¿Qué es Blockchain?

A menos que te escondas bajo una piedra, estoy seguro de que has oído hablar de Bitcoins y Blockchain. Después de todo, son los temas favoritos de los medios de comunicación en estos días - las palabras de moda del año. Incluso la gente que nunca ha minado una criptomoneda o entendido cómo funciona, está hablando de ello. Tengo más amigos no técnicos que técnicos. Me han estado molestando durante semanas para explicarles esta nueva palabra de moda. Supongo que hay miles de personas que sienten lo mismo. Y cuando eso sucede, llega el momento de escribir algo a lo que todos pueden apuntar a las otras almas perdidas -ese es el propósito de este post- que cualquier usuario normal de internet entiende.

A diferencia de cualquier otra publicación en internet, en lugar de definir primero la cadena de bloques, entenderemos el problema que resuelve.

Imagina, Juan es tu mejor amigo. Está viajando al extranjero, y en el quinto día de sus vacaciones, te llama y te dice: "Necesito algo de dinero. Me he quedado sin él ".

Respondes, "Enviando algo de inmediato", y cuelgas.

Luego, llamas a tu gerente de cuenta en tu banco y le dices: "Por favor, transfiera $1000 de mi cuenta a la cuenta de Juan".

Tu gerente de cuenta contesta: "Sí, señor".

Abre el registro de cliente, revisa el saldo de tu cuenta para ver si tienes suficiente para transferir $1000 a Juan. Porque eres un hombre rico, tienes mucho, así que hace una entrada en el registro típica de un asiento contable bancario:

Llamas a Juan y le dices: "He transferido el dinero. La próxima vez que vayas a tu banco, puedes retirar los $1000 que acabo de transferir ".

¿Qué acaba de pasar? Tú y Juan confiáis en el banco para manejar el dinero. No hubo movimiento real de billetes físicos para transferir el dinero. Todo lo que se necesitaba era una inscripción. O más precisamente, una entrada en el registro que ni tú ni Juan controlan ni poseen.

Y ese es el problema de los sistemas actuales.

Durante años, hemos dependido de estos intermediarios para que confíen el uno en el otro. Podrías preguntarte, "¿Cuál es el problema dependiendo de ellos?"

El problema es que son singulares en número. Si se desea provocar un caos en la sociedad, todo lo que requiere es que una persona/organización se corrompa, intencionadamente o no intencionadamente.

¿Y si el registro en el que se registró la transacción se incendia?

¿Y si, por error, el gerente de cuenta hubiera escrito $1500 en vez de $1000?

¿Y si lo hizo a propósito?

¿Podría haber un sistema en el que todavía podamos transferir dinero sin necesidad de un banco?

Para responder a estas preguntas, necesitaremos profundizar más y hacernos una pregunta mejor (después de todo, sólo mejores preguntas nos llevan a mejores respuestas).

Piénsalo un segundo, ¿qué significa transferir dinero? Sólo una entrada en el registro. La mejor pregunta sería entonces:

> **¿Hay alguna manera de mantener el registro entre nosotros en lugar de que alguien más lo haga por nosotros?**

Esa es una pregunta que vale la pena explorar. Y la respuesta es lo que ya podrías haber adivinado. La cadena de bloques (blockchain) es la respuesta a la pregunta.

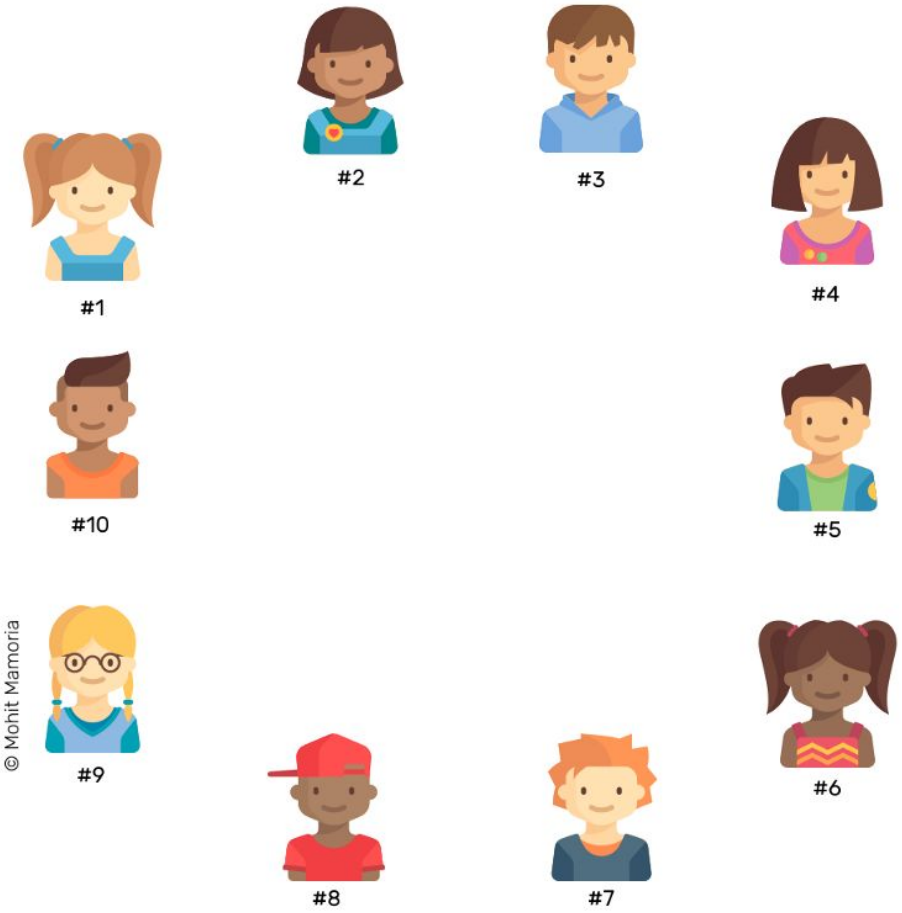
Es un método para mantener ese registro entre nosotros mismos en vez de depender de que alguien lo haga por nosotros.

