin en 2014.

Motivado por la falta de flexibilidad de Bitcoin, Vitalik Buterin decidió embarcarse en este proyecto desarrollando una Blockchain alternativa. Cuya diferencia principal con la Blockchain de Bitcoin erradicaba en permitir que los nodos de esta nueva red fuesen capaces de procesar lógica.

Pero como esto realmente es difícil de entender, vamos a hacer una pausa, vamos a abstraernos y en vez de ver todo de golpe, vamos a ir descubriendo poco a poco como funciona el sistema de Ethereum.

Sistema Ethereum - Visión general
El sistema de Ethereum, al igual que Bitcoin, mantiene en funcionamiento su propia criptomoneda, conocida como Ether.

Esta, de igual manera que Bitcoin, permite que se lleven a cambo múltiples procesos de pagos e intercambios. Y siguiendo la misma filosofía que su antecesor, se mantiene gracias a un registro ordenado de transacciones fraccionado en bloques de datos, cuyo sistema de consenso, sigue basándose en un proceso de minado de datos por parte de sus usuarios.

Ahora, el Ether, no es, ni pretende ser, un sistema de pagos e intercambios. El objetivo del Ether es servir como ficha de intercambio para los Contratos Inteligentes.

Los contratos inteligentes, o del inglés, Smart Contracts, son básicamente programas ejecutables que viven en la red de Ethereum. Y que como programas que son, no son más que un conjunto de líneas de código (funciones) y datos (estado).

Así pues, en la red de Ethereum conviven dos conceptos por igual, las monedas digitales y los programas ejecutables. Y por tanto, ambos son serializados en la Blockchain de Ethereum y mantenidos por sus usuarios.

Y las transacciones son las encargadas de que todo esto sea posible. En Ethereum existen tres tipos de transacciones.

- Transacciones regulares.
- Transacciones de despliegue de contratos.
- Transacciones de ejecución de contratos.

Las transacciones regulares, son las encargadas de que se pueda llevar a cabo el traspaso de Ethers entre usuarios. Funcionando exactamente de la misma manera que en Bitcoin.
Las transacciones de despliegue de contratos, permiten a un usuario enviar al sistema un programa ejecutable y con ello serializarlo.
Estas transacciones tienen un campo especial, en el que el usuario podrá incrustar todo el código y los datos del programa desarrollado.
Y las transacciones de ejecución de contratos, permiten a los usuarios ejecutar cada uno de los Contratos inteligentes de la red, ya hayan sido desarrollados por ellos mismo o por otros usuarios.

Como información extra, de igual manera que en Bitcoin, estas transacciones tienen asociadas una pequeña comisión para recompensar a los mineros. Pero aquí, estas transacciones son obligatorias. Se les conoce como Gas, y va en función del tamaño que ocupen y el número de operaciones que se deban realizar con cada una.

Es decir y poniendo en contexto, cuando un usuario cree una transacción regular, además de traspasar los Ethers pertinentes, debe asociar una comisión en Gas que cubra los gastos de memoria y la única operación que tiene asociada (almacenarla en un bloque de datos).
De igual manera pasa con las transacciones de despliegue de contratos. Salvo por la diferencia de que por lo general los contratos ocupan bastante más memoria que una transacción simple y el usuario deberá pagar una comisión más alta.
Y las transacciones de ejecución de contratos, y aquí la importancia real de las comisiones, deberán incorporar el Gas necesario para que el minero ejecute todas y cada una de las operaciones contenidas en el contrato.

Para finalizar, podemos resumir todo lo comentado en este punto en lo siguiente:

Los usuarios podrán realizar traspasos de Ethers mediante las transacciones regulares. Estas, llegaran a los mineros, que se encargarán de serializarlas en un bloque de datos, con lo que indirectamente se hace posible que pueda existir y funcionar este concepto de criptomonedas.

De igual manera, los usuarios podrán crear sus programas y subirlos mediante las transacciones de despliegue de contratos. Estas, llegarán a los mineros, encargándose de serializarlas en un bloque de datos, con lo que de nuevo, indirectamente se hace posible que pueda existir y funcionar este concepto de contratos inteligentes.
Y para finalizar, los usuarios podrán ejecutar estos contratos, mediante las transacciones de ejecución de contratos, que llegarán a los mineros, per esta vez, se encargan de ejecutar el programa, de ahí lo mencionado anteriormente sobre que la red Ethereum permite a sus nodos procesar lógica; y serializan el nuevo estado del contrato y con ello el de la red, en un bloque de datos.

Sistema Ethereum - EVM

La EVM, Ethereum Virtual Machine, o del español, Máquina Virtual de Ethereum, es el nombre que se le da al concepto abstracto de tener una máquina de Turing en Ethereum.

Esta máquina de Turing será la encargada de almacenar y de procesar toda lógica que se de en la red, con el objetivo de que se pueda hacer realidad este concepto de una programación descentralizada mediante aplicaciones descentralizadas (DApps).

La EVM, como concepto abstracto que es, se apoya en la capa real de usuarios. Es decir, la EVM almacenará sus programas, datos y estado en la Blockchain (memoria de todos aquellos usuarios que tengan un cliente Ethereum abierto) y ejecutará las instrucciones de sus programas, modificando datos y estado, en el proceso de minado de los bloques de datos (potencia de calculo de las máquinas de aquellos usuarios que ejecuten un cliente de minado de Ethereum).

Así pues, el compendio de las máquina de los usuarios de Ethereum forman en conjunto la máquina de Turing de Ethereum.

Cabe destacar, que esta máquina de Turing, es Turing completa, esto es, que puede codificar cualquier cómputo que se pueda llevar a cabo, incluyendo bucles infinitos.

En cuanto al código, los Contratos Inteligentes funcionan sobre un lenguaje de bajo nivel bytecode basado en pila, conocido como Código de Máquina Virtual de Ethereum, o Código de la EVM.

En la siguiente dirección oficial de Ethereum, se puede ver alguno de los códigos EVM más importantes: https://ethereum.org/es/developers/docs/evm/opcodes/

Pero este Código EVM no es el que usan los programadores para llevar la programación del día a día de los Contratos Inteligentes. Han surgido una serie de lenguajes de programación de alto nivel, como por ejemplo Solidity o Vyper y de nivel intermedio como Yul y Yul+, que ayudan a llevar a cabo dicha labor.

Por ejemplo, en el siguiente modelo, podemos ver el código en Vyper necesario para implementar un sistema de subastas mediante Contrato Inteligente:

```
# Subastas Abiertas

# Params de subastas
# Beneficiario recibe dinero de la oferta más alta
beneficiary: public(address)
auctionStart: public(uint256)
auctionEnd: public(uint256)

# Estado actual de subasta
highestBidder: public(address)
highestBid: public(uint256)

# Establecer a verdadero al final, deshabilita cualquier cambio
ended: public(bool)

# Mantener un seguimiento de las ofertas reembolsadas para que podamos
seguir el patrón de retirada
pendingReturns: public(HashMap[address, uint256])

# Crea una subasta simple con `_bidding_time`
# segundos de tiempo de oferta en nombre de la
# dirección beneficiaria `_beneficiary`.

@external
def __init__(_beneficiary: address, _bidding_time: uint256):
    self.beneficiary = _beneficiary
    self.auctionStart = block.timestamp
    self.auctionEnd = self.auctionStart + _bidding_time

# El valor solo será reembolsado si la subasta
# no es ganada.
@external
@payable
def bid():
    # Comprobar si el periodo de oferta ha terminado.
    assert block.timestamp < self.auctionEnd
    # Comprobar si la oferta es suficientemente alta
    assert msg.value > self.highestBid
    # Registrar el reembolso de la oferta alta anterior
    self.pendingReturns[self.highestBidder] += self.highestBid
    # Seguimiento de la nueva oferta alta.
```

```
        self.highestBidder = msg.sender
        self.highestBid = msg.value

    # Retira una oferta previamente reembolsada. El patrón de retirada se
    # utiliza aquí para evitar un problema de seguridad. Si los reembolsos
    fueron directamente
    # enviados como parte de la oferta(), un contrato de licitación
    malicioso podría bloquear
    # esos reembolsos y así bloquear la entrada de nuevas ofertas más
    altas.
    @external
    def withdraw():
        pending_amount: uint256 = self.pendingReturns[msg.sender]
        self.pendingReturns[msg.sender] = 0
        send(msg.sender, pending_amount)

    # Finalizar la subasta y enviar la oferta más alta
    # al beneficiario.
    @external
    def endAuction():
        # Es una buena guía para las funciones de estructura que
    interactúan con
        # con otros contratos (es decir, llaman funciones o envían Ether)
        # en tres fases:
        # 1. condiciones de comprobación
        # 2. realizar acciones (condiciones potencialmente cambiantes)
        # 3. interactuando con otros contratos
        # Si estas fases se mezclan, el otro contrato podría llamar a
        # de vuelta al contrato actual y modificar el estado o causar
        # efectos (pago ether) a ser realizados varias veces.
        # Si las funciones llamadas internamente incluyen interacción con
    contratos externos
        #, también deben considerarse interacción con
        # contratos externos.

        # 1. Condiciones
        # Comprueba si se ha alcanzado el fin de la subasta
        assert block.timestamp >= self.auctionEnd
        # Comprueba si esta función ya ha sido llamada
        assert not self.ended

        # 2. Efectos
        self.ended = True

        # 3. Interacción
        send(self.beneficiary, self.highestBid)
```

Ilustración 38: Ejemplo de código de un Contrato Inteligente. Uso del lenguaje Vyper
Fuente: https://ethereum.org/es/

ERCs

Los ERCs, Ethereum Request for Comments, son documentos técnicos que permiten implantar estándares de programación. Con el objetivo, de que todos aquellos programadores y desarrolladores que se lancen a crear en Ethereum mediante los Contratos Inteligentes, sigan una serie de referentes, criterios y normas que permitan mejorar sus proyectos… y más importante aún, sigan un esquema base para que no tengan que reinventar la rueda.

Es decir, si ya hay algo inventado, estos ERCs lo recogerán y facilitarán a los desarrolladores implementar su propia versión de dicho concepto o proyecto.

De todos los estándares que hay, destacan dos por encima del resto, el ERC-20 y el ERC-721.

El estándar ERC-20 permite crear tokens dentro de la cadena Ethereum mediante el uso de Smart Conctracts. Estos tokens, se pueden entender como fichas, a las cuales se les puede asociar una funcionalidad en concreto o pueden ser usadas para canjear una funcionalidad en concreto.

Completemos esta definición tan abstracta con algunos ejemplos de tokens ERC-20. De entre los que podemos destacar los conceptos y proyectos siguientes:

- Security Tokens
- Governance Tokens
- Utility Tokens
- Transactional Tokens
- Platform Tokens

Los Security Tokens funcionan como valores financieros, estando actualmente muy vinculados con los valores tradicionales, como las acciones, bonos o activos físicos.
Es decir, sirven para otorgar al titular del token algún tipo de participación en un negocio o bien. Y suelen percibirse como un medio de inversión, en el que hay expectativas de obtener algún beneficio económico.
Estos tokens son los responsables de las tan hablas Finanzas descentralizadas (DeFi). Que no son más que eso, una forma experimental de finanzas descentralizadas, en las que no son necesarios intermediarios financieros centrales, como los bancos para ofrecer instrumentos financieros tradicionales.

Los Governance Tokens por su parte otorgan una mejor gestión de la toma de decisiones. Permitiendo a las personas interesadas en determinados proyectos o entornos la posibilidad de colaborar, debatir y votar.
Es decir, otorgan voz al propietario del token dentro de un determinado proyecto o empresa.
Y son los responsables de que se puedan descentralizar los proyectos e incluso las empresas. Y las famosas Organizaciones Autónomas Descentralizadas (DAO) o Empresas Autónomas Descentralizadas (DAC) son dirigidas mediante estos tokens.

Los Utility Tokens otorgan derecho de acceso y uso a un producto o servicio. Es decir, solo las personas que dispongan de dicho toquen, por el que han tenido que pagar previamente, podrán disfrutar de los beneficios de una serie de recursos de un ecosistema en especifico.

Actualmente, están muy vinculados a las ICO, Ofertan Iniciales de Monedas, o del inglés Initial Coin Offering. Estas ICO, consisten en lanzar una oferta de tokens limitados, con el objetivo de que el desarrollador de la propuesta obtenga la financiación necesaria para desarrollar su proyecto. Y en el futuro, una vez que se haya llevado a cabo dicho proyecto, todas las personas que dispongan de estos tokens podrán acceder al producto o servicio desarrollado.
Aunque hay que destacar que las ICOs no están solo restringidas a proyectos de futura creación, se pueden lanzar ICOs disponiendo ya del producto o servicio y emitir el token para ampliar el abanico de inversores y levantar un mayor capital.

Los Trasactional Tokens, funcionan como medio de cambio. Como si fuesen criptomonedas realmente, salvo por la diferencia de que se establecen a pequeña escala. Normalmente se usan para implementar un pequeño sistema de intercambio dentro de una plataforma o aplicación en especifico. Por ejemplo como moneda de cambio dentro de un videojuego, con la que se puedan comprar los diferentes items.

Y los Platform Tokens, se utilizan para construir y apoyar sistemas concretos. Son tokens que tienen utilidades muy concretas dentro de plataformas y aplicaciones concretas, como por ejemplo establecer un sistema de identidad o reputación.
Se podría decir incluso que los Transactional Tokens son un caso de uso de los Platform Tokens, pero debido a su concreta funcionalidad se habla de tokens diferentes.

Por su parte el estandar ERC-721, es un protocolo que permite desarrollar tokens, igual que el ERC-20, pero con una característica muy interesante, y es la no fungibilidad.

