Considere una situación que se muestra en la imagen.

Doble Gasto

Como se ve claramente aquí, Bob está ofreciendo un billete de 10 dólares a Lisa a cambio de un libro. Una vez que Lisa recibe este billete físico de $10, Bob no tiene forma de reutilizar este dinero para alguna otra transacción, ya que la moneda física está ahora en posesión de Lisa.

Ahora, considere una situación en la que el dinero se paga en forma digital. Esto se ilustra en la imagen.

Formulario de pago digital

Como el formato para el cambio de dinero está en el formato digital, es esencialmente un archivo físico binario almacenado en algún lugar en el dispositivo de Bob. Después de que Bob le dé este archivo (dinero digital) a Lisa, también puede darle una copia del archivo a Alice. Ambos ahora piensan que han recibido el dinero sin tener ningún medio de autentificar la moneda digital y así entregarían sus respectivos bienes a Bob. Esto se denomina doble gasto cuando el remitente gasta el mismo dinero en más de un lugar para obtener servicios o mercancías de varios proveedores.

Para resolver este problema de doble gasto, se emplearía una autoridad centralizada para controlar todas las transacciones. Esto se ilustra en la imagen.

Autoridad Centralizada

La autoridad centralizada, que en términos comunes es su banco, mantiene un libro mayor que registra todas las transacciones. Ahora, Bob tiene que enviar su dinero digital al banco, que haría una entrada en su libro mayor debitando la cuenta de Bob. Después de asegurarse de que Bob tiene suficiente saldo para pagar el dinero digital que quiere enviar, enviaría el dinero a Lisa acreditando su cuenta en su libro mayor.

Ahora, está garantizado que Bob no puede gastar el dinero dos veces. Si cada transacción digital se enruta a través de una autoridad centralizada como ésta, se resolvería el problema del doble gasto. Esto también proporciona otro beneficio al validar la autenticidad de cada moneda (dinero digital) que recibe en la transacción. Así que el dinero falso (dinero duplicado como en el caso de Bob pagando a Alice usando una copia) sería fácilmente detectado y prevenido de la circulación.

La introducción de la autoridad centralizada, aunque resuelve el problema del doble gasto, introduce otro problema importante: el costo de crear y mantener la propia autoridad centralizada.

Como los bancos necesitan dinero para sus operaciones, empiezan a recortar comisiones en cada transacción de divisas que realizan para sus clientes. Esto a veces puede llegar a ser muy costoso, especialmente en las transferencias de dinero al extranjero, donde múltiples agentes (bancos) pueden estar involucrados en todo el negocio.

Todos estos problemas se resuelven con la introducción de la moneda digital, llamada Bitcoin. Ahora les daré un breve resumen de lo que es Bitcoin antes de profundizar en su diseño y arquitectura.

El Bitcoin fue introducido en este mundo por Satoshi Nakamoto a través de un libro blanco de investigación titulado Bitcoin: A Peer-to-Peer Electronic Cash System en el año 2008.

El Bitcoin no sólo resolvió el problema del doble gasto, sino que también ofreció muchas más ventajas, una de las cuales vale la pena mencionar aquí es el anonimato en las transacciones. Satoshi, quien creó el sistema y realizó pocas transacciones con monedas en este sistema, es totalmente anónimo para todo el mundo.

Imagínense, en este mundo de los medios sociales, cuando la privacidad de cada individuo está en juego, el mundo no es capaz de averiguar hasta ahora quién es Satoshi? De hecho, no sabemos si Satoshi es un individuo o un grupo de personas. La búsqueda en Google también reveló el hecho de que las bitcoins que tiene Satoshi Nakamoto valen alrededor de 19.400 millones de dólares, dinero que ahora sigue sin reclamarse en el sistema Bitcoin. ¿Qué es Bitcoin? ¡Echemos un vistazo!

¿Qué es Bitcoin?

Como se ha visto anteriormente, el banco mantiene un libro mayor que registra cada transacción. Este libro mayor es de propiedad privada y es mantenido por el banco. Satoshi propuso que este libro fuera público y mantenido por la comunidad.

En el momento en que se hace público un libro así, se le ocurren varias consideraciones. Este libro tiene que ser a prueba de manipulaciones para que nadie pueda modificar sus entradas. Como cada entrada en el libro de contabilidad es visible públicamente, tendremos que averiguar cómo mantener el anonimato - obviamente no le gustaría que todo el mundo supiera que le pagué un millón de dólares.

