JOSE ZARATE SOUSA
JORGE ZARATE SOUSA

La Blockchain

“El algoritmo de la confianza”

STAMPING.IO

JOSE ZARATE SOUSA
JORGE ZARATE SOUSA

La Blockchain
"El Algoritmo de la confianza"

Auspiciado por:

www.stamping.io

La Blockchain – El Algoritmo de la confianza
Primera Edición, Lima, agosto del 2019.

Editado por "El Gambito"
www.elgambito.com
ISBN: 9781686012037
Sello: Independently published
Edición: 1

Registro de propiedad intelectual en Leftherian.com:
Blockchain id: 5f72c4db5c7a9dcc2b9110882e23073a47f1205c

Código QR generado por Registrado.org

Centro Empresarial El Trigal
Los Antares 320, Of. 501 Torre A
Santiago de Surco,
Lima – Perú
Teléfono: (511) 2418343

Agradecimientos

Gracias Mathias, Samantha y Estéfano por darnos la motivación para que en veinte años, jamás hayamos dejado de luchar.

Gracias Andrea y Mario por inspirarnos a crear Stamping.io

Dedicatoria

Este libro se lo dedicamos a Satoshi, donde quiera que viva,
si es que aún existe.

Notas de los Autor

En veinte años de empresario en el rubro de tecnología, jamás había conocido una tecnología que haya motivado a tantas personas, de distintas profesionales, a hablar de ella. Largamente, la Blockchain ha superado al Business Intelligence e incluso a lo que en su momento fue el mismo lanzamiento de la Internet.

En un mundo donde la corrupción, los fraudes electrónicos, el ciber-delito u otras amenazas a la defensa de la verdad, la Blockchain llega para proponer una solución ante la falta de confianza en la sociedad, sobre todo cuando compromete el dinero o algún activo de valor.

Desde el 2016 vengo desarrollando una plataforma de registro de evidencias digitales y tokenización de activos no fungibles llamada Stamping.io. Esta herramienta ha permitido que muchos profesionales sin en conocimiento técnico en: criptografía, redes peer2peer, cifrados de datos u otros que permitan crear activos digitales seguros para demostrar su existencia y transferencia de propiedad en un momento del tiempo. Te invito a conocerlo y ver toda su potencialidad. Este libro que demostrará que solo diez minutos te separa de usar la Blockchain.

¡Bienvenido!

Escanee este código QR y registre tu libro. Así podré compartirte información de nuevas actualizaciones, nuevas ediciones, invitarte a conferencias virtuales y presenciales, además deseo enviarte un autógrafo virtual que estará registrado en la Blockchain.

Contenido

Introducción

Un día te encuentras paseando por un parque y de pronto vez caer del cielo un pequeño meteorito en pleno centro de la calle; impresionado por lo que estás viendo, gritas muy fuerte para llamar la atención de la gente que se encuentra alrededor. A todos los seres humanos nuestra lógica nos hace creer que necesitamos avisarles a otras personas con el objetivo de que nos ayuden a respaldar la verdad cuando sea cuestionada.

Estarás de acuerdo conmigo que para demostrar la existencia de algo en el futuro, es necesario contar con testigos o pruebas que nos ayuden a demostrarlo, en algún momento nuestra palabra no será suficiente para convencer de la existencia de algo, sobre todo a personas desconocidas.

La veracidad de un hecho podrá ser comprobado cuando se cuente con pruebas suficientes para demostrar su existencia en un momento del tiempo, justamente los testigos son quienes te ayudarán a respaldarlo; a pesar que el hecho es difícil de creer.

Si al ver el meteorito no gritarás lo suficientemente fuerte como para llamar a atención del público que se encuentra cercano a ti, no podrás contar con los testigos necesarios, esos testigos que te ayudarán a convencer a otras personas de lo que ocurrió. Imagínate que dado por el bullicio, es probable que otras personas

levanten la mirada para observar lo que estas anunciado. Minutos más tarde, esas personas podrían contar "su versión" de lo sucedido, probablemente algunos narren una historia similar a esta:

"Desde el cielo vi caer una enorme piedra incandescente que incendió el centro del parque"

Pero, es probable que otras personas que sólo alcanzaron a ver el incendio o sólo escucharon el sonido de la explosión, tengan una versión diferente de lo que en realidad sucedido. Todos los testigos no registran la misma versión de la verdad, ya que tienen una perspectiva distinta del hecho ocurrido; sin embargo, es probable que ninguno de los testigos esté mintiendo, al menos intencionalmente.

¿Cómo se puede confirmar lo que realmente ocurrió?

Para comprobar la veracidad de un hecho se requiere contar con pruebas certeras de su existencia usando la mayor cantidad de testigos que te ayuden a respaldarla. Si tu versión de la verdad se basa en la historia contada por unas cuantas personas, alguien podría cuestionarla, considerando que existe la posibilidad que algunos de ellos se hayan puesto intencionalmente de acuerdo para mentir pero, cuando más testigos coinciden con la misma versión de la verdad la confianza se restablece.

Al contar con dos o más versiones sobre un mismo hecho, es lógico es pensar que la mayoría tiene la razón. En muchas ocasiones habrás comprobado que "la verdad nunca es absoluta", siempre hay distintas versiones de la verdad de un hecho, lo que

obliga a realizar un consenso entre todos los testigos involucrados, para que de alguna manera se decida cuál será "la verdad". Incluso cuando se condena a un asesino, en la mayoría de los casos, el culpable niega lo sucedido, pero un juez, usando las pruebas que se presentan, demuestran su culpabilidad lo declara culpable.

¿Cuántos testigos son necesarios para brindar la confianza certera de que algo realmente sucedió?

En realidad, no existen una cantidad mínima de testigos para obligar a que se confié en una versión de la verdad pero, amigo lector, estarás de acuerdo que cuando más testigos respalden un hecho, será mejor.

"Es probable que en algunos casos los testigos mientan o se pongan de acuerdo para mentir en conjunto con el deshonesto propósito de beneficiar a alguien"

También suele ocurrir que la confianza en algo, no siempre se basa en la cantidad de testigos que la respalden, a veces, un solo testigo puede ser suficiente para confiar en su versión de la verdad, incluso así discrepe del resto de testigos.

A veces es muy difícil confiar en una versión de la verdad cuando esta beneficia directamente a alguien, cuando ese beneficiario es el único testigo y no puede ser comprobada la veracidad de su versión. Veamos un ejemplo:

"Un grupo de amigos deciden hacer una colecta de dinero con la finalidad que al fin de mes se haga un sorteo, el que gane se llevará

el dinero. Uno de ellos asegura haber hecho el sorteo en su casa y como resultado él es el ganador."

¿El resto de participantes, creería esa versión de la verdad?

Cuando la verdad beneficia directamente a uno de los participantes y a la vez el beneficiario es el único testigo, es común que el resto del grupo dude de la honestidad y veracidad de los resultados; por lo que terminarán solicitando una demostración de la transparencia del sorteo, con el propósito de aceptar al beneficiario como el verdadero ganador.

Estarás de acuerdo conmigo que la mejor opción para brindar la transparencia de un sorteo, es hacerla en presencia de un grupo o de todos los participantes, donde cada uno hace el rol de veedor o testigo del resultado. Asegurando de esta forma que el sorteo se realizó en forma justa, y que efectivamente la suerte beneficio a alguien en particular. Con la participación de los testigos que den fe de la veracidad del sorteo, el resultado no será cuestionado y es altamente probable que todos los participantes acepten por consenso al ganador.

Justamente, esta es la forma como funciona la *Blockchain* para brindar la confianza que requieren las empresas o personas necesitan para respaldar un hecho que tiene valor para los participantes. Las redes Blockchain llevan un registro compartido entre un colectivo de testigos digitales, conformado por decenas, cientos o miles de ordenadores que den fe que algo se ocurrió en un momento del tiempo (o al menos que se registró o se realizó) y que estos registros no han sido ni serán adulterados, por nadie jamás.

La aparición de la tecnología Blockchain es probablemente el cambio tecnológico más disruptivo que ha ocurrido en los últimos años. Pero, ¿por qué está teniendo un impacto mediático tan importante? Eso lo descubriremos durante el desarrollo de todo el libro. ¡No perdamos más tiempo! Te invito a aprender a usar la *Blockchain*, la tecnología que se ha convertido en la siguiente gran cosa inventada por el ser humano, que solo es comparable con el descubrimiento de la imprenta o del internet.

Capítulo 1
Fundamentos de la Blockchain

En los últimos años se ha escuchado y leído mucho acerca de esta novedosa arquitectura llamada: "*La Blockchain*", algunos la llaman *tecnología*, otros dicen que solo se trata de una *técnica de almacenamiento* o plataforma de *comunicaciones de redes* entre pares. ¡No importa!, para nosotros es *la Blockchain*.

Cuando alguien sube a un avión y mira por la ventana descubre que su ciudad, su país y el mundo son realmente grandes. Estamos poblados por muchas personas, y millones de ellas no se conocen entre sí. Las empresas y las personas tendrán que hacer negocios, contratarse o intercambiar valor entre ellas aun sin que tengan que confiar entre ellas, ¿Cómo se puede lograr hacer ese intercambio de productos y/o dinero, si muchas de esas personas no se conocen?

La Blockchain permite escribir entradas en un registro inmutable y público, donde una comunidad de usuarios interesados podrán controlar y validar que nadie modifique y/o elimine la información. Una vez que la información se guarda en la Blockchain nade podrá eliminarla nunca jamás.

