BLOCKCHAIN

1. Introducción.

En 2008 un usuario anónimo llamado Satoshi Nakamoto, publicó un paper en el que hablaba sobre el BitCoin, una forma de dinero electrónico basada en el Peer-to-Peer.
Esta moneda permitiría hacer pagos online directamente entre los usuarios sin pasar a través de una institución financiera central.
En este vídeo no nos centraremos directamente en el BitCoin, sino en el concepto de BlockChain y la tecnología que hay detrás de todas las criptomonedas.
Veremos conceptos como el de Peer-to-Peer, Proof-of-Work y la Función de Hash.
Antes de empezar con las explicaciones, en la descripción del vídeo tenéis una lista de documentos de donde he sacado la información de este vídeo. El más importante de todos es el propio paper que publicó Satoshi Nakamoto en 2008, explicando como funciona el BitCoin.

2. El concepto de CriptoMoneda.

El comercio en Internet depende principalmente de las instituciones financieras que se encargan de procesar y administrar los pagos electrónicos, este proceso de administrar los pagos, incrementa los costes de las transacciones mediante Internet. Estas transacciones también tienen el problema de que no son anónimas, y nos vemos obligados a confiar nuestra actividad bancaria electrónica a estos intermediarios.
Satoshi propuso un sistema de pago electrónico basado en criptografía, en lugar de confianza. Permitiendo transacciones sin necesidad de un tercero en el que confiar.

3. El uso del BlockChain en las CriptoMonedas.

Empezaremos hablando del concepto más sencillo y puede que el más conocido: El Peer-to-Peer.

3.1 Peer-to-Peer (P2P)

El Peer-to-Peer o P2P es una red de ordenadores descentralizada, en la que no hay un ordenador central que contenga toda la información de la red, todos los ordenadores de esa red son cliente y servidor al mismo tiempo. Una de las aplicaciones más conocidas del P2P es el sistema Torrent.
Al descargar un archivo mediante el protocolo Torrent, no te estas descargando ese archivo de un servidor central, ese archivo lo tienen miles de usuarios de la red, de manera que las personas que ya tienen descargado el archivo pueden hacer de servidor. El archivo es descargado en distintas partes que provienen de distintos usuarios, finalmente las partes se unen para que tu tengas en tu ordenador el archivo completo. Este sistema, nos permite usar la red sin que haya un servidor central que tenga el poder y control absoluto.

Ahora imaginemos una red de ordenadores entre los que queremos poder hacer transacciones. Imaginaremos que cada ordenador es un usuario distinto.
Para tener el control de la cantidad de dinero de cada usuario, todas estas transacciones se guardarán en un registro, al que todos los ordenadores de la red tienen acceso, así que accediendo al registro y haciendo unos pequeños cálculos, podemos saber el saldo de cada uno de los usuarios de la red.

Aquí podemos ver que hay un problema, ya que todos los usuarios de la red pueden modificar este registro, de manera que no podemos evitar que el Usuario A de forma malintencionada añada “Usuario B paga 10€ al Usuario A.”, sin que el Usuario B haya confirmado esta transacción.
Necesitamos una forma de poder verificar las transacciones, así que añadiremos una Firma Digital a nuestra transacción.

3.2 La Firma Digital

La Firma Digital, es un mecanismo usado para verificar la autenticidad de un mensaje o archivo. Cada usuario de esta red, tendrá una firma digital, formada por dos claves, la clave pública y la clave secreta. Tal y como se puede deducir por los nombres, la clave pública la puede ver todo el mundo y la secreta solo el propietario de la Firma Digital. Si alguien se hace con nuestra clave secreta, es como si alguien obtiene nuestras contraseñas bancarias, ya que podrá verificar transacciones en nuestro nombre.

Una de las diferencias más importantes entre la firma escrita manualmente en un papel y la Firma Digital, es que la Firma Digital es diferente para cada mensaje que firma.
Las Firmas Digitales son completamente distintas para archivos similares, si vemos estas firmas, veremos que el resultado es completamente distinto, parece aleatorio.