Los tokens generados con el ERC-20 son fungibles, es decir, que da igual que token tengas, que va a representar siempre lo mismo, por ejemplo, si se lanzan acciones de una empresa mediante tokens, el token que pueda tener el usuario A y el usuario B van a valer y representar lo mismo, es decir, la misma acción; incluso en caso de se los cambien entre ellos, seguirían teniendo la misma cantidad de acciones, y estás seguirán valiendo lo mismo.

Nada cambia por tener un token u otro, lo importante es tener un token.

Pero con los tokens ERC-721 no da igual tener un token, importa que token tengas. Cada token ERC-721 es único, completamente exclusivo e insustituible. Y en función de eso valdrá y servirá para una cosa u otra.

Estos tokens han servido para explotar el mundo del arte, de los coleccionables y de los videojuegos. En el que cada articulo es intrínsecamente único.

Y tanto es así, que con los tokens ERC-721 se han lanzado al mercado multitud de colecciones exclusivas, como por ejemplo la famosa colección de Mutant Ape Yacht Club, en el que cada avatar es un mono personalizado y único que sirve para identificar a cada usuarios y representan una obra de arte en si.

Ilustración 39: Algunos tokens de la colección Mutant Ape Yacht Club
Fuente: Internet

Estos tokens ERC-721 se conocen comúnmente como NFTs, Tokens No Fungibles, o del inglés, Non Fungible tokens. Haciendo referencia a su propiedad de la no fungibilidad, que les hace tan interesantes e importantes.

Para finalizar, otra de las características particulares de los NFTs es que estos no pueden dividirse. En contraposición con los tokens ERC-20 que si pueden fraccionarse. Y realmente es lógico, el NFT es algo único, debe permanecer siempre completo, no hay cabida a que exista subdivisión alguna.

Además, tampoco podrán consumirse al usarse, venderse o comprase, como si pasa con algunos ERC-20, ya que volvemos a las mismas, al se únicos, no se pueden reemplazar, por lo que si al realizar alguna transacción o uso con el mismo, se consume, desaparece el NFT para siempre.

ERC721

Obviamente, y como se mencionaba, estos dos estándares no son los único en el mercado, pero sí los más importantes y los que realmente han sentado las bases del fenómeno token que tanto se habla en la actualidad.

Tanto es así, que múltiples estándares son simples revisiones y correcciones de ambos, como por ejemplo los estándares ERC-223, ERC-777 y ERC-621, que mejoran la usabilidad del ERC-20.

Otros por ejemplo, como el ERC-1155, que aunque siga siendo una mejora de los estándares ERC-20 y ERC-721; incorpora funcionalidades bastante interesantes. Como es el caso, el ERC-1155 admite en un mismo contrato tokens fungibles y no fungibles. Muy útil para los videojuegos play-to-earn, en los que se usan simultáneamente y en gran cantidad ambos estándares, el ERC-20 y el ERC-721.

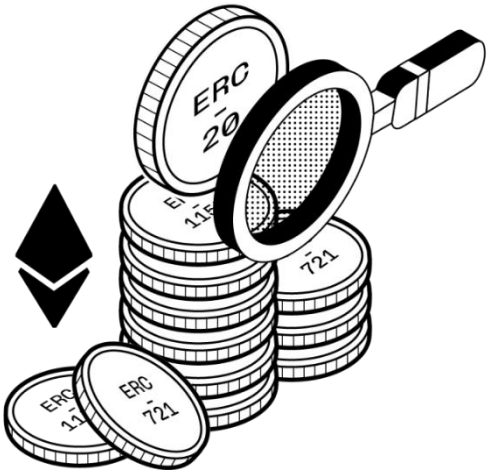

Ilustración 40: Resumen estándares ERCs
Fuente: Internet

4. WEB 3.0

Otro de los conceptos en los que se puede aplicar esta tecnología de consenso descentralizado que trajo Bitcoin, es en construir un Internet descentralizado, erigido y operado por sus usuarios. En el que las grandes empresas tecnológicas queden fuera del tablero del juego, y la propiedad de todo lo que tenga que ver referente a los usuarios, sea en definitiva de los usuarios.

Internet en la actualidad

Internet se ha convertido en el centro neurálgico de nuestras operaciones diarias, incluso, de nuestra vida e identidad. Si necesitamos buscar trabajo, llevar a cabo las entrevistas pertinentes e incluso desarrollar las diferentes actividades asociadas al puesto; se hace por Internet. Si queremos acceder a los fondos o a los ahorros almacenados en nuestras cuentas bancarias, se hace por Internet. Incluso, y cada vez más, si queremos comprar cualquier producto o servicios, se hace por Internet.

Igual pasa con cualquier trámite burocrático o con cualquier interacción que se tenga con las empresas, estos se llevan a cabo mediante Internet. Y más aún, las interacciones sociales, las comunicaciones y muchas actividades de ocio; se hacen por Internet. Por ejemplo, si queremos consumir cualquier tipo de contenido, como un libro, un podcast o un vídeo, se consumen por Internet.

Y es que son innumerables las ventajas que trae consigo Internet. Tenemos una mayor rapidez en las comunicación, una mayor y mejor iteración con diferentes grupos de interés, unos mejores y más simplificados procesos, acceso a múltiples contenidos e incontables beneficios más.

Pero hay un problema, todos estos contenidos e iteraciones se encuentran controlados por las grandes empresas tecnológicas. Porque aunque Internet sea el medio, no deja de ser en cierta medida un concepto abstracto, sobre el que hay que construir para que todo esto sea posible y funcione.

Y esto es lo que han hecho las empresas. Las empresas son las que han construido Internet, y por tanto son las que tienen el control absoluto sobre todo el tráfico que allí se genere.

Nosotros, los usuarios, simplemente navegamos por lo que las grandes empresas quieren que naveguemos.

Son las que tienen el control absoluto sobre los contenidos que consumimos. Y aunque permitan que los mismos usuarios creen y compartan libremente los contenidos que deseen, esto no es así. Cualquier contenido que no sea de su agrado podrá ser censurado, modificado, bloqueado o eliminado. Incluso los mismos usuarios podrán sufrir las mismas consecuencias. Lo usuarios que no sean del agrado de las empresas podrán quedarse fuera de sus plataformas, privándoles del derecho a comunicarse y ser comunicados. Y aún hay más, los productos y servicios que se oferten, estarán de igual manera controlados por ellas. No se podrá construir y comercializar nada que no pase antes por sus filtros. Sino, simplemente será ocultado.

Esto, nos está llevando cada vez más y más a una dinámica de desequilibrio de poder entre las plataformas y los usuarios.

Y precisamente este dilema es el que pretende solucionar un Internet descentralizado.
Un internet que se acercaría más al Internet libre con el que se pensó cuando se desarrolló que al Internet abusivo y centralizado que se acabó convirtiendo.
Sería el “protocolo abierto y descentralizado para permitir compartir información desde cualquier lugar de la Tierra” [42] con el que el señor Tim Berners-Lee sonó.

Web3.0

La Web3.0, sobrenombre que se le da a este nuevo concepto del Internet, pretende crear de nuevo Internet, usando para ello toda la tecnología desarrollada sobre Blockchain, para que todo lo que se construya y se comparta en él sea descentralizado, es decir, hecho por lo usuarios para y por los usuarios. Y obviamente propiedad de los usuarios.

Se podrían crear multitud de plataformas, aplicaciones o herramientas siguiendo un modelo de Organización Autónoma Descentralizada (DAO) en el que los mismos usuarios fuesen los encargados de dictaminar las reglas de su funcionamiento.
Se podrían seguir estos modelos de DAOs y Blockchain para compartir innumerables contenidos, productos o servicios sin tener el miedo constante a ser censurado o eliminado y teniendo la certeza de que nuestro contenido será siempre nuestro.
Se podrían comprar y adquirir estos contenidos y recursos también sin el miedo a ser bloqueado. Y en los casos en los que fuese necesario realizar una transacción monetaria para conseguirlos, se podrían recurrir a las criptomonedas, que dejarían fuera a los bancos y sus políticas abusivas.
Y siguiendo esto último, el de dejar fuera a los bancos y su política centralizada, se podrían usar las DeFi y los tokens para distribuir innumerables activos financieros, en el que el control y la propiedad de los mismos fuera única y exclusivamente de los usuarios. Aunque esto de los tokens no solo serviría para los activos financieros, sino para cualquier recurso del mundo real. Actualmente se ha puesto muy de moda la palabra tokenizar. Y no es más que la práctica de convertir a un token criptográfico todo recurso del mundo real, sobre todo si es digital, para que quede serializado en la Blockchain y refleje para siempre la titularidad del propietario correspondiente.

Y todo ello sin necesidad de ceder de forma voluntaria o involuntaria a las plataformas intermediarias nuestro historial de navegación. Este, sería solo nuestro y nosotros seriamos los encargados de cederlo o no.

Se podrían poner mil ejemplos para poder hacernos una idea de como funcionarían todos estos conceptos llevados a la realidad. Pero por amplitud del tema, solo vamos a ver uno, aunque con él es más que suficiente para captar la esencia de la Web3.0.

En la industria Gamer, millones de usuarios compran diariamente items para sus videojuegos, ya sea simplemente para personalizar la apariencia o para obtener alguna funcionalidad en especifico. Pero tienen el inconveniente de que nunca pasan a ser propiedad del jugador. Ósea, el jugador, le comprará el ítem a la desarrolladora del videojuego, pudiendo usarse en el juego desde ese mismo momento. Pero nunca podrá salir de ahí. En cuanto el cliente deje de jugar y abandone el juego, todos sus ítems se quedarán ahí para siempre. Por lo que la empresa se habrá llevado el dinero y el cliente habrá perdido todos sus activos.
Con la industria Web3, esto no pasa. Todos los ítems serán tokens, tanto fungibles como no fungibles, y la propiedad será únicamente del usuario. Pudiendo dicho jugador venderlo cuando quiera y como quiera. Así pues, cuando decida abandonar el videojuego, podrá vender todos los ítems asociados y recuperar algo de dinero.

Web1.0 y Web2.0
El término Web3.0, tiene una curiosa historia detrás.

Internet nace en 1969, o, en 1990, según como quiera verse, ya que en 1969, el protocolo de Internet se hace público, y, en 1990, se crea el primer navegador web. Y desde entonces, independiente de cual de las dos fechas de referencia se quiera coger para empezar a contar, ha estado en continua evolución, sufriendo numerosos cambios, incluso en su paradigma de funcionamiento.

Desde 1990 hasta más o menos 2004, Internet estaba constituido principalmente por sitios web estáticos, en el que algunas empresas decidían compartir algunos contenidos e información. Pero con los cuales no se podía interaccionar.
Y aunque el protocolo estaba abierto a ello, los usuarios rara vez compartían el suyo propio.

A esta etapa, se le considera como la primera versión de Internet, ahora conocida como Web1.0. En el que Internet estaba visto como un sitio de solo lectura.

Ilustración 41: Resumen Web1.0
Fuente: https://ethereum.org/es/web3/

Pero desde más o menos el 2004 empezaron a aparecer y a popularizarse las plataformas de redes sociales, en las que los usuarios podían crear y compartir su propio contenido. Esto supuso un impulso enorme para Internet, ya que más y más usuarios fueron interesándose y uniéndose a la red. Convirtiéndose en la red masificada de plataformas, páginas web y contenidos que conocemos hoy en día, con todos los problema descritos en la parte primera de este mismo apartado.
Pero en definitiva, este cambio de paradigma, supuso la segunda versión de Internet, conocida como Web2.0. En el que Internet está visto como un sitio de lectura y escritura.

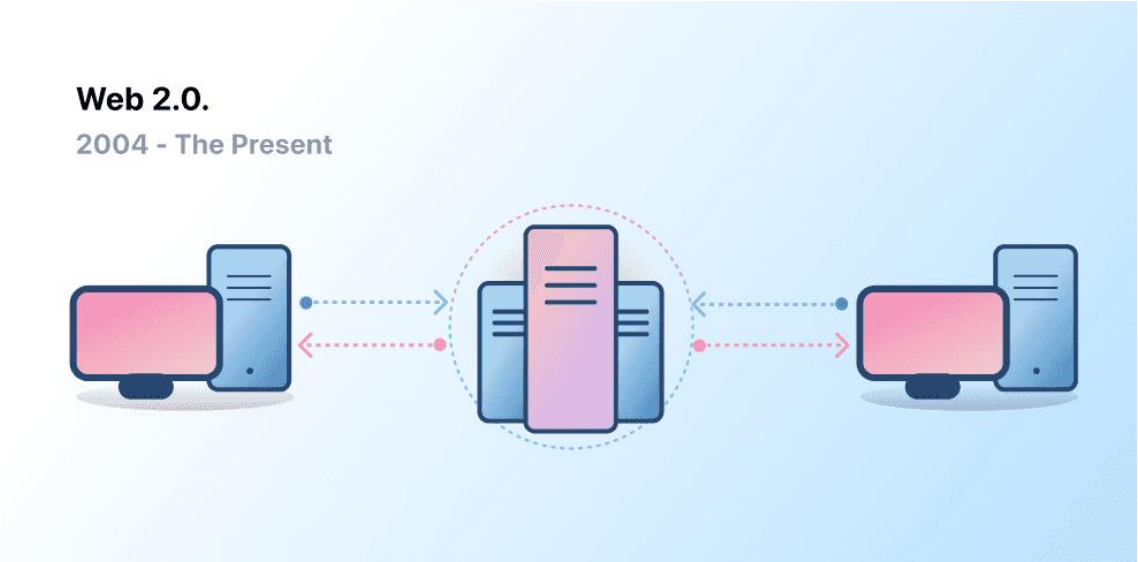

Ilustración 42: Resumen Web2.0
Fuente: https://ethereum.org/es/web3/

Y ahora, la Web3.0 pretende cambiar de nuevo el paradigma de Internet, mediante un Internet descentralizado, en el que los contenidos y el control sean devueltos a los usuarios. Siendo un sitio de lectura, escritura y propiedad.