La Blockchain está compuesta por una red de nodos, cada uno registra las transacciones en forma independiente, una vez que todos la validen y la acepten, se va a convertir en un registro oficial y nadie lo podrá modificar. Para darle mayor seguridad, por lo general la Blockchain utiliza técnicas de criptografía para resguardar la confidencialidad y autenticidad de la información *- más adelante hablaremos de este punto -*.

Para muchos innovadores que están utilizando esta tecnología, definen a la Blockchain o cadena de bloques como una gran base de datos abierta, pública, y descentralizada, donde los datos se encuentran distribuidos (replicados) entre varios ordenadores. Cada uno de los ordenadores mantiene una copia fiel de todos los registros en forma segura, sirviendo cada uno de ellos como un testigo digital; por lo tanto, todos cuentan con la misma información y nadie puede negar su existencia.

La red se crea conectado diferentes equipos que son conocidos como *nodos*. Ninguno gobierna la red, nadie tiene el control del acceso, nadie es dueño de la verdad, en otras palabras, es una red descentralizada y gobernada por el consenso de todos los participantes. Esta arquitectura permite que la información se registre en varios lugares al mismo tiempo y en forma confiable.

Los pasos para ejecutar la red son los siguientes[1]:

1) Las nuevas transacciones se transmiten en simultáneo a todos los nodos.
2) Cada nodo recopila nuevas transacciones en un bloque.

[1] Basado en el white paper de Bitcoin: A Peer-to-Peer Electronic Cash System by Satoshi Nakamoto

3) Cada nodo trabaja para encontrar una prueba de trabajo difícil para su bloque.
4) Cuando un nodo encuentra una prueba de trabajo, transmite el bloque a todos los nodos.
5) Los nodos aceptan el bloque solo si todas las transacciones en él son válidas y no se han gastado.
6) Los nodos expresan su aceptación del bloque trabajando en la creación del siguiente bloque en la cadena, utilizando el hash del bloque aceptado como el hash anterior.

Los nodos siempre consideran que la cadena más larga es la correcta y seguirá trabajando en extendiéndolo Si dos nodos transmiten versiones diferentes del siguiente bloque simultáneamente, algunos los nodos pueden recibir uno u otro primero. En ese caso, trabajan en el primero que recibieron, pero guarde la otra rama en caso de que se alargue. El empate se romperá cuando se encuentre la próxima prueba de trabajo y una rama se alargue; los nodos que estaban trabajando en el otro la rama cambiarán a la más larga.

Dado que cualquiera de los participantes puede agregar un nodo a la red Blockchain se dice que es una red P2P o red de pares que permite almacenar "activos digitales o tokens" que tienen valor para todos los participantes de la red. Si están pensando es participar dentro de una red Blockchain, lo ideal es que todos los participantes que intercambian información cuenten con un nodo interconectado a la red; sin embargo, por restricciones tecnológica y/o económicas, alguno podría utilizar el nodo de alguno de los miembros de la red para endosar o consultar alguna transacción.

Una de las ventajas más rescatable de la Blockchain es la posibilidad de "descentralizar la información", que evita contar

con instituciones que realizan funciones de intermediación en las transacciones que realizan varios participantes, siendo su único atributo de valor: *"Brindarles confianza"*.

La seguridad de una Blockchain se alcanza dado a que los registros se encuentran "firmados" para proteger la autenticidad y en algunos casos los datos podrían estar "cifrados" para proteger la privacidad de la información. Por estas características, una cadena de bloques no puede ser modificada por algún participante, para hacerlo, solo tiene la opción de "netearlo"; es decir, se debe crear una nueva transacción que revierta a la anterior, dejando registrada la trazabilidad del hecho.

La red hace uso de varios tipos de criptografía (Hashing, Cifrado de datos, Firmas asimétricas, firmas a ciega, etc.) convirtiéndose en una forma muy seguridad para almacenar la información, además su característica de almacenamiento entrelazado por bloques formando una cadena, lo hace inmutable.

La Blockchain es inmutable, toda la información registrada en este gran libro contable, técnicamente no existe la forma de modificar o borrar los datos. Todos los registros se encuentran dentro de un bloque, y a la vez el bloque se entrelaza con el bloque anterior y con el bloque siguiente, por lo que al cambiar un dato en un bloque toda la cadena se rompería. Esta forma de almacenar los registros dentro de esta base de datos distribuida hizo que se le diera el nombre de cadena de bloques.

No existe una única red Blockchain en el mundo, sino que se pueden crear tantas como se necesiten, incluso hay muchas empresas que pertenecen a varias Blockchain, o como el caso de

Stamping.io que es una plataforma multi-ledger, es decir, a pesar de contar con su propia red, también registra la información en otras redes a la vez como: Lacchain, Bitcoin, Roster, Ethereum o Evidenchain.

Ciertos especialistas en ciencias de la computación consideran que "la blockchain" cambiará la forma de realizar transferencias de valor en el mundo; además, muchos de ellos están convencidos que la Blockchain es una nueva forma de usar el Internet, que permite darle valor a los registros. Estamos entrando a nueva ola tecnológica, donde los servidores dejarán de almacenar y compartir contenidos entre sus diferentes usuarios para dedicarse a intercambiar "activos de valor", activos que serán replicados entre muchos servidores, en tiempo casi real. Por lo que algunos le han apodado a la Blockchain como el "Internet del Valor".

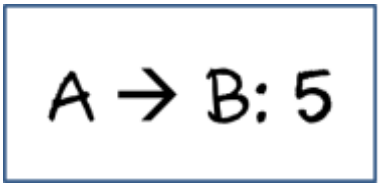
Dinámica grupal 1: La contabilidad distribuida

Objetivo: Demostrar cómo funciona cada nodo dentro de una red Blockchain

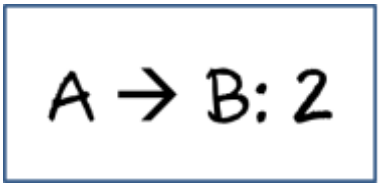
Pasos

El profesor deberá contar con 2 papeles y deberá apuntar lo siguiente:

- Papel 1:
  A → B: 5 (Significa que Ana le transfiere a Bruno 5 monedas digitales)



- Papel 2:
  A → B: 2 (Significa que Ana le transfiere a Bruno 2 monedas digitales)



Cada uno de los alumnos del salón deberá marcar una hoja de papel de la siguiente manera:

Hoja de Trabajo

Ejercicio: 1

STAMPING.IO

Bloque:____	Bloque:____	Bloque:____	Bloque:____
Transacciones	**Transacciones**	**Transacciones**	**Transacciones**
De: a: # Balance	De: a: # Balance	De: a: # Balance	De: a: # Balance
Saldos	**Saldos**	**Saldos**	**Saldos**
A:	A:	A:	A:
B:	B:	B:	B:
C:	C:	C:	C:
Confirmaciones:____	Confirmaciones:____	Confirmaciones:____	Confirmaciones:____

Los alumnos deberán copiar lo que el profesor dicte. Dado que el objetivo de esta dinámica es simular como funciona los nodos de una Blockchain se necesita al menos la participación de 3 alumnos.

Para este ejercicio se asume que solo existen 3 cuentas:

Ana (A), Bruno (B) y Carlos (C), además que al comienzo nadie tiene saldo en su cuenta, en ese momento el profesor comenzará dictando las transacciones del primer bloque:

- ➔ A: 10 (Ana compra 10)

- ➔ B: 15 (Bruno compra 15)

B ➔ C: 5 (Bruno transfiere 5 a Carlos)

Tarea 1: El Endose

Calcular el saldo actual de Ana, Bruno y Carlos.

Repuesta 1.1: Ana: 10 Bruno: 10 Carlos: 5

Se acaba de demostrar cómo funciona el proceso de endose de transacciones, donde cada uno de los participantes interesados está llevando por separado un registro de las transacciones, evitando que cualquiera de los alumnos cambie o modifique los datos; por lo tanto, se mantiene una base de datos única pero a la vez distribuida entre todos.

Tarea 2: El consenso

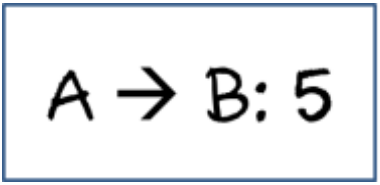
El profesor deberá consultar a todos los alumnos el resultado del saldo de A, B y C y verificar que todos tengan el mismo valor, si alguien ha realizado un cálculo errado, el profesor deberá indicarle que lo modifique, ya que la mayoría es quien determina cual es la verdad.

Para demostrar esta funcionalidad el profesor anunciará que el bloque 1 ha sido creado, ya que tiene N confirmaciones (La misma cantidad de alumnos) y pasará a indicar que se van a realizar nuevas transacciones que deberán registrarse en el bloque Nro. 2.

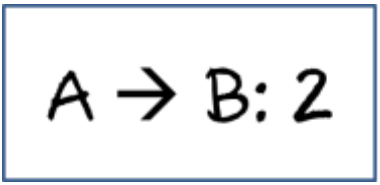
C ➔ A: 3

B➔ A: 5

El profesor saca la ficha 1 de su bolsillo y se la entrega a uno de los alumnos:



El resto va a realizar lo que dice la segunda ficha.



Luego se solicita que todos calculen el saldo, es lógico que el alumno que recibió la ficha1 tenga el resultado errado. Se deberá hacer una votación de los resultados y se establece lo que la mayoría ha calculado.

Se corrige los resultado del alumno errado y se procede a cerrar el segundo bloque con las confirmaciones equivalente a todos los alumnos menos uno, el alumno que había errado dado que había sido engañado por un general bizantino que le entregó la ficha 1.