Ahora, cuando varias preguntas han comenzado a aparecer en tu mente, aprenderemos cómo funciona este registro distribuido.

Sí, pero dime, ¿cómo funciona?

El requisito de este método es que debe haber suficientes personas que no quieran depender de terceros. Sólo entonces este grupo podrá mantener el registro por su cuenta.

¿Cuántos son suficientes? Al menos tres. Para nuestro ejemplo, asumimos que diez individuos quieren renunciar a los bancos o a terceros. De común acuerdo, tienen detalles de las cuentas de los demás todo el tiempo, sin conocer la identidad del otro.



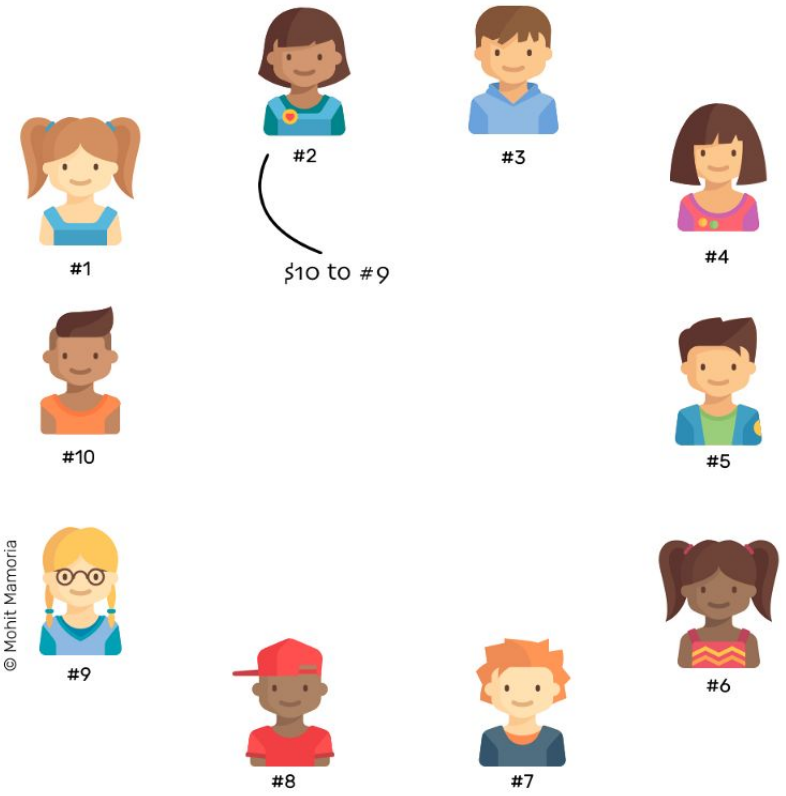
1. Carpeta vacía

Cada uno tiene una carpeta vacía con la que empezar. A medida que progresemos, estos diez individuos seguirán añadiendo páginas a sus carpetas actualmente vacías. Y esta colección de páginas formará el registro que rastrea las transacciones.

2. Cuando ocurre una transacción

A continuación, todos en la red se sientan con una página en blanco y un bolígrafo en sus manos. Todo el mundo está listo para escribir cualquier transacción que ocurra dentro del sistema.

Ahora, si el #2 quiere enviar $10 al #9. Para hacer la transacción, el #2 grita y le dice a todo el mundo,"Quiero transferir $10 al #9". Así que, todos, por favor anoten en sus páginas."



Todo el mundo verifica si #2 tiene saldo suficiente para transferir $10 a #9. Si tiene suficiente saldo, todos anotan la transacción en sus páginas en blanco.

A continuación, se considera que la transacción está completa.

3. Las transacciones continúan sucediendo

A medida que pasa el tiempo, más personas en la red sienten la necesidad de transferir dinero a otros. Siempre que quieren hacer una transacción, lo anuncian a todos los demás.