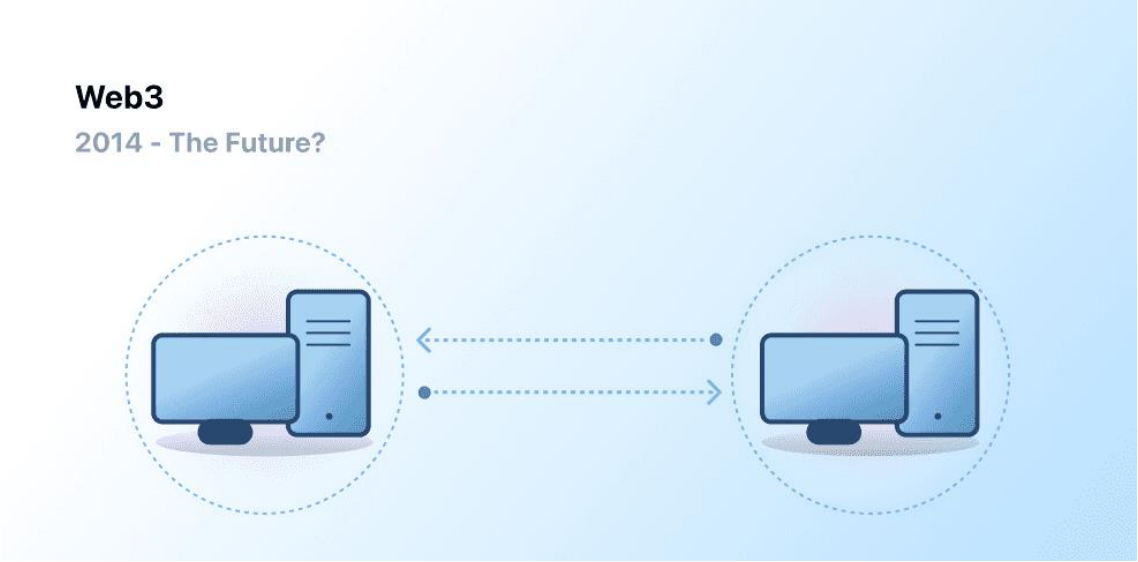

Ilustración 43: Resumen Web3.0
Fuente: https://ethereum.org/es/web3/

CAPITULO 4

Algoritmos de minado. Caso de uso: Ravencoin

En este cuarto capítulo veremos que son los ASICs y como influyen en el desarrollo normal de las redes Blockchains. Veremos, que estos son los causantes, en gran medida, de que haya multitud de algoritmos diferentes para resolver las Proof of Works, y que además, estos últimos, estén continuamente actualizándose y modificándose.

Cuando tengamos todos estos conceptos teóricos asimilados, culminaremos el tema con un análisis de la red Ravencoin, para ver claramente como los ASIC perpetúan la red y como la red se defiende con modificaciones y cambios en el algoritmo hash de minado criptográfico.

1. Introducción

En el Capitulo 2 Sistema Bitcoin, vimos que para garantizar la seguridad y el correcto funcionamiento de la Blockchain de Bitcoin se hizo necesario implementar una Proof-of-work. Esta, no consistía en otra cosa que en generar Hashes como identificadores de bloque siguiendo un algoritmo hash de minado criptográfico, concretamente el algoritmo SHA-256, para luego validarlos en función del número de ceros con los que comenzase y si cumplía dicha condición, darlos como válidos (pudiendo entonces subir a la red el bloque de transacciones).

En el Capitulo 3 Legado de Bitcoin, vimos, que esta tecnología de consenso descentralizado que acabamos de describir se trasladó rápidamente a otros proyectos y surgieron multitud de Blockchains alternativas siguiendo exactamente el mismo modelo que Bitcoin.

Ahora, la pregunta está en por qué cada una de estas Blockchains tiene un algoritmo hash de minado criptográfico diferente y no usan el SHA-256 de Bitcoin. Por poner en contexto, podemos encontramos que la red Ethereum usa el algoritmo Ethash, la red Litecoin usa Scrypt y la red de Dash usa el algoritmo X11. Todos ellos diferentes, pero todos ellos con el mismo objetivo.
Podríamos pensar que es porque estos algoritmos se adaptan mejor a los nuevos requisitos y funcionalidades de cada una de estas Blockchains. Pero no es así, el único objetivo detrás de ello es evitar la centralización de la minería, desarrollando algoritmos más seguros y más accesibles para todos los usuarios. Veamos todo esto más de cerca.

ASICs
La forma de minar bloques de datos en las diferentes Blockchains ha ido cambiando con el tiempo. Se empezó resolviendo las Proof-of-works con la potencia de calculo que aportaban las CPUs, pero a medida que aumentaba el valor de las criptomonedas, se fue convirtiendo en ventajoso realizar este proceso mediante procesamiento paralelo, es decir, mediante GPUs; para aumentar la potencia de calculo aportada y con ella las posibilidades de minar un bloque de datos y recibir la recompensa.
Pero como el valor económico de las criptomonedas siguió aumentando aún más, se acabó convirtiendo en económicamente viable la opción de usar FPGAs o Field Programable Gate Array. Que no son más que circuitos integrados totalmente personalizables y configurables que permiten sacar mayor rendimiento que las CPUs y GPUs al poder configurarlos específicamente para realizar esta tarea de minado.
Pero de nuevo, esta opción acabó quedándose corta con el incansable aumento del valor de las criptomonedas. Y acabó pareciendo razonable la opción de crear chips específicos para cumplir con las especificaciones necesarias para poder llevar a cabo este proceso de minado. Estos chips reciben el nombre de ASICs o Application Specific Integrated Circuit. Y gracias a su alta eficiencia en el proceso de minado dominaron rápidamente a todas las tecnologías competidoras anteriormente descritas.

Así pues, como resumen de toda esta cronología de tecnologías empleadas para minar bloques de datos podemos quedarnos con la siguiente conclusión: los ASICs hacen que no sea practico llevar a cabo el proceso de minado con otra tecnología.

Ilustración 44: Hardware ASIC
Fuente: Internet

Ahora, el acceso de un ASIC no es barato ni eficiente en cuanto al gasto de electricidad se trata (aunque cada vez están sacando ASICs más eficientes en ese sentido). Por lo que no todo el mundo puede optar ni quiere optar a estos dispositivos para minar. Así pues, esto se traduce a que aquellos que si que dispongan de estos ASIC puedan llegar a controlar con facilidad una mayor potencia de calculo en la red y por ende validen una mayor cantidad de bloques.
En principio, esto no es malo, ni mucho menos tiene un objetivo malicioso. Pero como sabemos, aunque la tecnología no sea mala por naturaleza, el ser humano puede hacer maldades con ella. Y tener dispositivos que permiten con gran facilidad a pequeños grupos superponerse al resto de usuarios de la red no es la más adecuado si se quiere mantener el principio descentralizad. Por lo que los desarrolladores y usuarios de las diferentes Blockchain suelen lanzar medidas al respecto.

Antes de describir algunas de las practicas que se llevan a cabo para desincentivar el uso de ASICs, primero hay que entender como operan realmente los ASICs, para después entender como luchar contra ellos.

Un ASIC es un circuito construido específicamente para llevar a cabo una única tarea, en contraposición a las CPUs y GPUs, que son de propósito general. ¿Esto qué representa? Representa las dos siguientes premisas:

1 Los ASICs pueden llevar a cabo una tarea de forma totalmente eficiente y eficaz, pero no pueden llevar a cabo ninguna otra tarea que no sea exactamente esa; mientras que las CPUs y GPUs pueden llevar a cabo multitud de tareas, pero con una eficacia y eficiencia estándar.
2 Los ASICs hay que crearlos específicamente para cada una de las tareas que se pretendan llevar a cabo con ellos; mientras que las CPUs y GPUs pueden ejecutar cualquier tarea que se proponga de manera inmediata.

Así pues, la manera de luchar contra ellos, teniendo en cuenta las dos premisas anteriores, se puede resumir en lo siguiente:

1 Modificar la forma en la que se lleva a cabo el proceso de minado, para que así, el ASIC se quede obsoleto y no pueda llevar a cabo dicha tarea.
2 Añadir multitud de tareas variadas al proceso de minado para que el ASIC acabe pareciéndose a un dispositivo de propósito general como CPUs y GPUs y por tanto resulte totalmente contraproducente generar estos ASICs por el precio que supone en contraposición a una GPU.

Así pues, por la solución número uno, no es raro ver que hay multitud de algoritmos hash de minado criptográfico en el mercado. Continuamente están saliendo nuevos algoritmos, nuevas versiones, modificaciones y demás practicas, con el objetivo de dejar a los ASICs obsoletos y sacarlos del mercado. Pero esto no significa ni mucho menos que sea lo que suceda, solo podemos suponer y esperar que los ASICs se reprogramen o salgan otros nuevos para poder seguir explotando estos nuevos algoritmos, y mientras eso suceda, los usuarios de CPUs y GPUs tengan unos meses de alivio.
Básicamente es una carrera interminable entre los desarrolladores de las Blockchains y los desarrolladores de los ASICs por ver quien puede mantener el control de la red.
Y precisamente por esto, es por lo que como comentábamos en la introducción de este apartado, que prácticamente cada Blockchain tiene un algoritmo de minado diferente.

Por la solución número dos, tampoco es raro ver que estos nuevos algoritmos, versiones y modificaciones son cada vez más complejos e innovadores.
Actualmente por poner en contesto hay dos prácticas muy interesantes que se llevan a cabo y funcionan relativamente bien contra los ASICs.
La primera de ellas usa un enfoque que consiste en implementar un proceso de minado que use una secuencia de algoritmos hash encadenados. En donde se implementen varias funciones hash, en vez de una sola, y en la que la salida de cada una de ellas sea la entrada de otra. Esto aumenta enormemente la complejidad para crear un ASIC debido a que tiene que superar la generación de múltiples funciones hash diferentes.
El otro enfoque consiste en implementar un proceso de minado con un uso de memoria intensiva. Los ASICs no tiene una forma plenamente eficiente del uso de la memoria como por ejemplo las GPUs, tienen que recurrir a dispositivos RAM, por lo que crear algoritmo variantes y flexibles, en vez de usar funciones fijas, que obliguen a usar memoria, perjudica notablemente la eficiencia de los ASICs

Variantes a la Proof-of-Work
No es el principal objetivo de este capitulo, pero también se puede luchar contra los ASICs mediante un cambio en el protocolo de consenso descentralizado.
O dicho de otra manera, el sistema de consenso descentralizado Proof-of-work, se sustenta en un sistema de minería por potencia de calculo aportada, como bien sabemos. Pues si cambiamos de paradigma, y hacemos que no sea necesario ejecutar procesamiento computacional para añadir bloques de transacciones, los ASICs no tendrán cabida en ninguna variable de la ecuación.

Para entender mejor como se puede llegar a variar el sistema de consenso de Proof-of-work propuesto por Satoshi Nakamoto en Bitcoin, debemos abstraernos en la idea que presenta.

Básicamente el sistema de consenso descentralizado de Proof-of-work se sustenta en que:

1 El usuario que desee añadir bloques en la Blockchain debe aportar por adelantado un stake (una participación) que suponga algún tipo de valor para él, y que lo disuada de actuar de forma deshonesta por miedo a perderlo.
2 El usuario, se tomará esta molestia de poner en juego sus recursos, para recibir una recompensa.
3 Y por completar la definición, cuanto mayor sea el stake aportado por el usuario, mayor serán las probabilidades de poder añadir bloques en la red.

Este stake, en la Proof-of-work, consiste en aportar potencia de calculo mediante un gasto en hardware y electricidad. Pero puede ser cualquier cosa, como por ejemplo, activos, dinero, criptomonedas o reputación. En definitiva, cualquier cosa que el usuario no quiera perder. Y cuanto más se aporte del mismo, cuanto más ponga en juego, más probabilidad hay de que el sistema confíe en él y le permita validar bloques de datos.

Así pues, han salido multitud de protocolos de consenso descentralizado alternativos a la Proof-of-work desde su nacimiento es 2008 con Bitcoin. Entre los que podemos destacar los siguientes:

- Proof of Stake (PoS)
- Proof of Authority (PoA)
- Proof of Burn (PoB)
- Delegated Proof of Stake (DPoS)
- Leased Proof of Stake (LPoS)
- Proof of Time (PoT)
- Proof of History (PoH)

E incluso híbridos entre la Proof of Work y algunas de las descritas, como:

- Proof of Work y Proof of Stake (PoW / PoS)

Estas variantes del sistema de consenso descentralizado, obviamente no tienen el único objetivo de dejar fuera del tablero de juego a los ASICs, sino que tienen como objetivo suplir algunas de las limitaciones de la Proof of Work, como: la escalabilidad, la eficiencia, el consumo de energía (huella de carbono) o la misma descentralización.

Quizás las Proof of Stake es la alternativa más popular a la Proof of Work de las descritas. Está ya implantada en varias Blockchains como Binace Coin, Solana o Cardano. E incluso, algunas Blockchains que funcionan con PoW pretenden cambiarse a Proof-of-stake, como por ejemplo Ethereum, mediante Ethereum2.0.