Además, como sólo hay un único ledger que lleva un registro de todas y cada una de las operaciones en el mundo, el tamaño del ledger sería otra gran preocupación. Proporcionar una solución a estas complejidades no era trivial y eso es lo que intento hacer aquí para que entiendas la arquitectura subyacente de Bitcoin en palabras sencillas.

Esta arquitectura subyacente es el Blockchain y de eso se trata este tutorial. Para entender la arquitectura Blockchain, necesita entender algunas características clave en las que se basa. Así que, comencemos con PKI - Criptografía de Clave Pública.

La criptografía de clave pública o, en pocas palabras, PKI, también se conoce como criptografía asimétrica. Utiliza dos pares de teclas: pública y privada. Una llave es un número binario largo. La clave pública se distribuye en todo el mundo y es verdaderamente pública, como su nombre indica. La clave privada debe ser estrictamente privada y uno nunca debe perderla.

En el caso de Bitcoin, si alguna vez pierde la clave privada de su billetera Bitcoin, todo el contenido de sus billeteras sería instantáneamente vulnerable al robo y antes de que se dé cuenta, todo su dinero (el contenido de su billetera) desaparecería sin ningún mecanismo en el sistema para rastrear quién lo robó - ese es el anonimato en el sistema que mencioné anteriormente.

La PKI cumple dos funciones: la autenticación y la privacidad del mensaje a través del mecanismo de cifrado/descifrado. Ahora explicaré ambas funciones.

Autenticación

Cuando las dos partes intercambian mensajes, es importante establecer una relación de confianza entre el emisor y el receptor. Especialmente, el receptor debe confiar en la fuente del mensaje. Pasando a nuestro escenario anterior (representado en la Figura 1) de Bob enviando algo de dinero a Lisa para la compra de algunos bienes de ella, veamos cómo el PKI construye esta confianza entre Bob y Lisa. Mira la imagen de abajo.

Autenticación

En primer lugar, si Bob quiere enviarle dinero a Lisa, tiene que crear una clave privada/pública propia. Tenga en cuenta que ambas teclas siempre están emparejadas y no puede mezclar las claves privadas y públicas de diferentes individuos o instancias.

Ahora, Bob dice que le está enviando $10 a Lisa. Así que crea un mensaje (un mensaje de texto plano) que contiene la clave pública de Bob (remitente), la clave pública de Lisa (receptora) y la cantidad ($10).

El propósito de esta remesa, como "Quiero comprarte calabazas", también se añade al mensaje. El mensaje completo se firma ahora con la clave privada de Bob. Cuando Lisa reciba este mensaje, utilizará el algoritmo de verificación de firmas de PKI y la clave pública de Bob para asegurarse de que el mensaje proviene de Bob. El funcionamiento de la PKI está fuera del alcance de este tutorial. Se remite al lector interesado a este sitio para un análisis más detallado de la ICP. Esto establece la autenticidad del creador del mensaje. Ahora, veamos la privacidad del mensaje.

Privacidad de los mensajes

Ahora, como Lisa ha recibido su pago, quiere enviar el enlace a su ebook que Bob quiere comprar. Así que Lisa creaba un mensaje y se lo enviaba a Bob como se muestra en la imagen.

Privacidad de los mensajes

La Lisa crea un mensaje como "Aquí está el enlace a mi libro electrónico que usted había solicitado", lo firma con la clave pública de Bob que ha recibido en el mensaje de solicitud de Bob y también encripta el mensaje usando alguna clave secreta que es compartida entre los dos durante el apretón de manos HTTPS.

Ahora, Lisa está segura de que sólo Bob puede decodificar el mensaje usando la clave privada que sólo Bob posee. Además, alguien que intercepte el mensaje no podrá recuperar su contenido porque el contenido está encriptado por una clave secreta que sólo poseen Bob y Alice. Esto garantiza a Lisa que el acceso a su libro electrónico sólo se le concede a Bob.

Habiendo visto las dos características, Autenticación y Privacidad del mensaje, implicadas por PKI, sigamos adelante para ver cómo Bitcoin hace uso de PKI para asegurar el libro de contabilidad público que mencioné en el capítulo "¿Qué es Bitcoin?

Para su conocimiento - Los algoritmos PKI más populares son RSA y ECDSA, Bitcoin utiliza este último.