El problema de los generales bizantinos

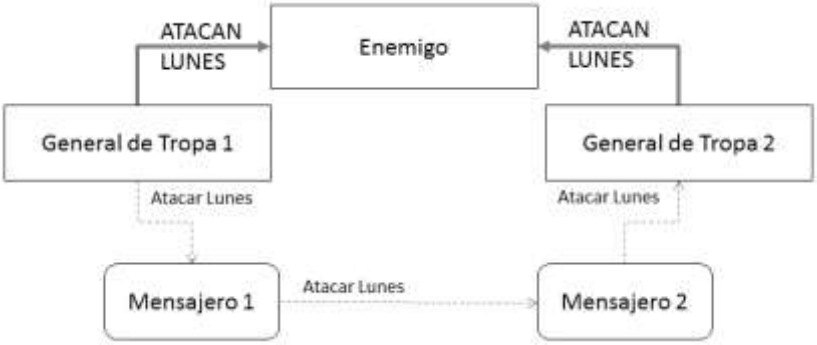
Imagina que hay un grupo de generales, cada uno posee el control del ejército bizantino. Van a atacar una ciudad y tomar el control, pero para eso, tendrán que decidir cómo atacar. Puedes pensar que es algo fácil. Sin embargo hay una ligera dificultad.

Los generales sólo pueden comunicarse por medio de un mensajero, y algunos generales traidores intentarán sabotear el ataque. Pueden enviar información falsa a través del mensajero, o el mismo mensajero puede convertirse en el enemigo. El mensajero podría sabotear intencionalmente haciendo entrega de información errónea o alguien podría obligarlo a decir una mentira.

Es por eso que el problema debe ser tratado con cautela. En primer lugar, de alguna forma tenemos que hacer que cada general tome la misma decisión y, en segundo lugar, asegurarnos de que incluso el menor número de traidores no pueda hacer que la misión fracase.

Imaginemos que hay 2 tropas de solados que están al lado de la ciudad enemiga. La defensa de la ciudad enemiga es suficientemente fuerte como para vencer a cada tropa por separado, pero nunca a las dos tropas a la vez, por lo que el ataque deberá ser en simultáneo y estar bien coordinado.

Cada tropa tiene un general al mando. Cada tropa cuenta con un mensajero para comunicarse entre ellos. El mensajero es un experto soldado que puede rodear la ciudad para ir de un campamento a otro con las órdenes de ataque tratando que el enemigo no lo atrape.



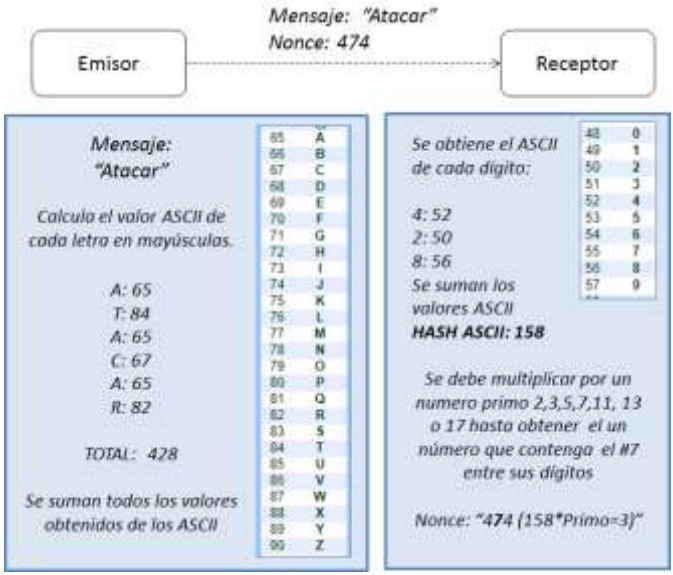
El mensajero de una de las tropas informará al mensaje de la otra tropa que planean atacar, recuerden que para salir victorioso es necesario que ambos ataquen juntos. El mensaje le dice: "El próximo lunes vamos atacar, favor confirmar si es posible" La segunda tropa debe confirmar si se necesita más tiempo para prepararse o de lo contrario también está listo para atacar, en este ejemplo ambos confirmar que atacarán el lunes, al hacerlo juntos saldrán victoriosos.

El problema es que el mensajero podría ser interceptado por el enemigo o simplemente ser un traidor, el mensaje de uno de los mensajeros puede ser modificado y enviado de nuevo haciendo que los dos ejércitos no ataquen de manera sincronizada y por tanto sean vencidos por el ejército enemigo.

Si un mensaje de los generales dice: "Atacar el Jueves", al ser únicamente un mensaje de texto, podría ser modificado con facilidad a "atacar el lunes", por lo que ambas tropas atacarían en días distintos y serían vencidos.

Puede parecerte algo simple; sin embargo, no lo es. Según la investigación, se necesitarían 3n+1 generales para lidiar con n traidores. Tomaría cuatro generales para hacer frente a un solo traidor, lo que hace que sea un poco complicado.

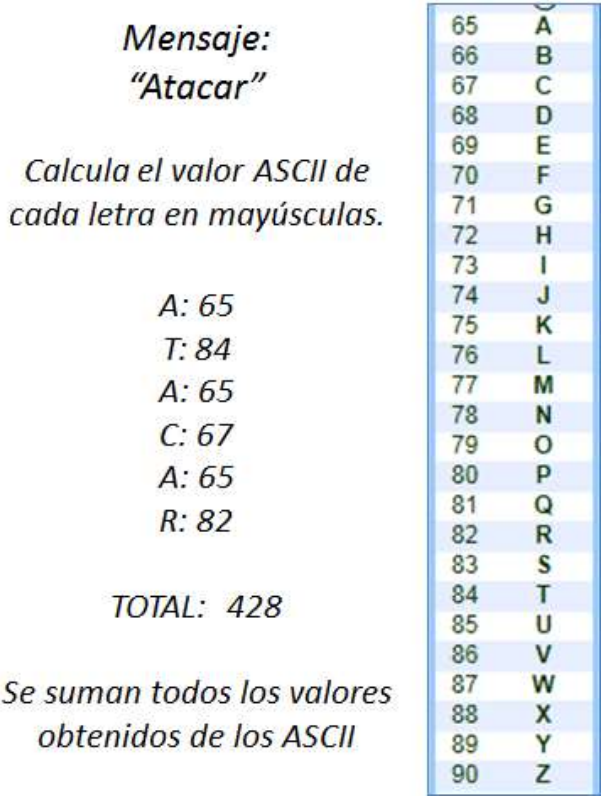
Hay varias formas como la Blockchain resuelve el problema de los generales bizantinos, pero todas se basan en acompañar al mensaje con un valor que sea muy fácil de comprobar pero dificultoso en calcularse, ese valor se llama "nonce".



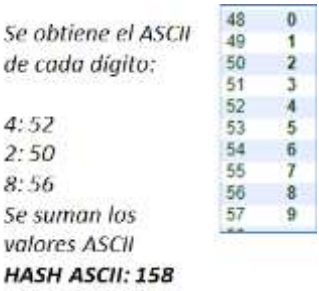
Vamos a hacer el siguiente ejemplo: El mensajero envía un mensaje con el texto "ATACAR", será acompañado de un valor "nonce: 474" que ha sido calculado de la siguiente forma:

Primero se debe obtener el código "Hash ASCII" del texto del mensaje. Ese valor es calculado de la siguiente manera:

Paso 1: Calcular el SUM del código ASCII de cada letra del mensaje. Calculemos el valor ASCII de cada letra que contiene la palabra del mensaje "ATACAR", luego vamos a sumar esos valores:



Paso 2: Se calcula el hash del texto, para encontrarlo se debe colocar el código ASCII de cada número que dio como resultado al sumar los valores ASCII de cada letra del texto:



Paso 3: Se busca un valor *nonce*, que consiste en multiplicar el HASH ASCII con los números primos hasta encontrar un número que tenga al número 7 dentro de sus caracteres.

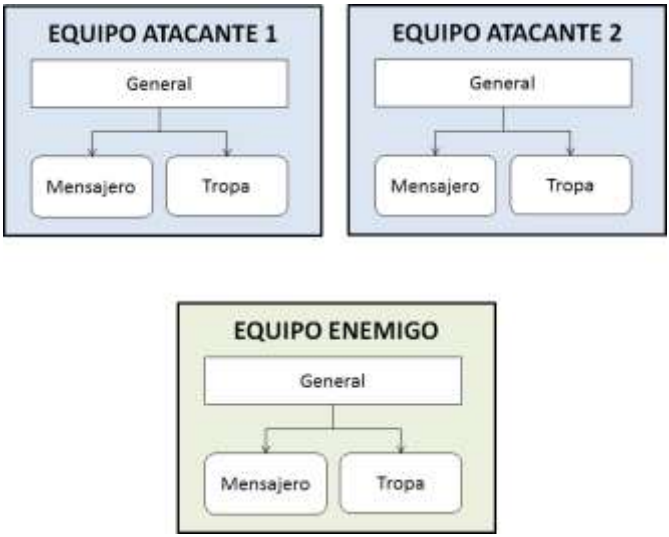
			2	3	5	7	11
Atacar	158	525056	316	474	790	1106	1738

Tenga en cuenta que el algoritmo de Hash ASCII de un texto ha sido inventado por los autores de este libro para fines didácticos y evitar la complejidad de algoritmos complejos como el SHA2 o SHA3 que no es fácilmente calculados a mano en un cuaderno.

Dinámica grupal 2: Atacando a la red

El profesor deberá armar tres equipos, donde los dos de ellos serán los atacantes y uno de ellos será el enemigo.