Así pues, sería interesante entrar a analizar en detalle la Proof-of-stake por ser la más importante, y con dos objetivos en mente: ver con ella como es posible este cambio de paradigma y ver como con este cambio de paradigma se pueda dejar fuera a los ASICs.

En la Proof of Stake, los participantes aportan como stake cierta cantidad de monedas nativas de la Blockchain en la que se está llevando el proceso de minado, por ejemplo, si estuviéramos en Ethereum, los usuarios deberán aportar Ethers. Estas monedas

quedarán bloqueadas en la cuenta del usuario y en función de dicha cantidad monedas, el participante tendrá más poder de validación o menos. Es decir el tamaño del stake del participante determinará la probabilidad que tendrá este de ser elegido como validador del siguiente bloque de transacciones.

El proceso de selección se lleva a cabo por el propio sistema y aunque cada Blockchain es libre de implementarlo como quiera, lo normal es llevarlo a cabo mediante una combinación entre los dos siguientes métodos: Randomized Block Selection (selección aleatoria de bloques) y Coin Age Selection (selección de monedas por antigüedad).
El método de Randomized Block Selection seleccionará al validador en función de una combinación del valor del Hash identificador de bloque más bajo generado y el stake aportado más alto.
Y el método Coin Age Selection seleccionará al validador en función de cuanto tiempo llevan sus monedas en stake, es decir, cuantos días llevan las monedas en staking.
Eso sí, cuando un validador haya forjado (sustituto al término minado) un bloque, la edad de su stake se pondrá a cero; para evitar que los validadores con grandes stakes dominen indiscutiblemente la Blockchain.

Ahora, todo esto funciona, porque las criptomonedas tienen un valor, y el usuario no querrá perderlas por llevar a cabo practicas poco honorables. Ya que si sube un bloque corrupto o invalido, el sistema eliminará parte de su stake de criptomonedas o incluso el stake completo.
Hasta ahora, todo exactamente igual que la Proof-of-work, si sube un bloque corrupto, se invalida y pierde todo el gasto en electricidad que ha puesto para poder subirlo. Pero la Proof-of-Stake tiene una diferencia muy importante con la Proof-of-work. En la PoW, el usuario puede realizar ataques a la red sin tener consecuencias más allá de las ya descritas en este mismo párrafo, y en cualquier momento y sobre todo en caso de que la situación se ponga fea y el valor de la criptomoneda baje, puede marcharse sin perder más inversión en hardware y electricidad; pudiendo vender las instalaciones, el hardware o emplearlos para minar en otras Blockchains. Pero en la PoS, toda la inversión está en las criptomonedas de su stake, si la Blockchain se vuelve poco segura, el precio bajará y perderá literalmente todo (aunque si es cierto que puede cancelar el stake cuando quiera, pero con una penalización de tiempo, que será suficiente para que si el valor baja, pierda toda la inversión). Es por eso, que la variante de Proof of Stake tiene un factor de seguridad extra al ya conocido de la Proof-of-work, que incentiva a todos los mineros a mantener la red segura y descentralizada.

El enfoque del sistema de consenso de Proof of Stake tiene como principal ventaja con respecto a la Proof of Work la eficiencia energética, ya que no es necesario tal gasto ingente de electricidad para crear un stake desincentivador de practicas deshonestas.
Pero también se puede destacar la seguridad, por este doble factor desincentivador que hemos mencionado en el párrafo anterior. La descentralización, ya que al nos ser necesario tener acceso a grandes equipos de minado (como sucede con los ASICs) para poder minar, sino tan solo una pocas monedas relativamente fáciles de conseguir, incentiva a que más usuarios se anime a validar bloques, lo que se traduce directamente en una mayor descentralización. Y la escalabilidad, ya que al no ser necesario tal complejidad a la hora de validad bloques, estos, pueden validarse sustancialmente más rápido.

Ahora, el principal inconveniente de la Proof of Stake, es que al usarse las propias monedas como sistema de validación, la economía de la Blockchain se estanca.

Básicamente, en los sistemas con Proof of Work, como la inversión está fuera del sistema, los mineros, cuando logren obtener las recompensas, intentarán venderlas rápidamente para conseguir dinero real y mejorar sus sistemas de minado. Pero aquí, sus sistema de minado son las propias monedas, y por tanto, las mantendrán bloqueadas en el stake y no circularán entre los usuarios y por tanto no movilizando su valor y economía.

2. Ravencoin

Para ver un poco más de cerca todo esto todo esto de los ASICs y de los cambios de algoritmo, vamos a analizar en detenimiento la cronología de un proyecto Blockchain en concreto, conocido como Ravencoin. Ya que a lo largo del tiempo ha ido pasando por varios cambios de algoritmo. Concretamente, ha tenido 3 algoritmos de minado criptográfico diferentes, empezó con el algoritmo X16R, el cual se modifico y pasó a convertirse en el algoritmo X16Rv2, para acabar finalmente sustentándose sobre el algoritmo de minado criptográfico KawPow.

Forks

Antes de pasar a describir que es Ravencoin y como funciona, tenemos que ver un concepto muy importante: los Forks o bifurcaciones. Ya que podría decirse que sobre ellos se sustenta el proyecto Ravencoin.

El término bifurcación, ya nos es familiar del Capitulo 2 Sistema Bitcoin. Allí vimos que una bifurcación se produce cuando se separa la unicidad del registro Blockchain debido que en el lapso de tiempo que se tarda en transmitir la noticia de que se a conseguido minar un bloque de datos, y con ella, el propio bloque de datos; otro usuario al que no le ha llegado dicha noticia y ha conseguido resolver su Proof-of-work ha empezado a compartir su propio bloque de transacciones, por lo que se produce un conflicto y una división de la cadena en dos versiones diferentes. Los usuarios que tienen y han aceptado el primero de los bloques, y los usuarios que tienen y han aceptado el segundo de los bloques que se han transmitido.
A este tipo de bifurcación se le conoce como Blockchain Fork. Y auto converge sola con la regla de la Cadena Lineal más Larga.
Pero hay otros tipos de bifurcaciones: las Hard Forks, las Soft Forks y las Codebase Forks.

Una nota importante antes de analizar en detenimiento cada uno de los tipos de bifurcaciones: La única bifurcación que sucede de forma inesperada es la Blockchain Fork. La Hard Fork, la Soft Fork y la Codebase Fork son lanzadas deliberadamente por los usuarios.

Empecemos por las Soft Forks. Una bifurcación suave (en español), es un tipo de actualización del protocolo de la Blockchain sobre la que se aplica, en la que se refuerzan o modifican reglas de funcionamiento.
Es decir, es simple y llanamente una pequeña actualización del protocolo de actuación de la Blockchain, que lanzan los desarrolladores o los mismos usuarios, y, que con ella

se pretende corregir pequeños errores o vulnerabilidades. Y que aunque se pueda añadir pequeñas nuevas funcionalidades, rara vez se producen.

Ahora, ¿por qué una actualización del sistema debería producir una división? Simple, el principio fundamental de las Blockchains es la descentralización. Y por tanto, todos los usuarios tienen el mismo poder de decisión y actuación. Cuando se lanza una actualización, no se obliga a los usuarios a aceptarla, se deja a decisión de cada uno. Por lo que si no todos lo usuarios la aceptan, habrá dos versiones de la Blockchain, una versión con las reglas y funcionamiento antiguo, y otra, con las nuevas reglas. De ahí el nombre de Fork o bifurcación que se le da a estas actualizaciones.

Lo normal es que las Soft Forks sean aceptadas por la mayoría de los mineros y no acaben en una bifurcación de la cadena. Ya que realmente no se cambia ninguna característica importante y ni si quiera su funcionamiento. Por lo que a priori no debería de haber ningún inconveniente en actualizar. Pero la opción de que aquello suceda siempre estará presente.

Cabe destacar que, estas Soft Forks tienen la ventaja de que como son una actualización, los nodos actualizados pueden validar bloques de datos siguiendo o el viejo modelo o el muevo modelo. Y por tanto, al trabajar bien con las reglas antiguas, tienen más fácil crear la cadena de bloques más larga. Un gran incentivo para que la mayor parte del poder hash acabe concentrándose en esta nueva rama, e indirectamente este mayor poder de hash acabe garantizando una convergencia final del historial de transacciones.

Ilustración 45: Resumen de una Soft Fork
Fuente: https://www.criptonoticias.com/criptopedia/que-es-bifurcacion-fork-soft-hard-blockchain/

Ahora, las Hard Forks o bifurcaciones duras por su parte, son un tipo de actualización en la que se añaden o eliminan reglas del funcionamiento en el protocolo de actuación de la Blockchain en la que se aplica.
Es decir, aunque sigan siendo una actualización del sistema al igual que las Soft Forks, estas son más un cambio de versión que de actualización propiamente dicho.

Y por tanto, ahora sí, esto hace que haya un cambio importante en las características y funcionamiento de la Blockchain. Las dos ramas que se generen no pueden ni podrán ser nunca compatibles. Ya que no comparten las mismas reglas.
Así pues, cuando se lanza una Hard Fork en el sistema, se divide para siempre la cadena de bloques.
Si todos los usuarios aceptan la actualización y se cambian al nuevo protocolo, la rama del protocolo antiguo desaparecerá y todo convergerá a la nueva. Sino, como hemos dicho, habrá para siempre dos versiones de la Blockchain.

Aunque lo normal es que no suelan converger. Habrá una división de opiniones por parte de los usuarios debido al tan alto grado de cambio en el funcionamiento de la cadena. Unos preferirán las características originales y otros preferirán apostar por el progreso y las actualizaciones.

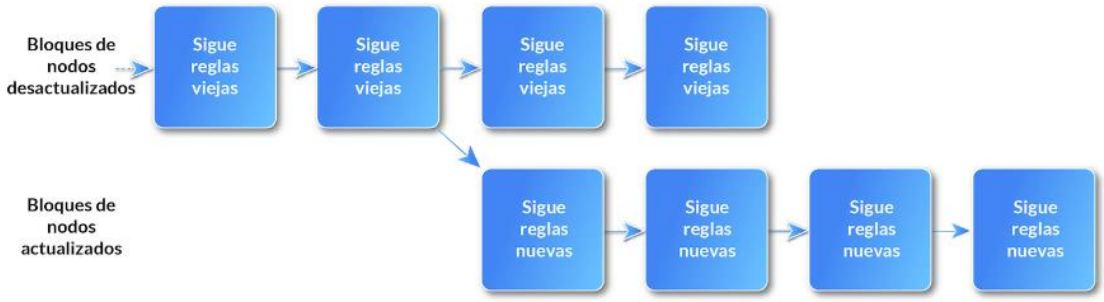

Ilustración 46: Resumen de una Hard Fork
Fuente: https://www.criptonoticias.com/criptopedia/que-es-bifurcacion-fork-soft-hard-blockchain/

Para poner un poco en contexto, estas Hard Forks, suelen utilizarse para cambiar partes importantes del funcionamiento del protocolo de una Blockchain. Como por ejemplo, para cambiar el tipo de Proof-of-work o el algoritmo de minado hash criptográfico. Cambios que como acabamos de mencionar, muchas veces no son bienvenidos y se acaba bifurcando la cadena de bloques en dos versiones completamente válidas pero complementarias.
Poniendo un caso de ejemplo de esto último, podemos encontrarnos con la criptomoneda Monero, lanzada al mundo en abril de 2014. Monero, más o menos por abril de 2018 sufrió un Hard Fork que básicamente daba paso a la versión 12 del protocolo. Pero muchos usuarios decidieron mantenerse en la versión 11 del protocolo de Monero, y acabó dando lugar a diferentes proyectos: Monero Classic (XMC), Monero 0 (XMZ) y Monero Original (XMO), todos ellos bifurcaciones de la cadena original.

Para finalizar con este análisis de los Forks, tenemos que mencionar a las Codebase Forks. Este tipo de bifurcaciones no tienen tanto que ver con el término propio de una bifurcación en una cadena de bloques como con el término Fork en el desarrollo de Software. Un Fork de un proyecto Software, a grosso modo se podría decir que es la creación de un nuevo proyecto partiendo como base de todo lo desarrollado en un proyecto ya existente, con el objetivo de modificarlo para adaptarse a unas funcionalidades totalmente complementarias a las principalmente planteadas en el proyecto original.
Es una practica muy común en proyectos de código abierto o software libre. Ya que en definitiva ese es uno de los objetivos principales de los proyectos de código abierto: “el libre acceso, modificación y distribución de los proyectos informáticos”. Y pasa con multitud de criptomonedas y Blockchains. Por ejemplo es el caso del proyecto Ravencoin.

Ravencoin
Como acabamos de comentar, el proyecto Ravencoin surge como una bifurcación de código o Codebase Fork, de concretamente, el sistema Bitcoin. Cuyo objetivo se basa en mejorar y desarrollar un sistema completamente enfocado y eficiente en la creación, uso y traspaso de activos.

No entraremos en mucho detalle, pero el sistema Bitcoin permite implementar una política de activos. Al igual que Ethereum. Obviamente el soporte que ofrece Ethereum es bastante más flexible que el que ofrece Bitcoin. Pero aún así, los dos, siguen siendo toscos. Estos sistemas, no están pensados para trabajar de forma nativa con los activos, simplemente se construyen encima. Por lo que los desarrolladores y usuarios están continuamente luchando contra los problemas derivados de estas prácticas.

Ravencoin sin embargo se ha diseñado precisamente para eso, se ha diseñado con el único objetivo de facilitar la creación, seguimiento y traspasado de estos activos. Evitando que se pierdan, se destruyan o simplemente no se pueda hacer un correcto tratamiento de los mismos.
Poniendo en contexto, por ejemplo, en Bitcoin, cuando se genera un activo, a grosso modo, este se asocia a una UTXO, es decir, la UTXO es el activo, y por tanto, si al realizar una transferencia monetaria, se llega a usar esta UTXO sin querer, el activo desaparece para siempre del control del usuario y no se puede recuperar.