Tan pronto como una persona escucha el anuncio, lo escribe en su página.

Este ejercicio continúa hasta que todos se quedan sin espacio en la página actual. Suponiendo que una página tiene espacio para registrar diez transacciones, tan pronto como se hace la décima transacción, todo el mundo se queda sin espacio.

Es hora de guardar la página en la carpeta y sacar una nueva página y repetir el proceso desde el paso anterior 2.

4. Cómo quitar la página

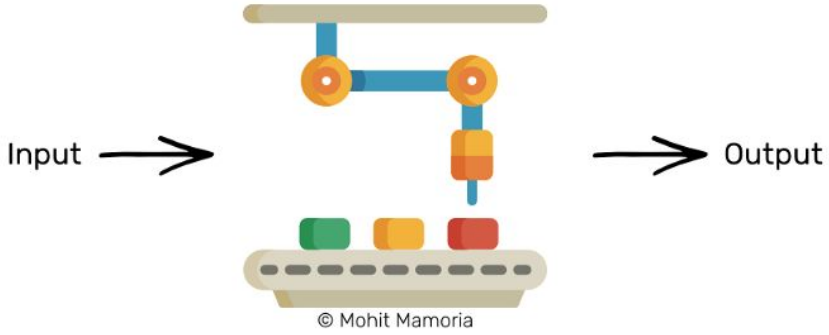
Antes de guardar la página en nuestras carpetas, necesitamos sellarla (minería) con una clave única que todos en la red estén de acuerdo. Al sellarla, nos aseguraremos de que nadie pueda hacer cambios en élla una vez que sus copias hayan sido guardadas en la carpeta de todos - no hoy, ni mañana ni pasado un año. Una vez dentro de la carpeta, ésta permanecerá siempre en la carpeta - sellada. Además, si todos confían en el sello, todos confían en el contenido de la página. Y este sellado de la página es el quid de este método.

Interesante! ¿Cómo sellamos la página entonces?

Antes de saber cómo podemos sellar la página, sabremos cómo funciona el sello, en general. Y como prerrequisito para ello es aprender sobre algo que me gusta llamar…

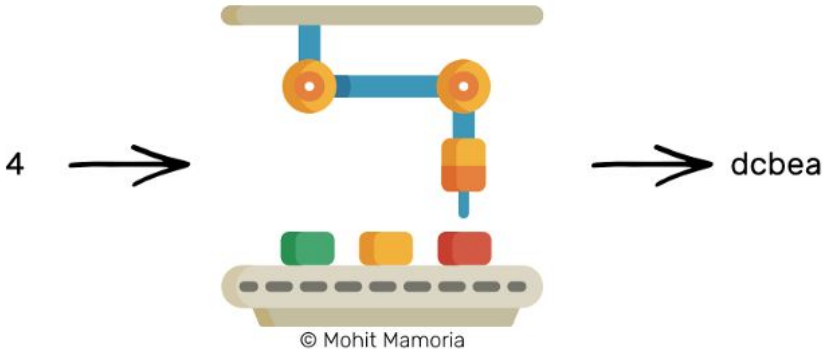
La Máquina Mágica

Imagina una máquina (función *Hash)* rodeada de gruesas paredes. Si envías una caja con algo dentro de ella desde la izquierda, expulsará una caja que contenga algo más.



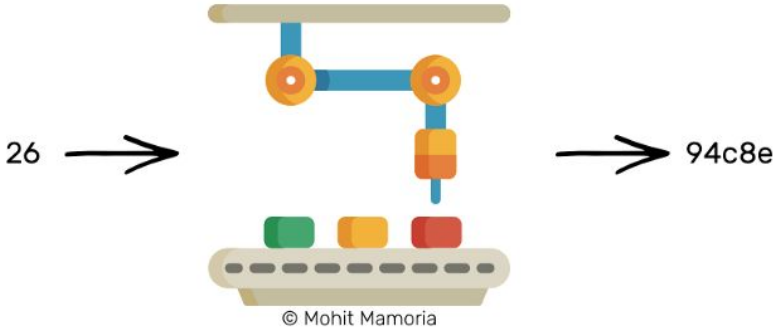
Suponiendo que envías el número 4 dentro de élla desde la izquierda, encontraríamos que escupió la siguiente palabra a su derecha: 'dcbea'.

¿Cómo convirtió el número 4 a esta palabra? Nadie lo sabe. Además, es un proceso irreversible. Dada la palabra 'dcbea', es imposible saber qué alimentaba la máquina a la izquierda. Pero cada vez que alimentas el número 4 a la máquina, siempre escupirá la misma palabra "dcbea".



Dada la palabra' dcbea', es imposible saber qué alimentaba la máquina a la izquierda. Pero cada vez que alimentas el número 4 a la máquina, siempre escupirá la misma palabra "dcbea".