El ideal de esta actividad es que cada grupo deberá estar compuesto por al menos 3 personas, de contarse con más alumnos, ellos pueden distribuirse equitativamente en cada grupo como tropa, de no contar con muchos participantes se puede armar equipos donde uno de los estudiantes haga más de un rol. Al final cada grupo será organizado de la siguiente manera:



El enemigo puede vencer a cualquiera de los atacantes siempre que ellos no lo ataquen en forma simultáneamente, si es atacado por ambas tropas a la vez, el enemigo será vencido. Por lo tanto, los generales a cargo de las tropas atacantes 1 y 2 deberán ponerse de acuerdo para atacar juntos. Las reglas del juego son las siguientes:

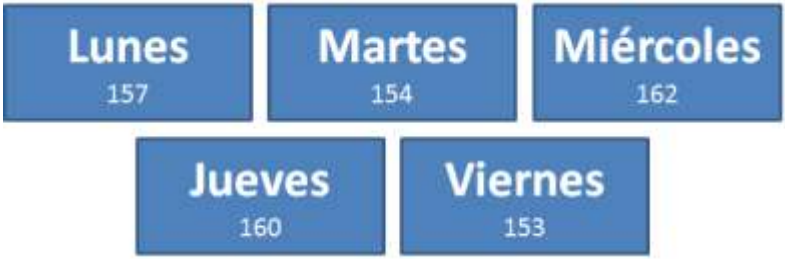
- Los generales no pueden hablar entre ellos, solo pueden enviar mensajes a través del mensajero.
- El mensaje solo contendrá el día en que el "equipo atacante" atacará.

- El mensajero del equipo atacante 1 está obligado a darle el mensaje al equipo enemigo por 30 segundos.
- El equipo enemigo podrá cambiarle el mensaje para confundir al atacante 2, solo tiene 30 segundos para hacerlo, si no es capaz de cambiar el mensaje estará obligado a darle el mismo mensaje que le mostró el mensajero.
- El equipo atacante 2 tiene 30 segundos para determinar si el mensaje que ha recibido es verdadero o falso. Si detecta que es falso se tendrá opción a pedir otro mensaje caso contrario deberá dar la orden de atacar, en ese momento el equipo atacante 1 y 2 mostrarán el día que ordenaron atacar, si ambos días son iguales, el atacante ganó el juego sino acaban de perder.

Instrucciones del Juego

Para que este juego funcione se necesita que previamente el profesor haya creado las siguientes fichas:

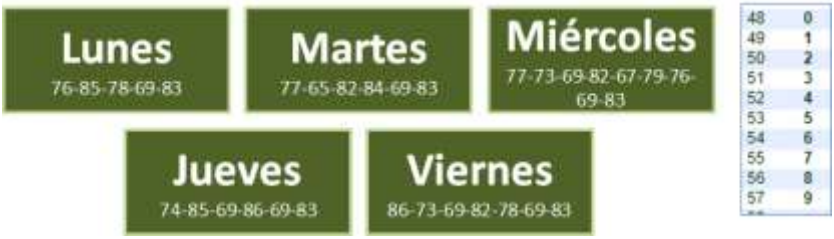
Fichas para el equipo atacante



Cada ficha contiene el nombre de un día de ataca y el código que se encuentra en la parte inferior es el hash ASCII del texto.

El profesor entregará las fichas al general del equipo atacante 1, las fichas están boca abajo y no puede ser vista por nadie, es importarte moverlas para evitar que alguien reconozca la ubicación de cada ficha.

Fichas para el equipo enemigo



Cada ficha contiene el nombre del día de ataque y el código ASCII de cada letra, el profesor entregará estas fichas al general del equipo enemigo, las fichas están boca abajo y no puede ser vista por nadie, es importarte moverlas para evitar que alguien reconozca la ubicación de cada ficha.

Desarrollo del Juego

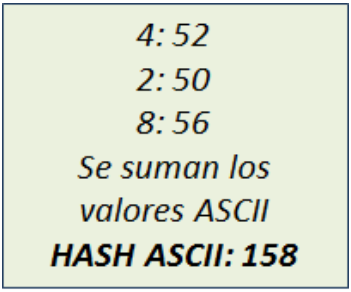
1. El general del equipo atacante 1, deberá seleccionar una de las fichas al azar, recuerde que no puede verla, solo deberá entregárselo al mensajero. Es importante que nadie vea el día que ha seleccionado (ni siquiera el mensajero).
2. El mensajero del equipo atacante 1, deberá entregársela al mensajero del equipo enemigo, quien tampoco podrá ver el mensaje, sin embargo tratará de cambiar el mensaje. Como ya se sabe, solo dispone de 30 segundos. Desde que recibe

la tarjeta, el profesor comenzará a calcular el tiempo. Recuerde que nadie puede ver el mensaje que envió el equipo atacante 1, ni siquiera el mensajero del equipo enemigo.

3. El general del equipo enemigo, toma una ficha al azar, el mensajero deberá calcular el código hash-ASCII del mensaje que ha seleccionado el general del enemigo., por ejemplo, si el mensaje fuera "Atacar", se buscaría el código ASCII de :

4. Luego el mensajero deberá sumar todos los valores, el resultado dará un número de 3 dígitos, los cuales se deben buscar en la tabla ASCII de números y colocar su valor ASCII de cada número, por ejemplo, si el mensaje fuera "Atacar", el resultado de la suma de los códigos ASCII sería 428, se buscaría el código ASCII de cada digito de la siguiente forma:

5. El mensajero deberá sumar los valores ASCII obtenidos, el resultado es:



6. El mensajero deberá calcular el ***nonce***, se obtiene multiplicarlo por los primeros 5 números primos (2,3,5,7,11y13) y verificar cual es el primer valor donde aparece el número 7 entre sus dígitos, por ejemplo, para el HASH ASCII del mensaje Atacar, el valor será 4**7**4:

Mensaje	Hash - ASCII	2	3	5	7	11	13
Atacar	158	316	474	790	1106	1738	2054

7. Una vez que ha terminado de calcular ese valor, deberá quedarse con el mensaje original y entregarle la nueva tarjeta con el día de ataque y además le deberá entregar ese valor en un papel para que el mensajero se lo entregue al equipo atacante 2. Si el tiempo se agota antes de llegar a este paso, el mensajero del equipo atacante 2 podrá darse cuenta que el mensaje ha demorado más de la cuenta y solicitar un nuevo envío por otro canal.
8. El mensajero del equipo atacante 2, deberá recibir el mensaje y verificar que el mensaje es correcto, lo que tiene que hacer es calcular el HASH ASCII del mensaje, luego el valor del *nonce* se divide entre el hash ASCII del mensaje, por ejemplo en el caso del mensaje Atacar, el hash ASCII es 158 y el *nonce* es 474, el mensajero deberá validar que el *nonce* tenga al menos un número 7, de no ser así, sabrá rápidamente que el mensaje es falso, caso contrario deberá comprobarlo haciendo este simple cálculo:

   nonce / hashASCII
   474 / 158 = 3
9. El mensaje deberá obtener un número entero y primo menor o igual a 13, de no ser así, el mensaje es falso.
10. Cuando haya terminado, el general del equipo atacante 2 deberá avisar a todos los participantes que está listo para atacar el día: "Indica el día xxxxx" lee la tarjeta, si ha detectado que el mensaje es incorrecto dado que el resultado no otorga un número primo, deberá indicar "Mensaje Errado".

Esta dinámica que puede realizar con sus compañeros de clase o trabajo, le ayudará a entender la forma como los mensajes son intersectados dentro de una red computacional, siendo importante contar con un mecanismo de validación que permita garantizar la

integridad del mensaje. Recuerde que generar el *nonce* toma mucho más tiempo que validarlo, más adelante veremos cómo se realiza la prueba de trabajo para determinar un *nonce* en algunos tipos de Blockchain, el tiempo que puede tomar es relativo y forma parte de las reglas de validación y tipo de consenso de la Blockchain, por ejemplo en el caso de Stamping.io toma hasta 30 minutos, en caso de Bitcoin aproximadamente 10 minutos.

Las pruebas de esfuerzo o trabajo, tratan de resolver el problema de los generales bizantinos para evitar que alguien mienta, lo que significa que se deberá validar cada cierto tiempo, que todos hayan recibido la misma información.

Tipos de redes Blockchain

Por el tipo de participantes, las Blockchain se clasifican en redes públicas y redes privadas, estas últimas requieren de permisos para conectar un nodo a la red de ahí que también se les conoce como redes permisionadas. En las redes Blockchain, ninguno de los participantes es dueño absoluto de los datos ni esta empoderado con un rol de administrador, por lo que se denomina como una base de datos neutral y democrática entre los participantes. Para garantizar la fiabilidad de los datos, nadie debería tener el poder de votar a otro participante de la red, sin embargo, existen algunas redes Blockchain que cuentan con reglas para gobernar la admisión o expulsión de la red.

Dado que la *Blockchain* ha sido diseñada para que nadie sea administrador ni dueño de los datos, se considera que es un repositorio resistente a la censura. Todos los datos que se almacenen en la cadena de bloques no podrán ser negados (ni su existencia y su integridad) por ninguno de los participantes; esto es debido a que ellos siempre tuvieron una copia de los datos y validaron su existencia cuando se registraron.