Estos activos de los que estamos hablando son tokens, tanto fungibles como no fungibles, que los usuarios pueden emitir sin la necesidad de extraerlos. Es decir, los usuarios del protocolo Ravencoin podrán crear fácilmente estos activos, decidir su propósito, sus reglas, su nombre o su denominación.
Y estos se ajustarán para cualquier cosa que la imaginación del creador pueda conjurar. Pueden representar activos físicos o digitales, como por ejemplo: barras de oro, monedas, obras de arte, escrituras o créditos; partes de proyectos, como por ejemplo: acciones de una empresa o proyecto, valores, participaciones o artículos de financiación colectiva; o bienes virtuales, como por ejemplo: boletos, entradas y tickets de eventos, licencias o monedas y artículos de plataformas.
Realmente son bastante parecidos a los tokens ERC-20 y ERC-721 que vimos en el Capitulo 2 Legado de Bitcoin con el sistema Ethereum, salvo por que estos, como hemos dicho, son nativos de la red.

Entrando en algunas características menos importantes, pero de igual manera interesantes, Ravencoin lanzó los binarios del código el 3 de enero de 2018. Fueron lanzados sin ICOs, sin minado previo y mediante una distribución justa en la que todos los tokens fuesen para aquellos que los consiguiesen (es decir, sin reparto de tokens entre, usuarios, mineros, desarrolladores, propietarios o inversores).
Su Blockchain aguanta un suministro total de monedas de 21 mil millones, y un tiempo de minado de 1 minuto, lo que logra un rendimiento de aproximadamente 116TPS (Transacciones por segundo). Este suministro de monedas Ravencoin (RVN) tiene la misma función que el Ether en Ethereum, es decir, suplir la generación de tokens, concretamente en 500 RVN por activo generado; y para recompensar a los mineros que soportan toda la potencia de calculo necesaria para mantener la red.
Implementa una Proof-of-work al igual que Bitcoin, pero en vez de usar el algoritmo hash de minado SHA-256, Ravencoin despega con un nuevo algoritmo de minería conocido como X16R, “destinado a evitar el dominio inmediato de los grupos de minería y el dominio futuro de los equipos de minería ASIC” [45], situación que actualmente no sucede con el algoritmo SHA-256 de Bitcoin.

Para finalizar, otras características muy interesantes de este proyecto son que Ravencoin pretende implementar, por así decirlo, servicios complementarios a su Blockchain. Concretamente plantea introducir un sistema de recompensas automatizado, un sistema de mensajería y un sistema de votación.

El sistema de recompensas está basado en la idea de poder tener un mecanismo que permita emitir pagos en RVN a todos aquellos usuarios que tengan determinados tokens en su posesión a modo de recompensas. Como por ejemplo, para todos aquellos que sean propietarios de tokens de acciones, participaciones, bonos o cualquier otro tipo similar de activos.
En el propio Whitepaper de Ravencoin, se muestra un ejemplo práctico, en el que se ve perfectamente la idea que se persigue con la implementación de todo este sistema. Y es el siguiente:

Un niño pequeño, de un país que lo permita, decide crear un puesto de limonada ambulante. Pero como no tiene dinero suficiente para llevarlo acabo, decide crear una ficha en Ravencoin que represente a dicho negocio y le permita recaudar financiación. Supongamos que acaba lanzando 10.000 fichas de LEMONADE, a un precio de 0.01$, lo que le permite recaudar AUD$ para construir su negocio. Estos tokens podrán ser vendidos y transferidos por sus propietarios. Hasta el punto que el niño decida recompensar a las personas que creyeron en su proyecto, ya que le está yendo especialmente bien porque el vecindario se está volcando e invirtiendo en este proyecto empresarial. En ese momento, podrá fácilmente emitir con este sistema de recompensas un pago en RVN a todos aquellos propietarios de los tokens LEMONADE en la cantidad de RVN que decida el niño emisor de estos tokens.

El sistema de mensajería persigue una idea similar a la expuesta con el sistema de recompensas. Pretende construir un mecanismo que permita enviar mensajes de texto a todos aquellos usuarios que tengan determinados tokens.
Por ejemplo, y volviendo al caso de uso del puesto de limonada, el niño, puede querer comunicarse con todos aquellos inversores que le han apoyado para darles las gracias en vez de emitir recompensas reales para ello. O puede querer comunicarse con ellos con antelación para transmitirles los planes de distribución de recompensas que pretende implementar a lo largo del tiempo. O simplemente para comunicarles como le va el negocio y en que y como está distribuyendo la riqueza.

Ahora, este enfoque tiene un problema. Y es que no siempre todos los propietarios de un token quieren ser notificados e identificados. Así pues, el sistema debe permitir que el titular del token se excluya en cualquier momento. Además de asegurar que solo determinadas partes usen el canal de mensajes para que no sea un conducto de spam. O dicho de otro modo, asegurar que solo el niño que ha creado los tokens de LEMONADE pueda comunicarse con los titulares del token LEMONADE.
Para todo ello, Ravencoin, implementa un sistema de comunicación en el que en vez de enviar mensajes a los propietarios de los tokens originales, se envían mensajes a los propietarios de los tokens de comunicación auxiliares que se transfieren de forma complementaria con dichos tokens originales. Es decir, y volviendo al ejemplo, el niño tendrá tokens LEMONADE:Alert que distribuirá junto con los tokens LEMONADE. Si los usuarios quieren recibir información, mantendrán este último token, sino, simplemente tendrá que deshacerse de él. Y cuando el niño quiera enviar comunicados, los enviará por el canal del token LEMONADE:Alert en vez de por el canal LEMONADE.
Obviamente, y al igual que con el sistema de recompensas, solo el creador de estos tokens podrá enviar mensajes a los propietarios.
Y con todo esto, se habrá conseguido que solo el emisor de los tokens se comunique con los propietarios y que estos propietarios puedan decidir si quieren ser comunicados o no.

Finalmente, el sistema de voto, que sigue un poco la misma filosofía que los dos sistema anteriores, pretende construir una herramienta que permita a los usuarios de determinados tokens votar.
Se construye de la misma manera que el sistema de mensajería, cada emisor de tokens, deberá crear tokens auxiliares de voto y distribuirlos 1:1 a cada poseedor del token original. Y con ellos, los propietarios podrán enviar a través del protocolo y a las direcciones que contabilizan los votos su voto.

Algoritmo de minado X11

Antes de empezar a analizar en detenimiento y de forma técnica el algoritmo hash de minado criptográfico X16R de Ravencoin, vamos a abrir un pequeño paréntesis para estudiar el algoritmo X11, ya que, el X16R es un descendiente del mismo.

El X11 nació en marzo de 2014 de la mano de Evan Duffield para dar soporte a la criptomoneda Dash (inicialmente conocida como Darkcoin) y a su Blockchain. E intentar corregir la centralización de la minería que se estaba dando en Bitcoin con el algoritmo SHA-256 en aquel momento debido a los ASICs.

El X11 pertenece a la familia de algoritmos anti-ASICs que usan un enfoque de secuencia de algoritmos hash encadenados, como vimos en el apartado de introducción de este mismo capitulo.
Concretamente ejecuta 11 funciones Hash diferentes para generar cada uno de los identificadores Hash de los bloques. Usando para ello el modelo en cascada descrito, en el que la salida generada por cada una de las funciones Hash es la entrada de la siguiente. Así pues, el target del bloque entrará a la función X11, e irá pasando de función en función, hasta que se apliquen las 11 y salga como resultado un Hash identificador de bloque.

El X11 fue un algoritmo muy innovador, ya que hasta entonces, los algoritmos existentes, se basaban en usar solo una función Hash, como por ejemplo Bitcoin con el algoritmo SHA-256.
Básicamente, fue el predecesor de este tipo de algoritmos secuenciales.
Aunque, en el Whitepaper de Dash, en donde se describe este algoritmo de minado, los desarrolladores no lo definieron como un algoritmo fuertemente resistente a ASICs, sino más bien como un algoritmo que solo pretende frustrar temporalmente, pero lo más posible, el desarrollo de ASICs.

Las funciones que usa el algoritmo de minado X11 se pueden observar en la siguiente *ilustración:*

X11	X12	X13	X14	X15	X17
blake	blake	blake	blake	blake	blake
bmw	bmw	bmw	bmw	bmw	bmw
groestl	groestl	groestl	groestl	groestl	groestl
jh	jh	jh	jh	jh	jh
keccak	keccak	keccak	keccak	keccak	keccak
skein	skein	skein	skein	skein	skein
luffa	luffa	luffa	luffa	luffa	luffa
cubehash	cubehash	cubehash	cubehash	cubehash	cubehash
shavite	shavite	shavite	shavite	shavite	shavite
simd	simd	simd	simd	simd	simd
echo	echo	echo	echo	echo	echo
	ocean?	hamsi	hamsi	hamsi	hamsi
		fugue	fugue	fugue	fugue
			shabal	shabal	shabal
				whirlpool	whirlpool
					loselose
					djb2

Ilustración 47: Funciones Hash del algoritmo X11 y variantes
Fuente: https://getpimp.org/what-are-all-these-x11-x13-x15-algorithms-made-of/

Podemos atisbar en la *ilustración* que vienen descritos también los algoritmos X12, X13, X14, X15 y X17. Y es que, el concepto detrás del X11 se puede extender fácilmente a algoritmos adicionales, con simplemente añadir más funciones Hash a la secuencia de algoritmos.

El problema del X11 (y de sus variantes) es que, las funciones se ejecutan siempre en el mismo orden, y en el que se puede observar en la *ilustración* anterior. Esto facilita enormemente la generación de ASICs. Por lo que el enfoque del X11 funcionó solo durante un tiempo, ahora ya hay varios ASCIs X11 en el mercado.
Si que es cierto que ir encadenando más y mas funciones hash agrega dificultad en la construcción de ASICs, y por tanto, algunas de sus variantes siguen vigentes. Pero no dejan de estar sujetas a la misma problemática, y se prestan fácilmente a la construcción de ASICs. Y más teniendo en cuenta que la única diferencia entre un algoritmo y otro, es la adición extra al final del encadenamiento de funciones. Que hace que los fabricantes de ASICs solo necesiten extender el diseño de los ASICs existentes para acomodar las funciones Hash adicionales.

Para finalizar, y hacernos una idea del gran potencial que tenía el X11 contra los ASICs, aunque luego fracasará y acabaran saliendo hardware ASIC, las once funciones Hash que incluye fueron todas ellas finalistas o semifinalistas (incluida la ganadora) en el concurso que llevó a cabo el National Institute of Standards and Technology (NIST) de EE.UU para completar el desarrollo de la función SHA-3.
Para tomar contexto de la importancia y repercusión de estas funciones Hash, si recordamos del Capitulo 2 Sistema Bitcoin, el algoritmo SHA-256 de Bitcoin es una versión del SHA-2, y este, es una variante del SHA, creado por la Agencia de Seguridad Nacional de los Estados Unidos (NSA) en conjunto con el propio NIST en 1993. Entonces el SHA-3 sería el nuevo sustituto de la familia para completar las funciones SHA-1 y SHA-2. Lo que se traduce en que las funciones Hash presentadas pasaron por unos análisis bastante extensos y minuciosos, para estar a la altura de lo que se estaba creando.
La competencia pública de funciones Hash del NIST duró casi 5 años y se presentaron más de 50 participantes. Para más información al respecto de la clasificación de las funciones y de cuales eran estas, se puede consultar el siguiente enlace: https://en.wikipedia.org/wiki/NIST_hash_function_competition#Finalists
Aquí solo vamos a resumir la posición de las once que componen al algoritmos X11:

Ganadora	*Finalistas*	*Semifinalistas*
Keccak	BLAKE	BMW
	Grostl	CubeHash
	JH	ECHO
	Skein	Luffa
		SHAvite-3
		SIMD

Algoritmo de minado X16R
El algoritmo hash de minado criptográfico X16R que implementa Ravencoin tiene la intención de resolver la problemática de los algoritmos X11 y sus variantes, introduciendo un componente de aleatoriedad en el orden en el que se ejecutan las funciones Hash, y por tanto, rompiendo con la distribución constante en la que se llevaban a cabo.

El algoritmo X16R incorpora 16 funciones Hash, que son, concretamente, las funciones que componen al algoritmo X15 más las función SHA-512.
Para cumplir con el factor de aleatoriedad cada una de estas funciones Hash se asociará a un valor hexadecimal y según se corresponda con los valores de los últimos 8 Bytes (16 nibbles) del Hash del bloque anterior se ejecutará una u otra.
Veamos esto con un ejemplo, pero antes de ello, debemos tener clara la correspondencia de valores con las funciones Hash:

0=blake	8=shavite
1=bmw	9=simd
2=groestl	A=echo
3=jh	B=hamsi
4=keccak	C=fugue
5=skein	D=shabal
6=luffa	E=whirlpool
7=cubehash	F=sha512

Ilustración 48: Funciones Hash del algoritmo X16R y valor de ordenamiento de las mismas
Fuente: https://ravencoin.org/assets/documents/X16R-Whitepaper.pdf

Así pues, si tenemos el siguiente Hash como identificador del bloque anterior:

Previous Block Hash:
00000000000000007e8a29f052ac2870045ae3970270f9***7da00919b8e86287***

Ilustración 49: EjemploX16R_Hash del bloque anterior
Fuente: https://ravencoin.org/assets/documents/X16R-Whitepaper.pdf

Las funciones Hash que se ejecutarán y en el orden en el que lo harán serán las siguientes:

Each hex digit (nibble) determines which algorithm to use next.
cubehash -> shabal -> echo -> blake -> blake -> simd -> bmw -> simd -> hamsi ->
shavite -> whirlpool -> shavite -> luffa -> groestl -> shavite -> cubehash

Ilustración 50: EjemploX16R_Funciones Hash y el orden en el que se aplicarán
Fuente: https://ravencoin.org/assets/documents/X16R-Whitepaper.pdf

Este enfoque tiene unas características importantes de mencionar: No tiene necesariamente porque ejecutarse las 16 funciones Hash que componen al algoritmo, y, puede repetirse varias veces seguidas una misma función Hash.
Ambas características, por su parte, pueden verse en el ejemplo.