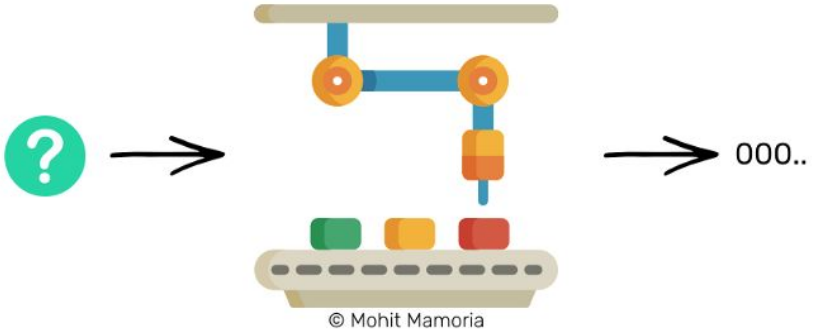
Intentemos enviar un número diferente. ¿Qué tal 26?



Esta vez tenemos' 94c8e'. Interesante! Por lo tanto, las palabras también pueden contener números.

¿Y si te hago la siguiente pregunta ahora:

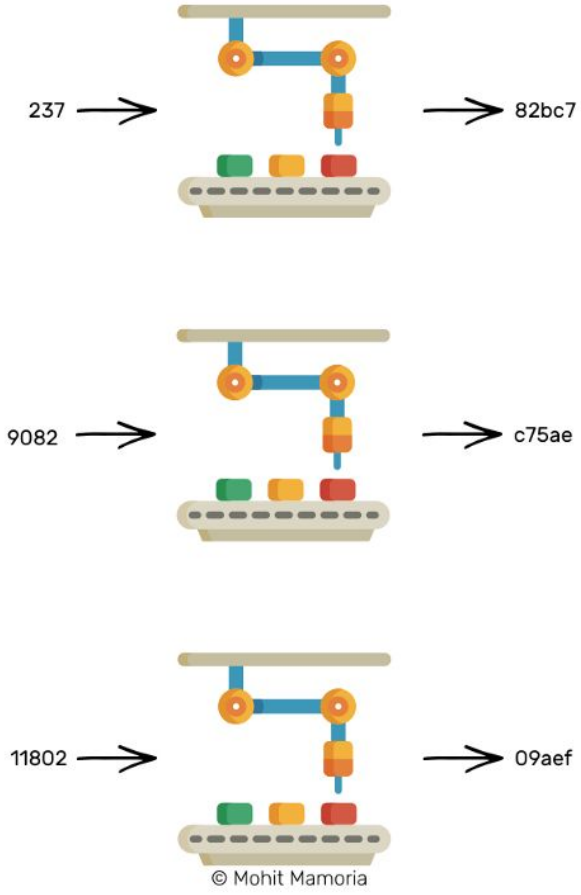
"¿Puedes decirme qué debo enviar desde el lado izquierdo de la máquina para que reciba una palabra que empiece con tres ceros a la derecha? Por ejemplo, 000ab o 00098 o 000fa o cualquier cosa entre los otros."



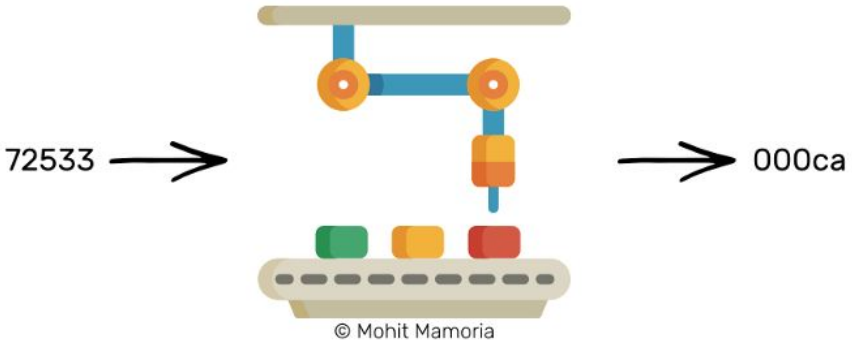
Piensa en la pregunta por un momento.

Te he dicho que la máquina tiene una propiedad que no podemos calcular lo que debemos enviar desde la izquierda después de que recibimos la salida esperada a la derecha. Con tal máquina que se nos ha dado, ¿cómo podemos responder a la pregunta que hice?

Se me ocurre un método. ¿Por qué no intentar cada número del universo uno por uno hasta que tengamos una palabra que empiece con tres ceros?



Siendo optimistas, después de varios miles de intentos, acabaremos con un número que dará el resultado deseado a la derecha.



Es extremadamente difícil calcular la entrada dada la producción. Pero al mismo tiempo, siempre será increíblemente fácil verificar si la entrada prevista produce el resultado requerido. Recuerda que la máquina genera la misma palabra para un número cada vez.

¿Qué tan difícil crees que es la respuesta si te doy un número, digamos 72533, y te hago la pregunta: "¿Este número, cuando se introduce en la máquina, genera una palabra que empieza con tres ceros a la izquierda?"