La cadena de bloque o *Blockchain* en inglés, se hizo famosa en el 2009 a raíz del lanzamiento de la criptomoneda bitcoin (con b en minúsculas), es muy difícil hablar de Blockchain sin mencionar a las criptomonedas. Este libro está enfocado en el uso de la Blockchain para usos empresariales, como medio de pago, transferencias de activos de valor, registros de propiedad, pruebas de existencia, firmas de documentos o trazabilidad digital; sin explicar cómo funciona bitcoin, jamás se podrá entender cómo se inventó toda esta maravilla. E

Contenido de una Blockchain

Dentro de la *Blockchain* se almacena información que tiene un valor intrínseco entre todos los participantes de la red, a esa información se le conoce como *activo digital*. Se puede registrar cualquier tipo de datos que represente algo de valor, no tiene que ser valorado por todo el mundo, pero si por los participantes de la red. Por ejemplo: dinero o criptomonedas, acciones de participación de la propiedad de una empresa o proyecto, documentos o archivos que fueron creados en un momento del tiempo, o algo que ni siquiera existe en el mundo real. A veces un simple hash (una secuencia limitada de números y caracteres hexadecimales) representa cualquier cosa de valor como: un auto, una mascota, un reclamo, un certificado de estudio, el derecho de propiedad intelectual de una canción o una enorme fortuna (dinero).

Como ya lo hemos mencionado antes, la *Blockchain* contiene internamente una base de datos que está compartida entre todos los equipos que forman parte de la red, dentro de esa base de datos se lleva un libro mayor distribuido (compartido) entre todos los nodos participantes de la red, similar a un grupo de mensajería instantánea, solo que el mensaje que se envía no es tan trivial como un simple saludo a tu grupo de amigos del colegio. Se envía mensajes con valor, que representan la creación o transferencia de la propiedad de algo, en vez de un simple mensaje de saludo como es el caso de telegram o whatsapp; pero lo cierto es, que se parece mucho, ya que de la misma forma en que el mensaje por whatsapp le llega a todos los miembros del grupo, en la Blockchain todos los que participan de la red reciben "el mismo mensaje al mismo tiempo", guardando una copia que les permita comprobar que nadie, absolutamente nadie, pueda negar la existencia en el futuro.

La forma de trabajar es sencilla, desde una aplicación o en forma manual, cualquier usuario puede crear un activo digital o transferir

la propiedad de alguno de esos activos que previamente estaban registrados, solo se debe endosar una transacción en uno de los nodos de la red, al hacerlo, la misma red envía en tiempo real a todos los equipos que se encuentran conectados a la red Blockchain. Como cuando envías un mensaje a tu grupo de amigos en el whatsapp, todos ven el mensaje y todos tienen una copia en cada equipo celular, del mismo modo funciona el envío de mensajes en una red Blockchain, todos los nodos guardan una copia de la existencia y propiedad de los registros, es decir, tienen una contabilidad compartida y conciliada entre todos.

Algunas plataformas Blockchain - *me refiero a los productos de software que algunas empresas o comunidades de desarrolladores están construyendo* - permite tener diferentes canales, es decir, dentro de una misma red se pueden crear diferentes grupos de información y por lo tanto, diferentes contabilidad a pesar de estar conectados a una misma red. Algunos nodos podrían no tener permisos a participar en ciertos canales de la misma red. Esta modalidad es frecuente en las redes Blockchain permisionadas o privadas, también conocidas como DLT.

En el caso de las redes públicas como es el caso de Bitcoin o Ethereum, cuando alguien quiere crear una propia base de datos que lleve el registro de las transacciones de una "nueva criptomoneda" copia el código y crea una nueva red, en estas plataformas no existen canales – *a este copiado se le conoce como bifurcación(fork)* -. Es lógico pensar, que en el caso que alguien haga un fork del código de bitcoin, esos nuevos registros representan a una nueva criptomoneda, a pesar de estar usando el mismo código fuente, los registros dentro de esta nueva Blockchain ya no serían bitcoin, serían cualquier otro activo pero no sería un bitcoin.

La criptomoneda bitcoin solo puede ser manejada en las redes de Blockchain de Bitcoin, hacerlo en otra Blockchain sería simplemente otra criptomoneda, ya que no se podría validar su uso o gasto. De hecho que existen muchas copias del código de bitcoin que se utilizan para hacer pruebas de desarrollos en bitcoin, estas redes se les conoce como testnet, donde funcionan exactamente igual que la red principal de bitcoin (conocida como main net), pero nadie le da ningún valor a esa criptomoneda, puesto que cualquier persona puede crearlas sin ningún control.

Ejercicio:

Cargar monedas a esta dirección: 2NAr4rDnwhTfDnb9ziNpF5JLJTNLFfeoM97

Forma de almacenamiento

Las transacciones dentro de una Blockchain se almacenan en una estructura secuencial, conformado por bloques y ordenados en forma cronológica para evitar errores en la validación de una transacción, por lo que el uso de una máquina de sellado de tiempo es un elemento esencial; sin ello, simplemente la Blockchain no funcionaría.

Los bloques están matemáticamente relacionados entre sí, se utilizan algoritmos de criptografía y firmas asimétricas para asegurar la propiedad, veracidad, integridad y privacidad de los datos, más adelante veremos estos puntos a más detalle.

El problema que resuelve la Blockchain

La Blockchain se usa en un proyecto de alcance mundial por primera vez con la criptomoneda de bitcoin, el propósito era que

esta moneda digital sea usada como un medio de pago confiable, de liquidación "casi rápida" y que sirva como método de pago alterno al sistema financiero actual. Muchos se preguntan, *¿qué tiene que ver la Blockchain con la criptomoneda?*, la respuesta es muy sencilla, se buscaba tener la confianza que nadie pueda crear dinero de la nada ni gastar más dinero del que realmente tiene sin recurrir a un tercero de confianza que lleve la contabilidad del gasto (libro mayor de transacciones de transferencias), veamos cual era el problema que conllevo al uso de la Blockchain en las criptomonedas:

Como ya lo habíamos mencionado, los creados de bitcoin buscaban crear un medio de pago que les permita a las personas transferir dinero de manera sencilla, evitando que no se pueda gastar más dinero que el que se dispone. Evitar el "doble gasto" de un fondo, eso solo podía lograrse llevando un registro de las transacciones realizadas en un libro contable, donde se registre cronológicamente el movimiento que cada persona ha realizado sobre una determinada cuenta. Solo así se podrá saber cuál es el saldo de dinero que cada cuenta dispone. El problema ha sido resuelto por muchos medios de pago como Visa, Mastercard, American Express o las entidades financieras, solo que esta vez se estaba buscando hacerlo sin un intermediario o agente central, es decir, a diferencia de cómo funciona actualmente el sistema financiero, se desea hacer en forma descentralizada. ¡Tremendo reto!

Centralizando las transferencias de valor

Si queremos llevar un registro centralizado de todas las transacciones que cada persona realiza sobre una determinada cuenta que sirva como un mecanismo de control que evité a que

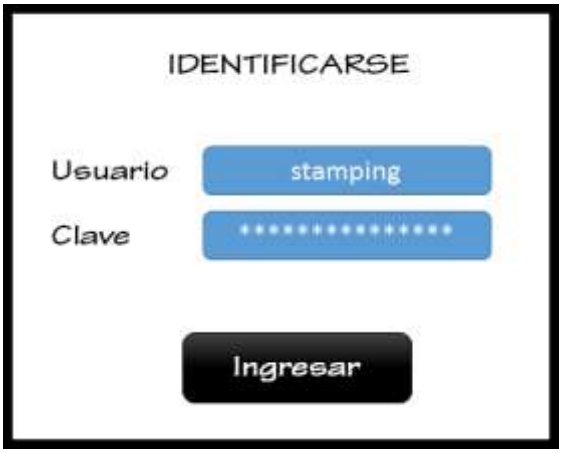
alguien gaste más dinero del que realmente dispone, solo se necesita registrar a cada usuario y cada vez que alguien desee realizar una transferencia, deberá informar a ese agente central para que lleve el control respectivo.

Una forma de hacerlo, sería crear un modelo de autenticación básica, ya sea usando un usuario y contraseña o como lo hacen algunas tarjetas es usando datos que se encuentran en la misma tarjeta (¿qué inseguro verdad?), solo así, el agente central podrá determinar de que cuenta se desea transferir y confirmar que realmente es el dueño de la cuenta (¿salvo si te roban la tarjeta?). No importa si el método no es seguro, el mundo lo ha venido usando hace muchos años para identificarse y autorizar una transferencia de su cuenta a la cuenta de un tercero. El agente central, utiliza este mecanismo para evitar que alguien robe el dinero de otra persona. ¿Crees que está funcionando?

Cuando la transacción se aprueba, el agente central crea un registro contable de donde partida, donde descuenta el saldo del emisor y lo abona en la cuenta del receptor. Si el emisor consulta el saldo de su cuenta, verá que se ha actualizado, evitado que gaste más dinero del que realmente posee.

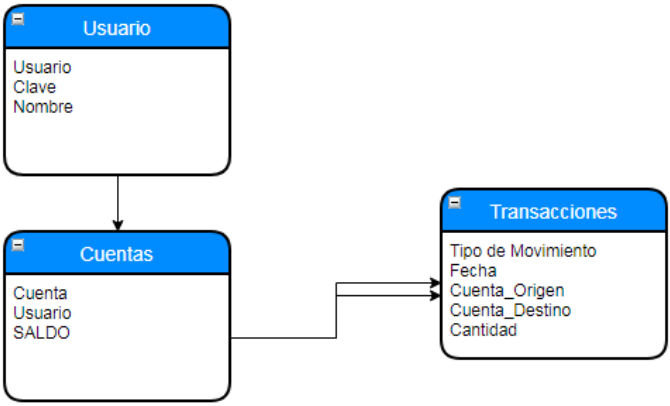
En resumen, el agente central lleva el saldo disponible de que cada cuenta y además registra un libro mayor que contiene todas las transacciones o movimientos que alteran el saldo de cualquier cuenta. Si nos damos cuenta, hacer un software que funcione de esta manera, realmente no es un reto para ningún desarrollador.