Para finalizar, el reordenamiento no hace que el X16R sea imposible de replicar con un ASIC, pero esta entrada adicional de aleatoriedad hace que los ASIC se adapten peor que las CPUs y GPUs. Además, de que evita que los ASIC puedan construirse como una pequeña extensión de los ASICs del X15. Y por tanto, asegura, al menos momentáneamente, la no existencia de ASICs en la red.

Hoja de ruta para el algoritmo de minado X16R
Como el algoritmo X16R no es infalible contra los ASICs, tener un plan de actuación contra ASIC es una medida preventiva muy interesante.
Ravencoin está muy centrado en ese aspecto en concreto, no quiere ningún grupo de minería ASIC en su red. Es por eso que desde aproximadamente su lanzamiento empezó a diseñar una ruta de actuación anti-ASIC, la cual iremos describiendo a lo largo de este punto. Empecemos.

La opción más intuitiva en caso de que se consigan pruebas de la existencia de ASICs en la red, es añadir una nueva función Hash al algoritmo. Esto dejaría momentáneamente obsoletos los posibles ASICs desarrollados para el X16R.

De forma más técnica, podemos decir que, se generaría el algoritmo X17R, que implementa la misma funcionalidad y funciones que el X16R, pero con 17 funciones en vez de con 16.

Ahora, ¿Qué función Hash se implementaría como esta diecisieteava función? Los desarrolladores de Ravencoin consideraron viable implementar una función ASIC-hard, o dicho de otra manera, fuertemente resistente a ASICs. Que no son más que funciones que implementan gran cantidad de tareas variadas que hacen que sea, aparte de difícil construir un ASIC, más rentable minar con GPUs e incluso CPUs que con ASICs.
Las más conocidas son: CNv4 (también conocida como CN-V9 o como CryptoNightR) actual algoritmo de la red Monero, RandomX principal sustituto para la red Monero o ProgPow principal sustituto en Ethereum.
Todas ellas son perfectas para resolver la problemática, pero decidieron que CNv4 sería la más interesantes entre las descritas ya que lleva implementada tiempo en la red Monero con unos resultados impresionantes.
El problema de esta solución es que el tiempo de ejecución de la función CNv4 es muy superior al tiempo de ejecución de las restantes dieciséis funciones Hash (hasta 100.000 veces más lento). Lo que provocaría un desequilibrio en el minado de los bloques, los mineros, incluidos los ASICs, podrían esperarse a minar aquellos bloques en los que no hiciese falta ejecutar el algoritmo CNv4 para generar el Hash como identificador de bloque.
Así pues, aunque sea una posible solución, no está ni mucho menos cerca de ser optima.

Como información adicional, los desarrolladores de Ravencoin midieron las velocidades relativas de las funciones Hash que implementa el X16R para asegurarse de que ninguna de ellas estuviese tan fuera de línea como para que tuviese sentido financiero esperar bloques que no incluyeran ciertos algoritmos, como si pasaría con el CNv4.
La siguiente *ilustración* muestra dicha tabla de velocidades relativas:

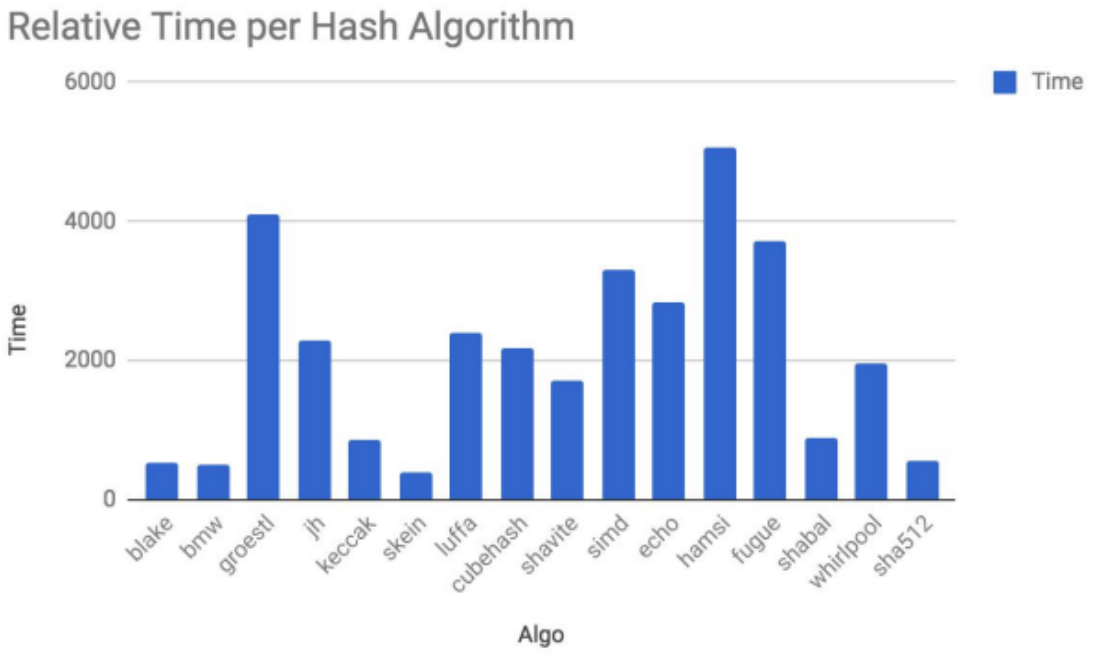

Ilustración 51: Velocidades relativas de los dieciséis algoritmos de minado del X16R
Fuente: https://ravencoin.org/assets/documents/X16R-Whitepaper.pdf

Otra opción y que es alternativa a la anterior, es desarrollar el algoritmo X16R+CNv4. Este nuevo algoritmo simplemente encadena el funcionamiento normal del X16R con el CNv4, pero hace que siempre se tenga que ejecutar el CNv4 y por tanto no se pueda llevar a cabo el vector de ataque anteriormente descrito.
El problema adyacente con este algoritmo se encuentra en que debido al alto tiempo de ejecución del CNv4 en comparación con el X16R hace que sea posible precalcular la salida del X16R mucho más rápido de lo que el algoritmo CNv4 puede ejecutarse.
Lo que hace que no sea muy diferente a simplemente cambiar el X16R por el CNv4.
Si que es cierto que mantener el algoritmo X16R con el X16R+CNv4 es más óptimo que cambiar directamente al CNv4, ya que evitaría que el hardware ASIC para CNv4 pudiese minar Ravencoins directamente.

Otra opción podría ser cambiar directamente de algoritmo. Por ejemplo del X16R al X21S. Tomado en cuenta por ser un algoritmo hash de minado criptográfico creado en una bifurcación dura o Hard Fork de Ravencoin y pertenecer a la familia.
Este algoritmo tiene dos diferencias con el X16R. La primera y más obvia es que incorporan 5 funciones Hash adicionales. La segunda, y que aporta la parte de la 'S', es que se ejecutan todas las funciones del algoritmo cada vez, es decir, las 21. Y ninguna de ellas puede repetirse.
Su funcionamiento es bastante parecido al X16R, gracias al valor del Hash del bloque anterior se sacan cuales y en que orden se van a utilizar las funciones Hash. Pero tiene la particularidad que en vez de realizarse con las 21 funciones Hash del algoritmo, solo sucede con las 16 del algoritmo X16R, las 5 restantes, se ubicarán uniformemente entre dichas 16 después de que se eliminen los duplicados y se hayan usado todas ellas.

Al X21S, se le puede aplicar la misma idea de incorporarle un algoritmo ASIC-hard, es decir, incluir el CNv4 al mismo, generando el X22S o el X21S+CNv4.

El algoritmo X21S+CNv4 por su parte sufriría del mismo problema que el X16R+CNv4, ya que el tiempo de ejecución del X21S es despreciable en comparación con el CNv4 y por tanto se podría precalcular.

En cuanto al algoritmo X22S nos encontramos con que en este algoritmo al contar con la parte 'S', en donde se ejecutan todos los algoritmos cada vez de forma aleatoria, el CNv4 se ejecutaría en todos los bloques y por tanto no se podría llevar a cabo el vector de ataque de esperar a uno que no lo implemente. Además de que tampoco se podría precalcular la parte del X21S.
Así pues este algoritmo es el más interesante de todas las opciones vistas ahora, pero sigue sin ser la opción perfecta.

La parte 'S' hace que sea más fácil la creación de ASICs debido a la estabilidad de potencia que estos aportan en contraposición a los algoritmos de parte 'R'. Además, debido a que el tamaño del dado de aleatoriedad requerido en los algoritmos con parte 'R' es proporcional al cuadrado del número de algoritmos, hace que el coste de fabricación de un ASIC aumente exponencialmente, con un aumento lineal de los algoritmos.
Por lo que podría decirse, que se vuelve más interesante el algoritmo X22R que el algoritmo X22S, aunque este tenga que sacrificar el algoritmo CNv4.

A modo de curiosidad, y en relación con la última aserción, en un post de uno de los principales desarrolladores de Ravencoin, Tron Black, nos encontramos con la siguiente conclusión, que resume muy bien toda la idea detrás de estos cambios:

> Es decir, más algoritmos, combinados con una selección aleatoria de algoritmos (permitiendo duplicados) es mejor para la resistencia ASIC que más algoritmos en secuencia (X11) o más algoritmos sin duplicados (X16S).

Los desarrolladores de Ravencoin seguían bastante interesados en incorporar el algoritmo CNv4, por lo que no acabaron satisfechos con implementar el X22R como última solución y terminaron ideando un nuevo algoritmo conocido como X22RC.
El algoritmo hash de minado criptográfico X22RC es exactamente igual que el X22R pero con el CNv4 como uno de los algoritmos garantizados para ser incluidos en el proceso.
Su funcionamiento se resume en dos pasos. El primero, es generar la lista ordenada de algoritmos que se va a aplicar para generar el Hash identificador de bloque. Exactamente de la misma manera que se hace con el X16R, pero en vez de usar 16 funciones Hash, se usan 22 (sin incluir el CNv4). Y el segundo paso, es sustituir alguno de los algoritmos de esa lista de manera aleatoria por el CNv4. Para elegir cuál, el valor de los 22 nibbles (Hash del bloque anterior) se suman y su resultado pasa por un módulo 22 (mod 22), lo que nos arroja un valor entre 0 y 21, es decir, la posición del algoritmo a sustituir por el CNv4.

Así pues como resumen final, el algoritmo hash de minado criptográfico X22RC acabó siendo la opción principal y favorita de los desarrolladores y usuarios de Ravencoin para implementar en caso de encontrar evidencias de minería ASIC en la red.

Algoritmo de minado X16Rv2
Por mediados del 2019, tras más o menos año y medio de funcionamiento, se acabó encontrando evidencias claras de ASICs para el algoritmo X16R en la red Ravencoin. Algunos artículos que ahondan más en el análisis y presentación de estas evidencias y que se pueden consultar son los siguientes:

- https://medium.com/@hardman/x16r-asics-in-the-fictional-world-of-westeros-b28460bf0322
- https://medium.com/@nbitsdev/presenting-evidence-of-mining-centralization-on-the-ravencoin-network-88743db1910a

Esto desencadenó que se activaran los procedimientos descritos en el punto anterior para cambiar de algoritmo y dejar obsoletos a dichos ASICs. Pero los desarrolladores y usuarios se encontraron con varias dificultades logísticas que impidieron implementar de manera correcta y oportuna el X22RC.
Básicamente, las aplicaciones de Wallet que soportan Ravencoin, como Medici Ventures o tZero, verifican cada bloque comprobando el Hash con una ejecución del encabezado a través del X16R. Esto se traduce, que las Wallet deben realizar un cambio de algoritmo, y, el algoritmo X22RC, debido al CNv4, agrega desafíos adicionales, sobre todo para dispositivos móviles.

Así pues, el plan cambió en el último segundo y se decidió hacer unas pequeñas modificaciones en el algoritmo X16R, generando el X16Rv2.

La solución consistió en agregar una nueva función hash, conocida como función Tiger, en tres partes diferentes del algoritmo X16R. O en otras palabras, hacer que se ejecute de forma adicional la función Tiger antes que las funciones Luffa-512, Keccak-512 y SHA-512.
Esta modificación dejaría totalmente obsoletos a los ASICs descubiertos al tener que ejecutar una función adicional para la cual no están preparados antes de poder ejecutar algunas de las funciones de las que sí está preparados.
Ahora el motivo de adicionar la función Tiger en tres funciones del X16R en vez de en una o en dos, es evitar que se generen bloques de transacciones en los que no sea necesario ejecutar este nuevo algoritmo, y por tanto, los ASICs puedan seguir minándolos.
La probabilidad de que ninguno de los tres algoritmos sea seleccionado para el bloque es $(13/16)^{16}$ o de alrededor del 3,5%. Que aunque no sea del 0%, como los propios desarrolladores comunicaron “Se puede vivir con ello”.