Todo lo que necesitas hacer es, introducir el número en la máquina y ver lo que conseguiste en el lado derecho de la máquina. Eso es todo.

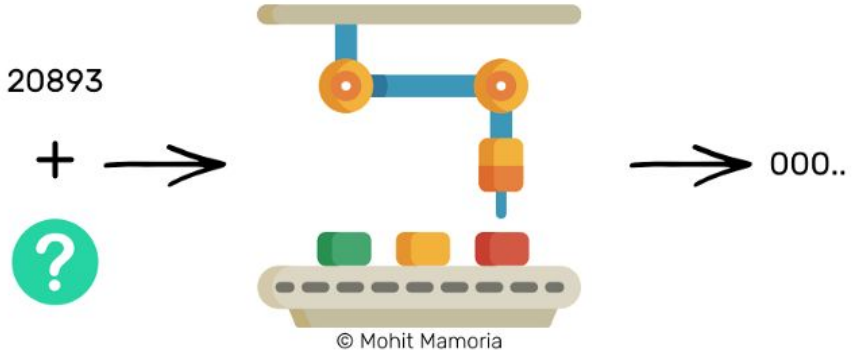
La propiedad más importante de estas máquinas es que, "Dada una salida, es extremadamente difícil calcular la entrada, pero dada la entrada y la salida, es bastante fácil verificar si la entrada conduce a la salida".

Recordaremos esta propiedad de las Máquinas Mágicas (o funciones Hash) a través del resto de este documento:

¿Cómo utilizar estas máquinas para sellar una página?

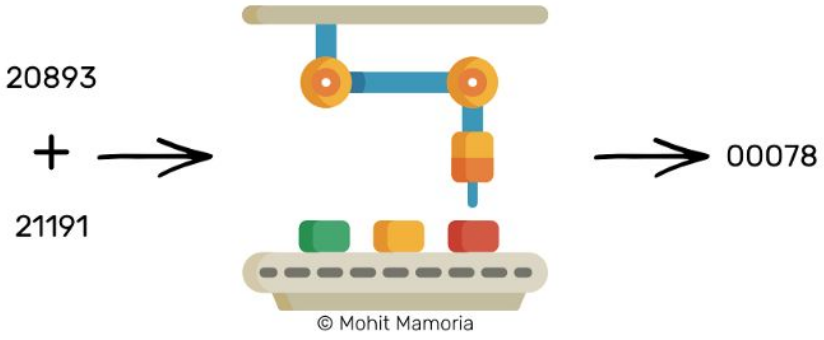
Usaremos esta máquina mágica para generar un sello para nuestra página. Como siempre, empezaremos con una situación imaginaria.

Imagina que te doy dos cajas. La primera caja contiene el número 20893. Yo, entonces, te pregunto: "¿Puedes calcular un número que cuando se suma al número en la primera caja y alimentado a la máquina nos dará una palabra que comienza con tres ceros a la izquierda?"



Esta es una situación similar a la que vimos anteriormente y hemos aprendido que la única manera de calcular tal número es probando cada número disponible en el universo entero.

Después de varios miles de intentos, encontraremos un número, digamos 21191, que cuando se añade a 20893 (es decir, 21191 + 20893 = 42084) y alimentado a la máquina, dará una palabra que satisfaga nuestros requisitos.



En tal caso, este número, 21191 se convierte en el sello para el número 20893. Supongamos que hay una página con el número 20893 escrito en ella. Para sellar esa página (nadie puede cambiar el contenido de la misma), pondremos una placa con la etiqueta '21191' encima. Tan pronto como el número de precinto (es decir, 21191) esté pegado en la página, la página está sellada.

El número de sellado se llama "Prueba del trabajo", lo que significa que este número es la prueba de que se han hecho esfuerzos para calcularlo.

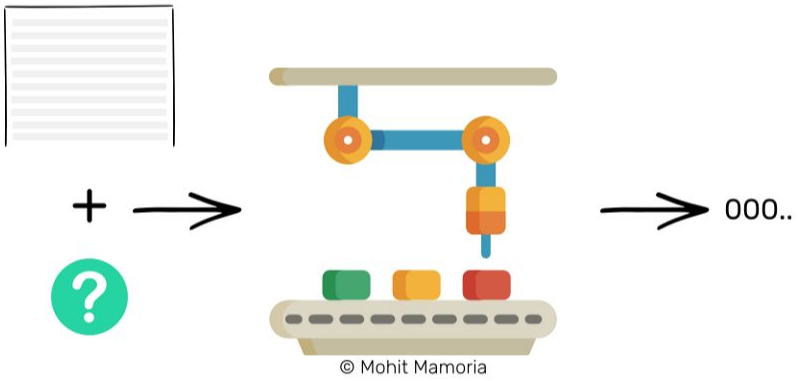
Si alguien quiere verificar si la página ha sido alterada, todo lo que tendría que hacer es añadir el contenido de la página con el número de sellado y alimentar a la máquina mágica.