Para identificar al usuario usaríamos la típica pantalla de acceso que usamos los informáticos:



Luego, cuando hayamos validado que el usuario y la clave coinciden, ingresará al sistema para mostrarle el saldo de su cuenta, con un botón para transferir el dinero a una tercera persona:

En la base de datos se guardaría información del usuario, su saldo y las transacciones que haya realizado, con un modelo similar a este:



Si lo pensamos en forma centralizada, el problema desde el punto de vista tecnológico no es complicado de resolver. Registrar las transacciones de las transferencias de dinero entre varias cuentas y mantener el saldo disponible (balance) es algo que cualquier programador podría desarrollarlo en poco tiempo - *claro sin descuidar el tema de seguridad* -.

Descentralizando las transferencias de valor

Entonces, que fue lo que conllevó a que Satoshi - *para nosotros es SHA2shi* ☺ - a proponer el uso de la tecnología Blockchain para realizar una plataforma de pagos, o *¿crees que solo buscaba hacerse famoso al hacer gala de su talento para la criptografía?* Pues, el reto no es trivial, se quería que hacer una plataforma que funcione en forma descentralizada, sin la necesidad de un agente central, ¿sabes qué significa eso?, es ahí donde se propuso el mayor reto tecnológico conocido hasta el momento por la comunidad de desarrollares. ¿Sabes por qué?, pues si no hay un agente central, ¿cómo se puede llevar el registro de los propietarios de cada cuenta?, ¿cómo se

puede llevar el registro del movimiento de dinero de cada cuenta?, ¿cómo se puede evitar el doble gasto?, ¿cómo se va a evitar los fraudes?, ¿cómo se va a llevar el derecho al secreto bancario? Y quizás lo más complicado, ¿cómo vamos a hacer que confíen en este sistema, si nadie es responsable del sistema?

Lograr hacer un sistema de pagos electrónicos descentralizado, un sistema donde nadie tenga que confiar en nadie sino la confianza se deposita en todos. La propuesta fue crear una red de equipos de cómputos (nodos) donde todos juntos lleven el registro de las transacciones y el balance de cada cuenta. Lo más arriesgado fue esperar a que las personas confíen a que nadie, se lleve su dinero o invente saldo que no tiene, es decir, que ninguno de los nodos pueda mentirle al resto. En otras palabras, era dejar a que las computadoras controlen el gasto de nuestro dinero y no las personas ni las organizaciones intermediarias.

No estoy seguro si se está entendiendo la magnitud de éste reto, pero el pretender dar una solución de pagos en forma descentralizada requiere de una serie de desafíos tecnológicos que a simple vista, parece imposible de resolver, al menos hasta esa fecha, nadie se había atrevido a hacerlo y probar su funcionamiento, y ¿sabes por qué?... Pensemos no solo en la tecnología, sino en otros aspectos que se necesitan para que este problema se pueda resolver: *¿Quiénes pondrían esos nodos y por qué lo harían?*, *¿cómo puedo estar seguro que nadie va a robarse el dinero?*, *¿Cómo voy a hacer para que la gente confíe en este sistema?*, *¿Cómo va a afectar este sistema a los poderosos líderes del sistema financiero (bancos, plataformas de pagos online y transferencias de divisas)?...*

Volviendo al desafío tecnológico, probablemente sin que él o ellos lo sepan <*nos referimos a Satoshi Nakamoto*> o quizás si lo sabían, pero en su afán de resolver el problema de descentralización

estaban creando, paralelamente una nueva arquitectura tecnológica que promete ser capaz de crear confianza entre personas u organizaciones que no se conocen entre sí y que tampoco tienen que tener confianza entre ellas.

La solución fue crear una red del tipo peer to peer, que es una red de nodos conectados entre sí que intercambien información en tiempo real, son redes punto a punto donde solo registrando algo en una de ellos, este nodo se encargará se enviárselo al resto, de tal forma que todos tengan el mismo contenido. Ahí fue cuando se encontraron con otro gran desafío que por muchos años no se ha estudiado por los especialistas en informática, el problema de los generales bizantinos, si no conoces de que se trata, no te preocupes en el capítulo 4 hablaremos de esto a detalle. Solo para no dejarte con la duda, el problema consiste en buscar u mecanismo que evite que un nodo malicioso le mienta a los otros nodos con el afán de confundir al sistema.

Los desafíos detrás de la Blockchain

Vamos a enumerar los principales desafíos en desarrollar un sistema de pago o transferencia de dinero en forma descentralizada.

Demostración de la propiedad de un activo

Desafío: En un sistema centralizado administrado por una entidad bancaria, será esta organización quien autorice y gestione el acceso al sistema, otorga un registro de acceso y brinda los privilegios respectivos para realizar ciertas acciones en el sistema; pero. ¿Cómo hacerlo en un modelo descentralizado? Una solución simplista será contar con una base de datos donde se mantengan todas las cuentas, donde exista un mecanismo de autenticación

donde solo el dueño de cada cuenta pueda demostrar si propiedad, pero como no deseamos que existan ningún agente central, entonces lo copiaríamos en todos los nodos, pero como evitaremos que algún nodo malicioso, utilice la información de los usuarios para realizar transferencias fraudulentas.

Otra forma de solucionar el problema para demostrar la propiedad de un activo, sin tener que replicarlo en todo los nodos, es nombrar a un nodo como responsable de llevar el registro de propiedad de cada activo, digamos como si fuera un nodo súper poderoso encargado de crear las cuentas y dar acceso. No sería una mala idea, pero te imaginas a los hackers, todos van a atacar ese punto para tratar de apoderarse del dinero. Dicho de paso, es lo que hacen con los bancos, atacar su registro de acceso.

Quería comentarte que existen algunas plataformas Blockchain que proponen este modelo hibrido. Un súper nodo se encarga de crear las cuentas y autentica el acceso. Por otro lado, se han creado empresas que crean billeteras o wallet en forma automática, usando un sitio web y con un par de clic te crean tu dirección y tu llave privada para que puedas enviar o recibir dinero.

Algunas de estas empresas son muy serias, pero cuando termines de leer el libro y conocer cómo funciona Blockchain, te darás cuenta "lo tonto" que puede sonar usar una de ellas; si ellos quisieran te pueden quitar todo tu dinero o el registro de propiedad de algún activo de valor, y no tendrás a quien reclamar.

En la Blockchain, la seguridad es tú responsabilidad.

Las diferentes Blockchain del mercado han propuesto soluciones donde no se requiere nombrar a ninguno de los nodos como el responsable de autorizar el acceso para utilizar la red, cualquier persona puede realizar registros y transferencias sin necesidad de identificarse con sus datos personales. El acceso a la Blockchain por lo general utiliza criptografía asimétrica. Este mecanismo se seguridad permite crear dos llaves que se encuentra relacionadas entre sí. Una llave pública que permite identificarte en el sistema y una llave privada que será usada para comprobar la propiedad de una cuenta cuando se desea transferir el dinero a otra cuenta. Más adelante profundizaremos este tema de firmas criptográficas asimétricas. Lo que se hace en la mayoría de las blockchain's, es crear una cuenta relacionada a la llave púbica y cuando se desea transferir la propiedad del activo, se solicita la llave privada, sin necesidad de comprar su existencia o privilegio en una base de datos central.

Anonimación

Desafío: Muy pocas personas saben, pero alguna vez alguien le preguntó en el grupo donde SHA2shi[2] propuso bitcoin, *¿a qué empresas le podría interesar utilizar bitcoin?*, quién contestó que podía ser utilizado para el acceso a sitios pornográficos, evitando la identificación y la posibilidad de que aparezca el registro de acceso en el estado de cuenta de las tarjetas de crédito de sus usuarios.

La necesitaba que las plataformas de Blockchain públicas sean anónimas se alinean a las leyes de privacidad y tratamiento de datos personales extrafronterizos, aunque para ser honestos, no

[2] Se refiere al pseudónimo utilizado por el creador o creadores de bitcoin Satoshi Nakamoto.

creo que eso le haya interesado mucho al grupo de SHA2shi, creo que la anonimización se dio como consecuencia por ser un declarado participe del movimiento cyberpunk[3].

Las llaves de acceso pueden ser creadas sin necesidad de identificare ante nadie, puedes crear un par de llaves (pública y privada) usando comandos openSSL desde tu propio equipo, en el caso del protocolo Bitcoin (con B mayúsculas porque se está refiriendo al protocolo Blockchain y no a la moneda digital) no se usas la llave pública para recibir o transferir dinero, sino se crea una dirección que se calcula matemáticamente desde la llave pública.

Para crear una dirección de bitcoin válida, deberás realizar el siguiente cálculo:

```
Base58Check ('00' + Riped160 (<Llave Pública>) +
      Substr(Sha256(Sha256(Riped160(<Llave
               Pública>))),0,4))
```

Las direcciones tienen este formato:

`1MtmDYKMq73MLmh36y2sSBL9jbasnjG3ve`

Si nos damos cuenta, una persona o empresa que desea recibir un pago a través de Bitcoin, puede crear una dirección (cuenta) sin necesidad de utilizar un software especializado ni estar conectado a un nodo en la red, solo hace el cálculo en forma descentralizada y anónima.