El cambio del X16R al X16Rv2 se hizo vigente el martes 01 de octubre de 2019 a las 16:00:00 UTC, mediante una bifurcación dura (Hard Fork) de la cadena.

Algoritmo de minado KawPow

Desde el mismo momento en que se implantó el algoritmo hash de minado criptográfico X16Rv2 en la red de Ravencoin, los desarrolladores, comenzaron de forma paralela una nueva hoja de ruta de actuación anti-ASIC.
Esta nueva hoja de ruta adquirió un enfoque un tanto diferente al anterior. A mucho pesar de los desarrolladores, se llevó a cabo un cambio en el paradigma del algoritmo de minado. Se decidió cambiar de los algoritmos de secuencia de algoritmos hash encadenados a los algoritmos de uso de memoria intensiva; y con ello abandonar la marca X16R que ellos mismos habían patentado.
En definitiva, se acabó desarrollando un nuevo algoritmo, denominado KawPow, como una adaptación del algoritmo de minado criptográfico ProgPow de memoria intensiva en la red Ravencoin.

El algoritmo hash de minado criptográfico ProgPow, era en su momento, uno de los principales sustitutos del algoritmo Ethash de Ethereum y una extensión del mismo.
ProgPow, como hemos mencionado en el primer párrafo, es un algoritmo con un enfoque del uso de memoria intensiva que pretende luchar contra los ASICs.
Aunque si es cierto que este enfoque de algoritmo es anti-ASIC, no pretende tanto eliminar a los ASICs del proceso de minado, como hacer que su eficiencia en comparación con las GPUs (e incluso CPUs) sea prácticamente despreciable, y por tanto, no supongan un gran problema para la descentralización de la red.

El funcionamiento de ProgPow es simple, se basa en tres patas:

1. Una alta dependencia al acceso a memoria.
2. Un proceso de minado adaptativo.
3. Un uso extenso y especifico de la arquitectura de las GPUs.

La alta necesidad a memoria, como comentábamos en la introducción de este capitulo, perjudica notablemente al rendimiento de los ASICs, ya que estos no tienen una forma plenamente eficiente del uso de la memoria como si pasa con los registros internos de las GPUs.

El disponer de un proceso de minado cambiante con el tiempo, y que no sea fijo, hace que los ASICs tengan serias dificultadas para adaptarse correctamente, en comparación con las GPUs y CPUs, que pueden ejecutar cualquier proceso en cualquier momento y sin muchos inconvenientes añadidos.
Y combinar ambas ventajas en un proceso plenamente consciente de la arquitectura de una GPU, hace que prácticamente un ASIC sea una GPU, y por ende, tenga unos puntos de eficiencia bastante parecidos.

Concretando de forma más tangible estas tres patas y su funcionamiento, tenemos que ProgPow, no tiene un proceso de minado fijo, sino que su declaración es cambiante en el tiempo. El protocolo, se genera en función de un conjunto de datos aleatorios que reciben el nombre DAG y que cambian cada X bloques, para que los ASICs no puedan nunca llegar a adaptarse a la nueva definición del protocolo, mientras que las GPUs y CPUs pueden adaptarse prácticamente al instante y no ver parada su actividad.
El DAG, tiene a proposito un peso importante de memoria, para que así sea necesario llevar a cabo múltiples accesos a memoria y por ende, los ASICs vean mermada su eficiencia.
Y por último, la declaración no cambiante del protocolo ProgPow, está optimizada para utilizar casi todos los componentes de las tarjetas gráficas, por tanto, los dispositivos de propósito especifico ASICs, acaben convirtiéndose prácticamente en GPUs. La única excepción en cuanto a componentes, son: la canalización de gráficos y las operaciones de punto flotante, para que así el algoritmo fuese compatible con los equipos de procesamiento paralelo de los diferentes fabricantes.

Para más información sobre las especificaciones del algoritmo ProgPow, se puede consultar el siguiente estándar EIP (Ethereum Improvement Proposal, o en español, Propuesta de Mejora en Ethereum): https://eips.ethereum.org/EIPS/eip-1057

El cambio del X16Rv2 al KawPow se hizo vigente el miércoles 06 de mayo de 2020 a las 18:00:00 UTC, mediante una bifurcación dura (Hard Fork) de la cadena de Ravencoin. Aproximadamente 7 meses después de la bifurcación del algoritmo X16Rv2.

CAPITULO 5

Presupuesto

En este quinto capítulo veremos una estimación del presupuesto que hubiese sido necesario recaudar para llevar con éxito el desarrollo de este proyecto de TFG (Trabajo de Final de Grado), si nos encontrásemos en una instancia o grupo de investigación de alguna entidad pública, como por ejemplo la Universidad; o de alguna entidad privada.

1. Presupuesto del proyecto

En la siguiente tabla se resumen todos los gastos y costes de material y personal que han sido necesarios para llevar de forma correcta el desarrollo de este proyecto:

Coste de material				
Material	**Precio**	**Duración**	**Uso**	**TOTAL**
Ordenador portátil	800,00€	3 años	5 meses	111,00€
Conexión a Internet	29,90€/mes	-	5 meses	149,50€
Cuenta Office Home o Students	149,99€	-	5 meses	149,99€
			Total:	410,49€
Coste por tiempo de trabajo				
Perfil	**Horas totales**	**Precio/Hora**		**TOTAL**
Ingeniero Informático Junior	425 horas	12€/hora		5.100,00€
			Total:	5.100,00€
		Total sin impuestos		5.510,49€
		IVA (21%)		1.157,20€
		TOTAL		**6.667,69€**

Así pues, el coste total del proyecto asciende a una cantidad de SEIS MIL SEISCIENTOS SESENTA Y SIETE EUROS CON SESENTA Y NUEVE CÉNTIMOS.

CAPITULO 6

Resumen, conclusiones y líneas futuras

En este sexto capítulo veremos un resumen de todo lo analizado en este proyecto de TFG (Trabajo de Final de Grado) para asentar todos los nuevos conocimientos adquiridos. Y finalizaremos, tanto el capitulo como el proyecto, con unas conclusiones y una disección sobre todos aquellos aspectos potencialmente interesantes para desarrollar en trabajos complementarios, ya que su alcance escapa a los primeramente planificados en este.

1. Resumen del proyecto

Hemos visto y analizado toda la arquitectura de Bitcoin al completo, lo que nos ha permitido entender cómo funciona y cuales son sus principios fundamentales.
Ahora, sabemos que el ecosistema Bitcoin es un sistema de pagos alternativo descentralizado basado en un modelo de UTXOs intercambiables entre usuarios. Respaldado por un sistema de verdad único, consistente en un registro Blockchain y en un sistema de consenso (basado en Proof of Work, con el algoritmo SHA-256 a la cabeza), ambos, fundamentados en criptográfica de clave publica y en funciones hash, que hacen posible mantener una correcta seguridad e integridad del sistema.

Hemos visto, que todo este ecosistema se puede extrapolar fácil y rápidamente a cualquier proyecto que imaginemos. Solo con disponer de un registro Blockchain y un sistema de consenso. Como por ejemplo sucede con el proyecto Ethereum.
Ethereum dispone de su propia Blockchain y de su sistema de consenso de Proof of Work basado en el algoritmo Ethash. Que permiten implementar un concepto de programación descentralizada mediante DApps y Smart Conctracts.

Y siguiendo con Ethereum, los tokens ERCs que se han podido desarrollar gracias al uso de Smart Contracts, han permitido digitalizar la propiedad de los activos de una forma fácil, segura y trazable. Lo que ha causado gran repercusión, sobre todo en el mundo de las Finanzas, con las DeFi (Finanzas descentralizadas), ya que han hecho posible eliminar a los Bancos y a sus políticas privadoras y abusivas. O en el mundo de la gestión de empresas y organizaciones, con las DAO (Organizaciones Autónomas descentralizadas), al permitir una mejor gestión de la empresa, más transparente, más rápida y más accesible.

Hemos visto también, que el sistema de consenso de Proof of Work y el algoritmo SHA-256 no son los únicos para llevar a cabo estos sistemas descentralizados. Han surgido multitud de variables a la Proof of Work, como por ejemplo, la Proof of Stake; y multitud de algoritmos, como por ejemplo, el X11, el X16R, el ProgPow o el KawPow.
Estos cambios y variaciones, han sido motivados por varios razones, como por ejemplo el consumo energético o la escalabilidad, pero sobre todo para evitar la centralización que estaba dando alrededor de Bitcoin por el uso de hardware especializado, como es el caso de los ASICs.

2. Conclusiones del proyecto

Personalmente creo que estos ecosistemas descentralizados que hemos ido analizando a lo largo de todo el proyecto tienen gran potencial. Básicamente, nos permiten desarrollar cualquier sistema, herramienta o recurso de una forma relativamente fácil, como en cualquier otra herramienta del mercado. Pero estos mantienen un registro inmutable de la propiedad, que hace inviable llevar a cabo cualquier tipo de censura, además, de aporta a los desarrolladores la posibilidad de recibir de forma rápida y transparente cualquier tipo de remuneración mediante el uso de criptomonedas nativas.

Si que es cierto, que todavía está muy poco asentada esta tecnología, y hace que proyectos interesantes no reciban toda la atención que se merecen o acaban fracasando por precisamente esta razón. Pero creo que es cuestión de tiempo, que la tecnología Blockchain acabe incrustándose en la sociedad como pasó con Internet.

Por criticar algún aspecto de esta nueva tecnología, no me gusta el tono que está tomando tan especulativo, literalmente, cualquier proyecto o recurso que se desarrolle acaba basándose en su potencial especulativo en vez de en su potencial innovador.
Los usuarios acaban usando el producto desarrollado para ganar algo de dinero y luego lo dejan abandonado. Y pienso que esto lo único que hace es alejar a la tecnología Blockchain de una correcta integración en la sociedad.

3. Líneas futuras del proyecto

Una vez entendidos todos los conceptos vistos en este proyecto, se puede empezar a opinar con fundamento en el mundillo. Y sobre todo, se puede empezar a trabajar en él. Ahora que se entiende y se sabe como funciona todo y como se puede llegar a manipular, sería interesante seguir la proyección obtenida con este TFG con el desarrollo de algo más tangible. Por ejemplo, desarrollar alguna DApp o Contrato inteligente, en el que se ponga en practica todos estos conceptos de los que hablamos y en el que podamos ver con nuestros propios ojos el funcionamiento real de todo ello. Además, de por su parte, tener la posibilidad de ampliar conceptos de programación, ya que como vimos, Ethereum dispone de una máquina de Turing completa que permite la programación, y, existen varios lenguajes de programación especializados como Solidity, Vyper o Yul, que son un tanto diferentes a los que ya conocidos como Python, C o Java.

Quizás, también sería interesante seguir el análisis por una rama un poco más económica. Viendo que aportan realmente estos activos, como las criptomonedas y los tokens a la sociedad y al mundo real. Comprendiendo los fenómenos económicos que tienen asociados y como repercuten a los propios activos y al entorno. O simplemente como poder interactuar eficientemente con ellos desde un punto de vista financiero.
Es una propuesta que deja de lado la parte técnica, pero no por ello es menos atractiva.

Quizás también sería interesante ahondar más en el campo del hardware ASIC y los algoritmos, para poder ver exactamente como se construyen, como funcionan y todas sus características particulares.
E incluso sería interesante iniciar proyectos alternativos sobre los mismos, como explorarlos y explotarlos en busca de algunos puntos débiles, para reportarlos y contribuir en el desarrollo de mejores algoritmos, o, simplemente buscar mejorar en cuanto a la eficiencia y seguridad de los mismos.

O simplemente, se puede seguir ampliando conocimientos del mundo cripto. Hay innumerables alternativas y proyectos construidos sobre toda esta tecnología, cuyos conceptos no pueden ser abarcados con un solo proyecto. Por ejemplo, hoy en día está muy de moda los juegos NFTs, y con ellos los Marketplaces de NFTs. Son unos conceptos muy interesantes de ser explotados. Aunque no los únicos.