Si la máquina da una palabra con tres ceros a la izquierda, el contenido no fue tocado. Si la palabra que sale no cumple con nuestros requisitos, podemos tirar la página porque su contenido está comprometido y no sirve de nada. He estado usando la frase 'palabra que comienza con tres ceros a la izquierda' solo como ejemplo. Ilustra cómo funcionan las funciones de Hashing. Los verdaderos desafíos son mucho más complicados que esto.

Utilizaremos un mecanismo de sellado similar para sellar todas nuestras páginas y eventualmente colocarlas en nuestras respectivas carpetas.

Finalmente, sellando nuestra página...

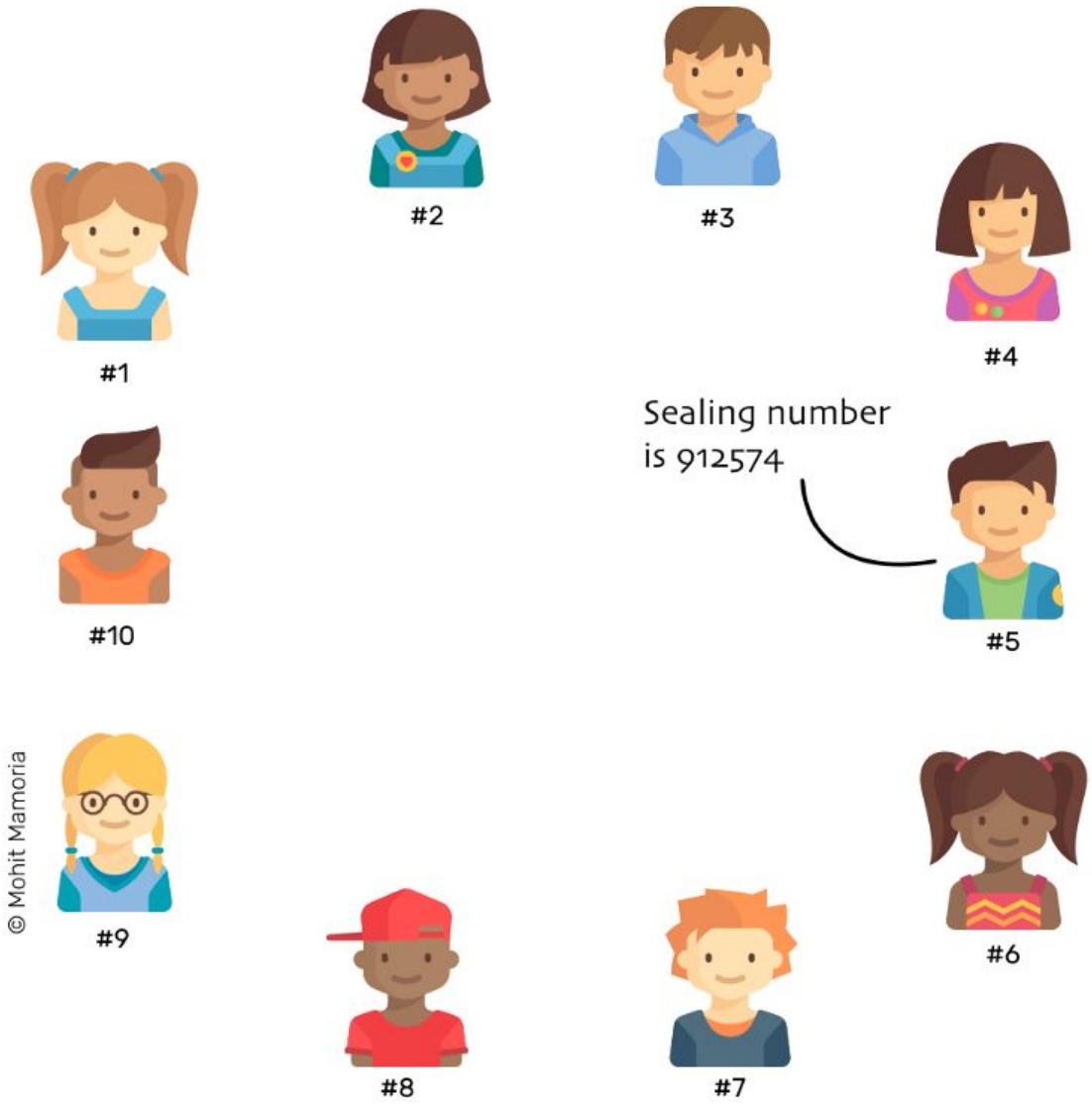
Para sellar nuestra página que contiene las transacciones de la red, necesitaremos calcular un número que cuando se agrega a la lista de transacciones y se alimenta a la máquina, recibimos una palabra que comienza con tres ceros a la derecha.



Una vez que ese número se calcula después de pasar tiempo y electricidad en la máquina, la página se sella con ese número. Si alguna vez, alguien intenta cambiar el contenido de la página, el número de sellado le permitirá a cualquiera verificar la integridad de la página.