[3] Persona que utilice una fuerte criptografía en un esfuerzo por lograr un cambio social o político

Cualquier persona que le transfiera dinero, la cuenta lo va a recibir, si el propietario desea mover el dinero a otra cuenta, en ese momento deberá identificarse con su llave privada a través de un nodo, quien validará que esa llave realmente le pertenece a la dirección de cobranza y la transferencia será aprobada. Un grupo de nodos validarán que la transacción fue real, sin que la llave privada este expuesta.

Validación y comprobación

Desafío: Al no existir un intermediario, se necesita un mecanismo seguro que garantice y permita demostrar que una transacción de pago fue realizada correctamente.

En la mayoría de las Blockchain que usan criptomonedas como Bitcoin o Ethereum, solo existe la posibilidad de crear transferencias de una determinada cantidad de monedas entre dos o más direcciones.

En las Blockchain que se utilizan para uso empresarial, donde las transacciones sirven para registrar un activo de valor y demostrar la propiedad en un momento del tiempo, también permiten transferencias de propiedad de los activos, pero en forma total, es decir, no se puede dividir en partes, se transfiere todo el activo o nada. Por ejemplo, cuando se desea registrar el registro de propiedad de un ganado o al productor que provee el contenido de una caja de productos perecederos que se van a exportar.

Si te das cuenta lo que se necesita es registrar y validar la transferencia de la propiedad, incluso cuando es una criptomomeda, solo que en este caso se trasfieren pequeñas cantidades o decimales.

Para que pueda validarse y comprobar su existencia en un momento del tiempo, por lo general los la información registrada en la Blockchain es pública. Ingresando a cualquier nodo, como por ejemplo en BTC.com o Stamping.io, podrás ver que existen muchas transacciones que se realizaron en los últimos minutos. Nadie sabe quién es la persona u organización que está transfiriendo la propiedad, tampoco se sabe el motivo por el cual lo hace ni el propietario de la cuenta receptora de la trasferencia. Únicamente los involucrados en la transferencia saben cuál de esos registros les corresponden y podrán validarlo sin necesidad de un intermediario que haga el rol de un tercero de confianza.

La función primordial de la Blockchain es certificar que las transacciones de registro o transferencia de un activo fueron realizadas en un momento del tiempo, evitar que las eliminen o modifiquen, además de compartirla sin atentar con la privacidad de los datos personales de los involucrados, y sin necesidad de un único intermediario, sino un colectivo de nodos que a través de modelos matemáticos, que conoceremos más adelante, puedan dar fe que la información es correcta y no ha sido adulterada por ninguno de los nodos participantes de lar ed.

El origen del nombre de cadena de bloques (Blockchain) se debe a la forma como se almacena la información, los datos asociados a una trasferencia de la propiedad de un activo son endosados en uno de los nodos, se replica ente todos los nodos y se espera a que se realice el consenso entre ellos. De estar todo conforme, los nodos acuerdan que estos nuevos datos, que se encuentran dentro de un bloque puedan sea agregado al libro mayor (conocido como ledger), este nuevo bloque estará entrelazado con el bloque anterior, forzando de esta manera a cambiar los siguientes registros si se desea modificar la historia, lo que computacionalmente lo

hace imposible de realizar, sin que los nodos se pongan de acuerdo para hacerlo.

En las redes Blockchain públicas existen miles de nodos ubicados en diferentes partes del mundo, cada uno de ellos tiene una réplica exacta de la base de datos, por lo que para cambiar la historia tendría que el 51% ponerse de acuerdo para engañar al sistema. Por otro lado, en redes privadas, los nodos son de alta confianza y son ellos los interesados en que el sistema no mienta, por lo que la probabilidad que se modifique la información es casi imposible.

Los registros en la Blockchain, son muy similar a la forma como se almacenan las transacciones en una base de datos de cualquier organización pero, con una gran diferencia, es que los datos asociados a una transferencia de propiedad han sido verificado por un colectivo formado por nodos imparciales; donde nadie tiene el control total de la información, ni el acceso o privilegios para adulterar los datos. Los nodos son quienes se encargan de verificar que todas las transacciones sean válidas, utilizando algoritmos matemáticos que pueden alertar si alguien está tratando de generar transferencias fraudulentas.

Lo que realmente busca la Blockchain es brindar confianza a todos los participantes que utilizan la red, los testigos serán suficientemente confiables para garantizar que la historia de lo que se registró es real; sin que nadie, y absolutamente nadie, pueda eliminar ni adulterar la información registrada una vez que los testigos hayan determinado por consenso que así sucedieron los hechos. Es por eso que algunos románticos apasionados por la Blockchain, la conocen como la base de datos de la confianza.

Sincronización de Nodos

Como ya lo hemos definido antes, los nodos son los equipos que se encuentran conectados entre sí y que contiene un software que permite almacenar y compartir la información entre todos los nodos que forman la red. En palabras simples de entender, son los testigos digitales que tiene la responsabilidad de dar fe de la existencia de las transacciones, cuentan con mecanismos que ayudan a detectar si alguno de ellos ha registrado información distinta. Dependiendo las reglas del protocolo de la red utilizada, algunas Blockchain sincronizan a los nodos con la información correcta u otros los expulsan de la red, por lo que todos los nodos de la redes Blockchain, no funcionan igual; ya que fueron creadas para propósitos específicos.

La cadena de bloques o Blockchain

Dentro de los nodos se almacenan activos de valor, que no son más que datos, esa base de datos también es conocida como "ledger" o libro mayor. Cuando la información es registrada en alguno de los nodos, esta es propagada hacia el resto de participantes de la red, los datos son entrelazados de tal forma que si se modifica un valor, por mínimo que sea, debería cambiarse toda la cadena de información; lo que hace que técnicamente sea difícil de lograr, y cada vez que se agreguen más nodos el nivel de complejidad aumenta.

La confianza entre los participantes

En el mundo actual, un negocio no podrá sobrevivir si no es capaz de ofrecer experiencias positivas que inspiren confianza a sus consumidores, sus proveedores, sus empleados, el gobierno y otras empresas. Lograr esa confianza implica, entre otras cosas, cuidar una serie de aspectos que van más allá de las políticas interna de la compañía. Ahora no basta con ser honesto, ni tampoco parecerlo,

cada vez más, las empresas están siendo obligadas a demostrar su honestidad, eso significa ser transparente en cada una de sus operaciones.

"La confianza demora para ganársela, pero se pierde en tan solo unos segundos"

Las empresas modernas ven a la confianza como un activo que se deben valorar y valorizar, dentro y fuera de la empresa. La confianza se gana poco a poco, se cuida, se cultiva y se gestiona. Las operaciones se están realizando de manera global y prácticamente todo el mundo se encuentra conectados entre sí. Gracias a la internet, donde la confianza es de suma importancia para alcanzar el éxito empresarial debido a la agilidad de las transacciones comerciales.

La mayoría de personas parecen confiar poco en los sitios web donde colocan sus tarjetas de créditos, comienzan a adquirir productos con la esperanza que realmente se los envíen y con las mismas características que se encuentran publicados en sus sitios web, las personas confían que sus datos personales no serán tratados de manera incorrecta. Y, en un sentido general, en cuanto una simple falla pueda ser crucial para perder ese activo tan preciado llamado "confianza", al perderla es muy probable que todas las personas dejen de hacer negocios en ese sitio web.

La confianza en los negocios incluye temas como seguridad perimetral, mecanismos antifraudes, protección de datos personales e informar honestamente sobre la calidad de un

determinado producto o servicio. Si algún aspectos falla, los consumidores harán saber su malestar en tiempo real, tendrán gran repercusión y de no poder demostrar que, a pesar del error, la empresa si es confiable, podrá perder muchos clientes.

La confianza es lo que realmente permite que las personas y las empresas puedan hacer operaciones comerciales, pero sin temores. Quizás por eso muchas personas todavía se muestran escépticas al oír que la "Blockchain" promete transformar la forma en que se generará la confianza en la sociedad. *¿Cómo es que un algoritmo matemático puede brindar confianza?*

La Blockchain es probablemente el cambio tecnológico más disruptivo que ha ocurrido en los últimos años a la comunidad informática. A logrado un nuevo modelo de la forma como se realizan las empresas y el modelo de confianza que se debe adoptar. Antes de la Blockchain, la confianza estaba centralizada en organizaciones de poder o intermediarios que daban confianza a los involucrados dentro de una red comercial; sin ellos, difícilmente se podía hacer una transacción.

Estarás de acuerdo conmigo que el dejar rastros en papel firmados, o escribir historiales comerciales en un libro contable, o plasmar físicamente el movimiento de inventarios en el almacén, solían ser la forma preferida de nuestros padres para establecer la confianza que algo se realizó en un momento determinado del tiempo y bajo las condiciones y características que están escritas. Hasta ahora recuerdo que muchas personas solían tomarse una foto con un diario para generar una prueba que les ayude en el futuro a demostrar que algo existió en un momento del tiempo; quizás ese fue el primer método pseudo digital que nuestros padres utilizaron

para "sellar el tiempo", ahora existe algo más simple de usar y más fácil de demostrar: Stamping.io. Solo una API Rest te ayudará a registrar cualquier evidencia digital de cualquier secuencia de datos. Definitivamente, hemos evolucionado.

Cuando en una transacción intervienen distintas partes que no se conocían previamente y por lo tanto no han establecido confianza entre ellos, los papeles abundaban y los notarios hacían lo que mejor saben hacer: "brindar confianza entre los involucrados". Cuando hay dinero de por medio, la seguridad toma un papel más importante, es por eso que los servicios financieros y bancarios, son muy difícil de transformarse digitalmente, como todos sabemos, la gente a veces miente y cuando hay mucho dinero involucrado, "mienten de verdad".