Bibliografía

[1] Bitcoin.org. Satoshi Nakamoto. 2008. Bitcoin: un sistema de dinero en efectivo electrónico peer-to-peer. [Online]. Available: https://bitcoin.org/files/bitcoin-paper/bitcoin_es.pdf

[2] YouTube. Nate Gentile. Septiembre 2017. Entiende Bitcoin y Ethereum - Explicación técnica a fondo en español sobre Criptomonedas. [Online]. Available: https://www.youtube.com/watch?v=YBNr69vrscw

[3] Banco España. Carlos Conessa. 2019. Bitcoin: ¿Una solución para los sistemas de pago o una solución en busca de problema?. [Online]. Available: https://www.bde.es/f/webbde/SES/Secciones/Publicaciones/PublicacionesSeriadas/DocumentosOcasionales/19/Fich/do1901.pdf

[4] Universidad de Alcalá de Henares. Álvaro Pérez Lietor. 2020. Introducción al Cryptojacking y creación de website maliciosa. [Online]. Available: https://ebuah.uah.es/dspace/bitstream/handle/10017/40887/TFG_Perez_Lietor_2020.pdf?sequence=1&isAllowed=y

[5] Mobile Transaction. Edgar Martin. Abril 2022. Cómo funciona el procesamiento de pagos con tarjeta. [Online]. Available: https://es.mobiletransaction.org/como-funciona-el-procesamiento-de-pagos-con-tarjeta/#:~:text=El%20terminal%20f%C3%ADsico%20del%20vendedor,solicitud%20al%20banco%20del%20cliente

[6] Bit2me. Bit2me. Julio 2022. ¿Qué es SHA-256?. [Online]. Available: https://academy.bit2me.com/sha256-algoritmo-bitcoin/

[7] Bit2me. Bit2me. Marzo 2022. ¿Qué es el bloque génesis (Genesis Block)?. [Online]. Available: https://academy.bit2me.com/que-es-bloque-genesis/

[8] Bit2me. Bit2me. Marzo 2022. ¿Qué es una transacción coinbase?. [Online]. Available: https://academy.bit2me.com/que-es-coinbase-transaccion/

[9] MarketScreener, Laurent Pignot. Mayo 2022. Bitcoin, el rompecabezas de 10 minutos. [Online]. Available: https://es.marketscreener.com/noticias/ultimas/Bitcoin-el-rompecabezas-de-10-minutos--40592803/

[10] Criptotario. Martín. Mayo 2022. ¿Por qué el bloque de Bitcoin tarda 10 minutos?. [Online]. Available: https://criptotario.com/10-minutos-bitcoin

[11] Bit2me. Bit2me. Marzo 2022. Explorador blockchain a fondo (IV): Bloques. [Online]. Available: https://academy.bit2me.com/explorador-de-blockchain-a-fondo-bloques/#:~:text=El%20tama%C3%B1o%20m%C3%A1ximo%20de%20un,del%20minado%20de%20ese%20bloque

[12] Criptonoticias. Isabel Pérez. Marzo 2021. Blockchain: bloques, transacciones, firmas digitales y hashes. [Online]. Available: https://www.criptonoticias.com/criptopedia/blockchain-bloques-transacciones-firmas-digitales-hashes/#:~:text=El%20bloque%20de%20una%20blockchain,completarse%2C%20como%20ya%20hemos%20visto

[13] Bit2me. Bit2me. Julio 2022. Cómo saber la comisión de una transacción Bitcoin. [Online]. Available: https://academy.bit2me.com/como-saber-la-comision-de-una-transaccion-bitcoin/

[14] Criptonoticias. Criptonoticias. Junio 2021. Lo que debes saber sobre las comisiones en Bitcoin y otras redes PoW. [Online]. Available: https://www.criptonoticias.com/criptopedia/debes-saber-sobre-comisiones-bitcoin-otras-redes-pow/

[15] Bit2me. Bit2me. Marzo 2022. ¿Qué es Coinbase Maturity?. [Online]. Available: https://academy.bit2me.com/que-es-coinbase-maturity/

[16] Binance Academy. Binance Academy. Febrero 2022. Introducción a los Merkle Trees (Árboles de Merkle) y Merkle Roots (Raíces de Merkle). [Online]. Available: https://academy.binance.com/es/articles/merkle-trees-and-merkle-roots-explained

[17] Wikipedia. Anónimo. Enero 2022. Estructura de transacciones y bloques en Bitcoin. [Online]. Available: https://es.wikipedia.org/wiki/Anexo:Estructura_de_transacciones_y_bloques_en_Bitcoin

[18] Real Academia Española. Real Academia Española. Diciembre 2021. Valor. [Online]. Available: https://dle.rae.es/valor

[19] Bit2me. Bit2me. Julio 2022. ¿Qué es una wallet o monedero de criptomonedas?. [Online]. Available: https://academy.bit2me.com/wallet-monederos-criptomonedas/#:~:text=El%20t%C3%A9rmino%20wallet%20hace%20referencia,claves%20privadas%20de%20nuestras%20criptomonedas

[20] Bit2me. Bit2me. Marzo 2022. ¿Qué es un exchange de criptomonedas?. [Online]. Available: https://academy.bit2me.com/que-es-exchange-criptomonedas/

[21] National Geographic España. Héctor Rodríguez. Mayo 2022. Criptomonedas, la huella de carbono del dinero digital. [Online]. Available: https://www.nationalgeographic.com.es/ciencia/criptomonedas-huella-carbono-dinero-digital_16761

[22] Bitcoin.org. Bitcoin.org. Página web del proyecto Bitcoin. [Online]. Available: https://bitcoin.org/es/

[23] Blockchain.com. Blockchain.com. Tiempo real. Gráficos de Blockchain. [Online]. Available: https://www.blockchain.com/es/charts

CAPITULO 3: Legado de Bitcoin

[24] Ethereum.org. Vitalik Buterin. Agosto 2022. Ethereum Whitepaper. [Online]. Available: https://ethereum.org/en/whitepaper/#code-execution

[25] Ethereum.org. Corwin Smith. Abril 2022. Cuentas de Ethereum. [Online]. Available: https://ethereum.org/es/developers/docs/accounts/

[26] Ethereum.org. Joshua. Mayo 2022. Transacciones. [Online]. Available: https://ethereum.org/es/developers/docs/transactions/

[27] Ethereum.org. Paul Wackerow. Julio 2022. Introducción a los contratos inteligentes. [Online]. Available: https://ethereum.org/es/developers/docs/smart-contracts/

[28] Ethereum.org. Joshua. Agosto 2022. Máquina Virtual de Ethereum (EVM). [Online]. Available: https://ethereum.org/es/developers/docs/evm/

[29] Ethereum.org. Joshua. Enero 2022. Lenguajes de contrato inteligente. [Online]. Available: https://ethereum.org/es/developers/docs/smart-contracts/languages/#example-contract

[30] Ethereum.org. Víctor Dusart. Julio 2022. Opcodes for the EVM. [Online]. Available: https://ethereum.org/es/developers/docs/evm/opcodes/

[31] YouTube. BitcoinPendium. Octubre 2020. Smart Contracts de Ethereum Explicados! ERC-20, ERC-721, ERC-1155, todo lo que tienes que saber!. [Online]. Available: https://www.youtube.com/watch?v=bYppbVKnxtM

[32] Binance Academy. Binance Academy. Mayo 2022. Una introducción a los Tokens ERC-20. [Online]. Available: https://academy.binance.com/es/articles/an-introduction-to-erc-20-tokens

[33] Marker Blog. Marker Blog. Febrero 2020. Los diferentes tipos de Tokens de Criptomonedas Explicados. [Online]. Available: https://blog.makerdao.com/los-diferentes-tipos-de-tokens-de-criptomonedas-explicados/

[34] BBVA. BBVA Communications. Marzo 2022. Qué son las DApps y por qué serán cada vez más importantes. [Online]. Available: https://www.bbva.com/es/que-son-las-dapps-y-por-que-seran-cada-vez-mas-importantes/

[35] Wikipedia. Anónimo. Mayo 2022. Finanzas descentralizadas. [Online]. Available: https://es.wikipedia.org/wiki/Finanzas_descentralizadas

[36] Wikipedia. Anónimo. Julio 2022. Organización autónoma descentralizada. [Online]. Available: https://es.wikipedia.org/wiki/Organizaci%C3%B3n_aut%C3%B3noma_descentralizada

[37] Binance Academy. Binance Academy. Marzo 2022. Todo lo que necesitas saber sobre Initial Coin Offerings (ICOs). [Online]. Available: https://academy.binance.com/es/articles/what-is-an-ico

[38] BBVA. Vanessa Pombo Nartallo. Noviembre 2021. ¿Qué diferencias hay entre un 'token' y una criptomoneda?. [Online]. Available: https://www.bbva.com/es/que-diferencias-hay-entre-un-token-y-una-criptomoneda/

[39] BBVA. BBVA Communications. Diciembre 2020. Los activos digitales del futuro: tokenizados, programables y más seguros. [Online]. Available: https://www.bbva.com/es/los-activos-digitales-del-futuro-tokenizados-programables-y-mas-seguros/

[40] Bit2me. Bit2me. Agosto 2022. ¿Qué es Ethereum (ETH)?. [Online]. Available: https://academy.bit2me.com/que-es-ethereum-eth-criptomoneda/

[41] Bit2me. Bit2me. Agosto 2022. ¿Qué es una Stablecoin?. [Online]. Available: https://academy.bit2me.com/que-es-stablecoin/

[42] Ethereum.org. Ethereum.org. Agosto 2022. Introducción a Web3. [Online]. Available: https://ethereum.org/es/web3/

[43] The New York Times. Kevin Roose. Marzo 2022. ¿Qué es la web3?. [Online]. Available: https://www.nytimes.com/es/interactive/2022/03/29/espanol/web3-que-es.html

[44] Ravencoin.org. Bruce Fenton & Tron Black. Abril 2018. Ravencoin: A Peer to Peer Electronic System for the Creation and Transfer of Assets. [Online]. Available: https://ravencoin.org/assets/documents/Ravencoin.pdf

[45] Ravencoin.org. Tron Black & Joel Weight. X16R: ASIC Resistant by Design. [Online]. Available: https://ravencoin.org/assets/documents/X16R-Whitepaper.pdf

[46] Binance Academy. Binance Academy. Agosto 2022. ¿Qué es un algoritmo de Consenso?. [Online]. Available: https://academy.binance.com/es/articles/what-is-a-blockchain-consensus-algorithm

[47] Binance Academy. Binance Academy. Enero 2022. Proof of Work (PoW) vs. Prood of Stake (PoS). [Online]. Avilable: https://academy.binance.com/es/articles/proof-of-work-vs-proof-of-stake

[48] Binance Academy. Binance Academy. Enero 2022. ¿Qué es Proof of Stake (PoS)?. [Online]. Available: https://academy.binance.com/es/articles/proof-of-stake-explained

[49] Binance Academy. Binance Academy. Agosto 2022. ¿Qué es el Staking?. [Online]. Available: https://academy.binance.com/es/articles/what-is-staking

[50] Binance Academy. Binance Academy. Diciembre 2020. Proof of Authority. [Online]. Available: https://academy.binance.com/es/articles/proof-of-authority-explained

[51] Binance Academy. Binance Academy. Diciembre 2020. Proof of Burn Explicada. [Online]. Available: https://academy.binance.com/es/articles/proof-of-burn-explained

[52] Binance Academy. Binance Academy. Diciembre 2020. Consenso de PoW / PoS híbrido explicado. [Online]. Available: https://academy.binance.com/es/articles/hybrid-pow-pos-consensus-explained

[53] Cointelegraph. Anthony Clarke. Julio 2022. Proof-of-time vs Proof-of-stake: cómo se comparan los dos algoritmos. [Online]. Available: https://es.cointelegraph.com/news/proof-of-time-vs-proof-of-stake-how-the-two-algorithms-compare

[54] Bitcoin Magazine. Bitcoin Magazine. Agosto 2020. What are Bitcoin Forks?. [Online]. Available: https://bitcoinmagazine.com/guides/what-are-bitcoin-forks#:~:text=A%20codebase%20fork%20is%20a,establish%20a%20whole%20new%20cryptocurrency.

[55] 99Bitcoins. Ofir Beigel. Marzo 2022. The Beginner's Guide to Bitcoin Forks. [Online]. Available: https://99bitcoins.com/bitcoin-forks/

[56] Criptonoticias. Criptonoticias. Marzo 2021. Qué es una bifurcación (fork) de blockchain. [Online]. Available: https://www.criptonoticias.com/criptopedia/que-es-bifurcacion-fork-soft-hard-blockchain/

[57] Medium. Tron Black. Julio 2019. Ravencoin – ASIC Thoughts. [Online]. Available: https://tronblack.medium.com/ravencoin-asic-thoughts-e6c0079609e6

[58] Bit2me. Bit2me. Marzo 2022. ¿Qué es el algoritmo de minería X11?. [Online]. Available: https://academy.bit2me.com/que-es-algoritmo-mineria-x11/

[59] Dash.org. Evan Duffield & Daniel Diaz. Agosto 2018. Dash: A payments-Focused Cryptocurrency. [Online]. Available: https://github.com/dashpay/dash/wiki/Whitepaper

[60] GetPimp. GetPimp. Junio 2018. Blog: What are all these X11, X13, X15 algorithms made of?. [Online]. Available: https://getpimp.org/what-are-all-these-x11-x13-x15-algorithms-made-of/

[61] Wikipedia. Anónimo. Febrero 2022. NIST hash function competition. [Online]. Available: https://en.wikipedia.org/wiki/NIST_hash_function_competition#Finalists

[62] Publish0x. CryptoMoneyMaker. Noviembre 2019. X16R & X16RV2 Algorithms For Dummies [Explained]. [Online]. Available: https://www.publish0x.com/passive-income-crypto/x16r-and-x16rv2-algorithms-for-dummies-explained-xvpdkr

[63] Medium. Hardman. Julio 2019. X16R ASICs in the fictional world of Westeros. [Online]. Available: https://medium.com/@hardman/x16r-asics-in-the-fictional-world-of-westeros-b28460bf0322

[64] Medium. Standarerror. Julio 2019. Presenting evidence of increasing mining centralization on the Ravencoin network. [Online]. Available: https://medium.com/@nbitsdev/presenting-evidence-of-mining-centralization-on-the-ravencoin-network-88743db1910a

[65] Medium. Tron Black. Enero 2020. Ravencoin – ASIC Thougths – Round Two. [Online]. Available: https://tronblack.medium.com/ravencoin-asic-thoughts-round-two-f4f743942656

[66] 2Miners. 2Miners. Febrero 2019. Ethereum ProgPow Explained. [Online]. Available: https://2miners.com/blog/ethereum-progpow-explained/

[67] 2Miners. 2Miners. Mayo 2020. KawPow: New Ravencoin Mining Algorithm. [Online]. Available: https://2miners.com/blog/kawpow-new-ravencoin-mining-algorithm/

[68] Ethereum.org. Greg Colvin, Andrea Lanfranchi, Michael Carter & IfDefElse. Mayo 2018. EIP-1057: ProgPow, a Programmatic Proof-of-work. [Online]. Available: https://eips.ethereum.org/EIPS/eip-1057

Universidad de Alcalá

Escuela Politécnica Superior

ESCUELA POLITECNICA SUPERIOR