La Firma Digital se genera mediante una función que recibe el mensaje y la clave privada, por lo que solo el dueño de esa clave privada puede generar la Firma Digital.
Una vez la Firma Digital se ha generado, se puede verificar mediante una función que recibe el mensaje que se quiere verificar, la Firma Digital generada y la clave pública, y nos dice si esa Firma Digital ha sido generada mediante ese mensaje y mediante la parte secreta de esa clave pública.

De esta forma, la transacción “Usuario Azul paga 10€ al Usuario Rojo.”, debe ser verificada por el Usuario Azul, si el Usuario Azul está de acuerdo en hacer ese pago, la verificará con su clave privada (Cosa que solo puede hacer el) y entonces se puede añadir la transacción al registro público, donde pondremos la transacción en si, la Firma Digital y la Clave Pública. De esta forma, mediante la función de verificar, podremos verificar cualquier transacción antes de añadirla en el registro definitivamente.

No entraremos en detalle de como funciona este método de Clave Privada y Clave Pública, pero nos quedaremos con la idea de que la única manera de verificar un mensaje solo con la Clave Pública, es ir probando Firmas Digitales de forma aleatoria. Estas Firmas Digitales se hacen mediante un sistema llamado SHA256, por lo que una firma digital, está formada por 256 Bytes, lo que son 2048 ceros y unos. Esto significa que las probabilidades de acertar la Firma Digital es $1/2^{256}$. Este número es descomunalmente pequeño, así que os dejo un video muy interesante sobre este mismo tema.

Es importante mencionar, que las transacciones contienen el instante exacto en el que se ha hecho la transacción, por lo que por mucho que el Usuario B pague 10€ al Usuario A diversas veces, las transacciones no podrán ser en el mismo instante, por lo que siempre serán distintas y tendrán una Firma Digital distinta. Esta Firma Digital se conoce como Hash.

Ahora tenemos un sistema que registra todas las transacciones y los movimientos de nuestra moneda, por lo que sabemos la cantidad de dinero que tiene cada usuario.
- Todos los usuarios pueden escribir en el registro.
- Siempre que se escriba en el registro, se debe añadir una Firma Digital a la transacción.
- Si el sistema verifica la transacción, esta queda escrita oficialmente en el registro y será válida.

Vemos que antes de añadir una transacción, hay un sistema encargado de ejecutar la verificación de la transacción y que este sistema es el que guarda el registro de transacciones.
Sabemos que nuestra moneda tiene el objetivo no depender de una institución central.
¿Entonces quien se está encargando de verificar las transacciones y guardar el registro?

3.3 El BlockChain.

El BlockChain es una secuencia de bloques encadenados donde cada bloque nos indica cual es el siguiente bloque. Esta secuencia de bloques no existe en un solo sitio de nuestra red, sino que versiones idénticas del BlockChain se encuentran en los ordenadores de algunos usuarios de nuestra red, estos usuarios se conocen como mineros. Por ahora, vamos a entender un bloque como una transacción de un usuario a otro. (Más tarde entraremos en detalles sobre su contenido real)
Los mineros, se encargan de gestionar el BlockChain, añadiendo a la cadena de bloques, transacciones correctamente verificadas.
Si “Alice paga 10€ a Bob.”, un minero añadirá esta transacción con su firma digital a la cadena.

Como el BlockChain se encuentra en los ordenadores de los mineros de la red, todos ellos deben tener el mismo contenido en los bloques, por lo que el minero que quiere añadir una transacción debe mandarla a todos los otros mineros y que todos ellos la verifiquen y la añadan. Si más de la mitad de los mineros aceptan el bloque, la transacción ha quedado registrada para siempre.

Realmente un bloque no contiene una sola transacción, un bloque está formado por texto: contiene unas 2000 transacciones, el momento exacto en el que se ha creado el bloque, la cantidad de mineros que lo han aceptado, el número de transacciones que hay en el, su tamaño en bytes, la recompensa, un número aleatorio y otra información menos importante. Sobre esta recompensa y este número aleatorio, entraremos en detalle más tarde.
De la forma que está programado el BitCoin, se añade aproximadamente un bloque cada 10 minutos. Esto son unas 3 o 4 transacciones por segundo.