Ahora que sabemos acerca de sellar la página, volveremos al tiempo en que habíamos terminado de escribir la décima transacción en la página, y nos quedamos sin espacio para escribir más.

Tan pronto como todos salen de la página para escribir más transacciones, se complacen en calcular el número de sellado de la página para que pueda ser guardado en la carpeta. Todos en la red hacen el cálculo. El primero en la red en descubrir el número de sellado lo anuncia a todos los demás.



Inmediatamente después de escuchar el número de sellado, todos verifican si se obtiene la salida requerida o no. Si es así, todos etiquetan sus páginas con este número y lo guardan en sus carpetas.

Pero, ¿qué pasa si para alguien, digamos #7, el número de sellado que fue anunciado no da la salida requerida? Estos casos no son inusuales. Las posibles razones de esto podrían ser:

- Podrías haber oído mal las transacciones que se anunciaron en la red
- Pudiste haber escrito mal las transacciones que fueron anunciadas en la red
- Podrías haber tratado de engañar o ser deshonesto al escribir transacciones, ya sea para favorecerte o a alguien más en la red

No importa cuál sea la razón, #7 tiene sólo una opción - descartar su página y copiarla de alguien más para que él también pueda ponerla en la carpeta. A menos que no ponga su página en la carpeta, no puede seguir escribiendo más transacciones, lo que le impide ser parte de la red.

Entonces, ¿por qué todo el mundo gasta recursos haciendo el cálculo cuando sabe que alguien más lo calculará y se lo anunciará? ¿Por qué no se sienta y espera el anuncio?

Gran pregunta. Aquí es donde los incentivos entran en escena. Toda persona que sea parte de la cadena de Blockchain es elegible para recibir recompensas. El primero en calcular el número de sellado es recompensado con dinero gratis por sus esfuerzos (ejemplo energía y electricidad de la CPU).

Simplemente imagínate, si #5 calcula el número de sellado de una página, él es recompensado con algo de dinero gratis, digamos $1, que es acuñado. En otras palabras, el saldo de la cuenta #5 se incrementa con $1 sin disminuir el saldo de la cuenta de nadie más.

Así es como Bitcoin entró en existencia. Fue la primera moneda que se negoció en una cadena de bloques (es decir, el registros distribuidos). Y a cambio, para mantener los esfuerzos en la red, la gente recibió Bitcoins.

Cuando hay suficiente gente que posee Bitcoins, crecen en valor, haciendo que otras personas quieran Bitcoins; haciendo que Bitcoins crezca aún más en valor; haciendo que aún más gente quiera Bitcoins; haciéndolos crecer en valor aún más; y así sucesivamente.

Y una vez que todos guardan la página en sus carpetas, sacan una nueva página en blanco y repiten todo el proceso de nuevo, haciéndolo para siempre. Piensa en una sola página como un “bloque de transacciones” y la carpeta como la “cadena de páginas” (Blocks), por lo tanto, convirtiéndola en una “Cadena de Bloques”.

Y así, es como funciona Blockchain.

Excepto que hay una pequeña cosa que no te dije. Aún así.

Imagina que ya hay cinco páginas en la carpeta - todas selladas con un número de sellado. ¿Qué pasa si vuelvo a la segunda página y modifico una transacción para favorecerme? El número de sellado permitirá a cualquiera detectar la inconsistencia en las transacciones, ¿verdad? ¿Qué pasa si sigo adelante y calculo un nuevo

número de sellado también para las transacciones modificadas y etiqueto la página con eso en su lugar?

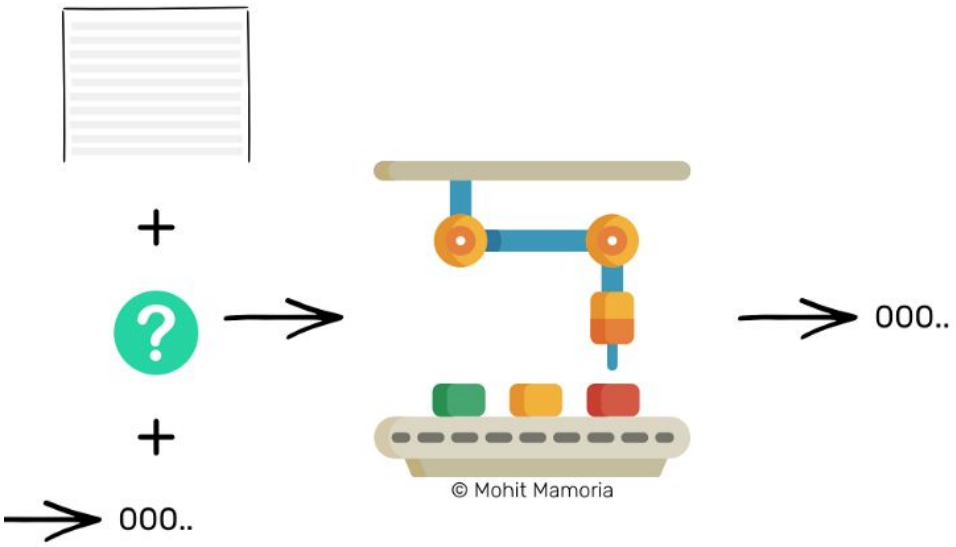
Para evitar este problema de que alguien vuelva atrás y modifique una página (bloque) así como el número de sellado, hay un pequeño giro en la forma de calcular el número de sellado.