Al sistema del BitCoin, le interesa que hayan mineros, ya que dan seguridad, velocidad y estabilidad a la red. Por esta razón, el trabajo del minero se ve recompensado, ya que al generar un bloque que se añada correctamente al BlockChain, se recibe una recompensa. Inicialmente, la recompensa era de 50 BitCoins. Pero esta cantidad se va reduciendo con el tiempo, cada 210 mil bloques, esta recompensa se divide entre dos. Actualmente la recompensa es de 6.25 BitCoins.

Anteriormente hemos visto que las transacciones se verificaban mediante una clave pública y una privada, que generaban una Firma Digital o Hash. Cada bloque también tiene asignado un Hash.

Usamos SHA256 que para un mensaje de entrada, nos devuelve siempre un conjunto de 64 números y letras, lo que son 256 bytes. Cada bloque contiene un Hash hecho mediante SHA256, y el Hash del siguiente bloque, por lo que podemos entender que la forma de identificar un bloque es mediante su Hash.

Finalmente falta un concepto, minar un bloque no es una operación sencilla. De esta forma se consigue que minar bloques no se pueda hacer de forma instantánea. Esto se hace mediante el sistema de Proof-of-Work.

3.4 Proof-of-Work

Una de las normas para añadir un bloque es que el Hash de todos aquellos bloques que añadamos a la cadena, debe empezar por un número determinado de ceros.
Por lo que una vez ya tenemos todas las transacciones y toda la información necesaria para crear nuestro bloque, debemos encriptar el contenido de nuestro bloque con SHA256, hasta que el Hash que se nos genere, empiece con un número determinado de ceros.
Antes hemos visto que una de las cosas que contiene un bloque, es un número aleatorio, así que debemos ir modificando su valor hasta conseguir un resultado que empiece con los ceros necesarios.
Este proceso tiene un coste muy alto y es lo que se llama minar BitCoins, aunque realmente se minan bloques que nos dan una recompensa en BitCoins.

El trabajo necesario para generar un Hash es exponencial al número de ceros necesarios, así que el propio sistema va regulando esta cantidad para mantener la regla de un bloque cada 10 minutos. Cada 2016 bloques, se revisa el número de ceros para asegurar que la regla se mantiene.

Estas reglas más concretas como los 10 minutos, las recompensas, las transacciones por bloques o cada cuantos bloques se revisa el número de ceros, pueden variar dependiendo de la criptomoneda. En este vídeo, eran las reglas del BitCoin, aunque la mayoría tienen las mismas o similares.

Todo esto ha sido mucha información, así que vamos a hacer un resumen de todo lo que hemos visto:
Una criptomoneda realmente es una cadena de bloques que existe en algunos usuarios de la red, estos usuarios se encargan de añadir y verificar bloques en esta cadena, su trabajo es minar. Los bloques contienen varia información, pero principalmente contienen unas 2000 transacciones, un Hash generado mediante SHA256, un número aleatorio y una recompensa. El Hash debe empezar por un número determinado de ceros, y la única forma de conseguir esto es ir modificando el número aleatorio de forma aleatoria. Al conseguir este Hash, se manda el bloque a todos los mineros, y si la mayoría lo aprueba, esas transacciones han sido confirmadas y el minero recibe una recompensa.

4. Conclusión

El BlockChain es de acceso público, y vosotros mismos podéis explorarlo mediante páginas web, podréis ver con detalle toda la información que contiene cada bloque y todas sus transacciones, es más, podéis llegar a buscar los primeros bloques de BitCoin que fueron minados por el propio Satoshi Nakamoto. El hecho de que los registros sean públicos, no implica que no haya privacidad en las transferencias, sino todo lo contrario, si veis los detalles de una transferencia, la información de el que manda el dinero y el que lo recibe es totalmente anónima. Solo tenemos un identificador de cartera con el que no podemos hacer nada.

Como veis, es un sistema muy complejo y con una gran seguridad. Y en este vídeo solo hemos visto algunas de sus características más importantes, ya que hay muchos detalles técnicos sobre programación, estadística y probabilidad que no he nombrado.

Pero me parece que por ahora esto es suficiente.
Recordad que en la descripción tenéis las fuentes y una enlace a una página web para explorar el BlockChain de BitCoin.

Muchas Gracias por ver el vídeo, cualquier duda en los comentarios y nos vemos en el siguiente vídeo.