Protección de las modificaciones de los números de sellado

¿Recuerdas cuando te dije que te había dado dos cajas - una conteniendo el número 20893 y otra vacía para que calculases? En realidad, para calcular el número de sellado en una cadena en bloque, en lugar de dos cajas, hay tres: dos prellenadas y una a calcular.

Y cuando el contenido de las tres cajas se añade y alimenta a la máquina, la respuesta que sale del lado derecho debe cumplir las condiciones requeridas.

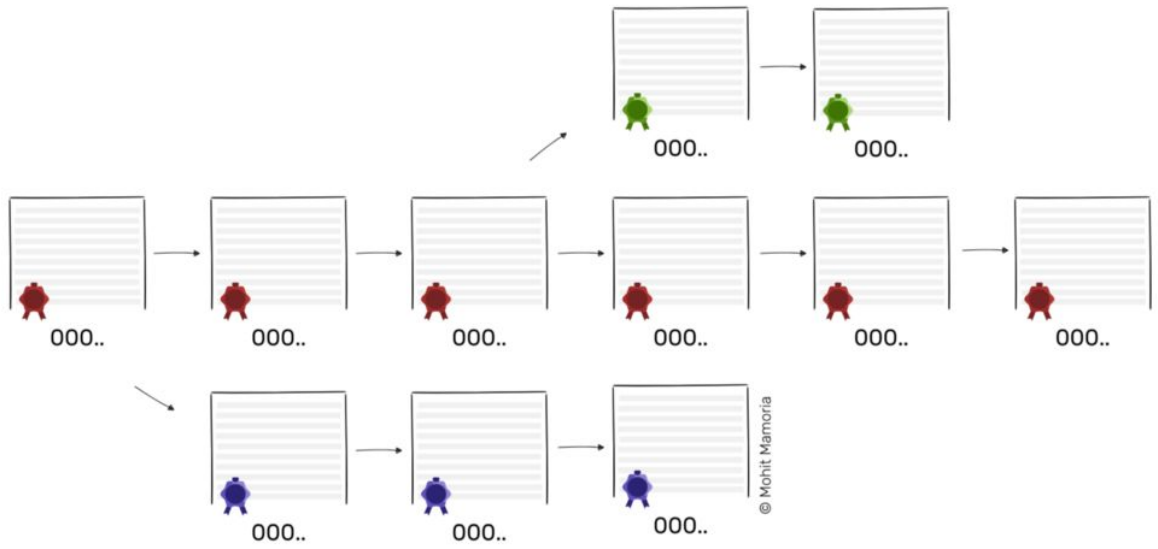
Ya sabemos que una caja contiene la lista de transacciones y otra caja contendrá el número de sellado. La tercera caja contiene la salida de la máquina mágica para la página anterior.



Con este pequeño truco, nos hemos asegurado de que cada página depende de su página anterior. Por lo tanto, si alguien tiene que modificar una página histórica, también tendría que cambiar el contenido y el número de sellado de todas las páginas después de eso, para mantener la cadena coherente.

Si un individuo, de los diez que imaginamos al principio, intenta hacer trampa y modificar el contenido de la cadena de bloques (la carpeta que contiene las páginas con la lista de transacciones), tendría que ajustar varias páginas y también calcular los nuevos números de sellado para todas esas páginas. Sabemos lo difícil que es calcular los números de sellado. Por lo tanto, un tipo deshonesto en la cadena no puede vencer a los nueve tipos honestos.

Lo que sucederá es que, desde la página que el tipo deshonesto trata de engañar, estaría creando otra cadena en la red, pero esa cadena nunca podría alcanzar a la cadena honesta - simplemente porque los esfuerzos y la velocidad de un tipo no pueden superar los esfuerzos acumulativos y la velocidad de nueve. Por lo tanto, garantizar que la cadena más larga de una red es la cadena honesta.



Cuando te dije que un tipo deshonesto no puede vencer a nueve hombres honestos, ¿te sonó algo en la cabeza?

¿Y si en vez de uno, seis mineros se vuelven deshonestos?

En ese caso, el protocolo se quedará sin efecto. Y se conoce como "Ataque 51 %". Si la mayoría de los individuos en la red decide volverse deshonesto y engañar al resto de la red, el protocolo fallará en su propósito.

Y esa es la única razón vulnerable por la que los Blockchains podrían colapsar si alguna vez lo hacen. Es poco probable que suceda, pero todos debemos conocer los puntos vulnerables del sistema. Se basa en la suposición de que la mayoría de la gente es siempre honesta.

https://hackernoon.com/wtf-is-the-blockchain-1da89ba19348