Todos alguna vez hemos mentido, lo que cambia es la dosis y el motivo que nos conlleva a hacerlo. Son muchas las razones que nos pueden forzar a mentir, casi siempre las mentiras son motivadas para evitar "un castigo o evitar ser culpado" o para "ganar algo que no lo mereces o que no puedes demostrar que sí lo mereces". En otras palabras, la mentira es usada por las personas para protegerse o para conseguir algún supuesto beneficio. Muchas empresas tienen que gestionar ese problema dentro de sus sistemas, siendo el "Repudio[4]" la forma más común que usan las empresas para "mentir", la Blockchain podría ayudarlos a hacerlo de manera segura y económica.

[4] Negar un hecho que realizaron.

"Alrededor de un tercio de la población
cuenta una gran mentira cada día"
- Richard Wiseman -

Cuando una entidad bancaria o cuando una empresa mayorista necesita dar una línea de crédito a alguna empresa distribuidora o minorista, se arriesga. Sus mecanismos para gestionar el riesgo crediticio se basa en "la confianza" que el deudor se ha ganado. Esa confianza se gana poco a poco a través de su historial y eso es lo más importante que un analista de crédito deberá evaluar, antes de decidir la aprobación de una línea de crédito, incluso tiene mayor peso en la decisión que la misma titularización de la deuda o la garantía prendada. Es decir, no es tan importante que el registro de la deuda quede sentado en una piedra, en comparación de la veracidad de la información que se tomó como referencia para aprobar el crédito.

Consideremos que la confianza es la esperanza fiel que alguien deposita en algo en particular, la confianza es una decisión personal, momentánea y motivada por 3 aspectos:

- *Confianza descubierta o informada*: Las personas cuentan con el conocimiento informado antes de depositar su confianza en algo.
- *Confianza heredada por terceros*: Las personas depositan su confianza en algo debido a que otros lo hacen (reputación del sistemas) o por que alguna persona informada se lo recomienda.
- *Confianza impuesta*: Cuando el gobierno o la escasez de otras alternativas nos obligan a confiar en algo, que no

necesariamente conocemos o que cuente con una buena reputación.

Como es que una tecnología puede pretender convencer a todo el mundo que en algún momento -*no muy lejano*-, todos comencemos a confiar en la información que se registra en un grupo de computadores conectados entre sí y sin que nadie, absolutamente nadie de los participantes, se haga responsable de nada.

Dinámica grupal 3: La confianza

Este ejercicio ayudará a que los alumnos descubran que en transacciones muy seguidas es difícil comprobar quien está mintiendo.

El profesor deberá contar con 12 o más fichas que contiene palabras asociadas a la Blockchain:

El profesor deberá sacar a dos alumnos al frente para jugar, los alumnos se ponen uno frente al otro, las fichas son entregadas a uno de ellos y el juego trata de que el jugador debe tratar de engañar al otro jugador, se supone que todas las palabras están vinculadas a la Blockchain, por lo que en algún momento el jugador que tiene las fichas se va a encontrar con esta ficha:

En ese momento debe inventarse rápidamente una palabra vinculada a la Blockchain, si logra pasarla como ficha real, al final del juego ha ganado, caso contrario pierde.

El profesor también puede usarla como una herramienta de repaso, donde cada el alumno recibe una de las fichas, y debe tratar de explicar qué rol tiene ese componente en la Blockchain con la finalidad que el resto de sus compañeros adivine, el que lo haga gana un punto. Si no sabe de qué se trata puede engañar al resto del grupo que tiene otra palabra referente a algo que si domine y que pueda explicarlo. El profesor apunta los resultados en la pizarra.

Cuando uno de los alumnos le toca la ficha que obliga a mentir, el alumno deberá inventarse algún componente y tratar de convencer al resto, que la ficha es correcta.

Al final todos mostrarán sus fichas, puede ser que algunos alumnos que no sabían de qué se trataba la palabra que le toco han

mentido, otros lo hicieron solo por diversión y al que le toco la ficha que obliga a mentir tuvo que hacerlo.

Se demostrará que es muy fácil engañar a una base de datos cuando no existe nadie que compruebe el valor, además que los datos tienen un mismo patrón que a simple vista dificulta su identificación. Por otro lado, al estar centrados en el core business del negocio no nos permite estar atentos cuando nos están registrando una transacción fraudulenta.

¿Les falta oxitocina[5] a las empresas y personas?

El investigador Paul Zak repartió diez dólares entre 19 personas para demostrar un experimento. Luego los invitó a que compartieran este dinero con un receptor anónimo. Zak andaba detrás de químicos que estimulan el cerebro y generan emociones y conductas en la gente. La confianza es una de ellas. Cuando los receptores anónimos recibieron el dinero de los voluntarios, Zak entonces triplicó la cantidad que recibiera cada uno y les exhortó a que compartieran lo que habían ganado con el voluntario que les había enviado la donación original. El 54% de los receptores compartió las ganancias con los voluntarios. Estudios de sus organismos indicaron que aquellos que habían sido más generosos tenían los niveles más altos de oxitocina.

Esta hormona es un mensajero químico muy especial. No sólo tiene el control de iniciar y estimular la producción de leche materna sino que su aparición en la madre y el niño afianza mucho más la unión entre ambos. La oxitocina también aparece, junto a la serotonina, en los cerebros enamorados y en las personas relajadas

[5] Basada en el artículo de Glenys Álvarez publicado en sindioses.org

ya que entre sus funciones está la de bloquear a las hormonas que producen el estrés. También se ha comprobado con ratas de laboratorios, que los niveles de la hormona incrementan notablemente ante el tacto.

La producción de oxitocina inicia un círculo que estimula y genera confianza. Luego, la confianza continúa engendrando más confianza. Un experimento realizado por Ernst Fehr de la Universidad de Zurich, en Suiza, demostró que una vez una persona es de fiar, sus altos niveles de oxitocina estimulan su generosidad lo que a su vez genera aún más confianza.

El equipo de Fehr también utilizó el dinero como herramienta para generar confianza o desconfianza. El investigador tomó a un grupo de voluntarios y los dividió en tres y a cada equipo los enfrentó a una situación distinta. En la primera situación, el grupo de voluntarios recibía de una persona una cantidad de dinero para que lo invirtiera en algo que le ganara más dinero. Pero junto a la cantidad también recibían una advertencia y una amenaza de penalizarlos si perdían el dinero. El otro grupo sólo recibió el dinero sin advertencias ni amenazas, sin embargo, el tercer grupo sabía de antemano que existía un castigo si perdían el dinero pero que era la opción de la persona que lo entregaba amenazarlos con la penalidad. La persona les entregó el dinero sin las amenazas. El análisis de los resultados demostró que este último fue el grupo más generoso y que el primero fueron los que menos devolvieron ganancias.

"Cuando alguien confía en ti, tiende a ser más generoso lo que a su vez lo hace mucho más confiable en los ojos de los demás. En otras palabras, la confianza estimula la

generosidad y los lazos entre las personas"
Fehr para el diario científico Nature.

Definitivamente, en algún momento del futuro, al saber que una empresa utiliza la Blockchain, va a generar oxitocina en sus usuarios, y esa confianza hará que se generen fuertes relaciones comerciales.

¿El mundo está preparado para este cambio de paradigma?

Quizás si nos remontamos hace diez años atrás, si alguien expusiera la hipótesis de crear confianza basada en una serie de testigos interconectados entre sí basado en resumen criptográficos llamados "hash", les aseguro la mitad del publico tildaría al expositor de loco, el resto no diría nada pero se pararía y se retiraría del auditorio. Un grupo de personas o una persona - *quién lo sabe*-, bajo el seudónimo de Satochi Nakamoto se atrevió a hacerlo, creando la primera moneda digital o criptomoneda llamada "bitcoin", sólo por usar un nombre en japonés no creo que haya sido suficiente, para que al inicio muchos puedan confiar en esta nueva forma de transferir dinero.

Algunos científicos, matemáticos y/o expertos en criptografía, vieron que esta solución podía funcionar. Al informarse de como funcionaria la red, a la forma en que se gestionaría la seguridad de las transacciones y los mecanismos de consenso que son capaces de garantizar que la información registrada no podrá ser víctima de manipulación; confiaron en la red, compraron esos primeros bitcoins que se ofrecían a unos cuantos centavos, y gracias a la

confianza que ellos depositaron en este red, muchos de ellos son millonarios.

Al pasar los años, la gente comenzó a hablar de aquella "criptomoneda" que registra todos sus movimientos en unos bloques que se encuentran encadenados entre sí, con la única finalidad de volverlos inmutables. A pesar que muchos realmente no entienden cómo es que realmente funciona esta tecnología pero, debido a que todo el mundo hablaba de esto, comenzaron a heredar la confianza de otros y se generó, sin querer, una burbuja económica que logró que bitcoin llegar a costar más de 20,000 USD por unidad. Recuerdo que la esposa de José, quien es del sector salud, hace unos años nos consultó: ¿Por qué no compras bitcoin, el esposo de mi amigo los compró a 4,000 USD y los acaba de vender en 12,000 USD? ¿Creen que ella tiene idea de cómo funciona una Blockchain, o qué es un hash, o qué es un minero o cómo funciona el algoritmo de consenso llamado PoW?, definitivamente no, pero ya estaba motivada a comenzar a confiar en la Blockchain debido a la reputación que bitcoin estaba tomando en las redes sociales y las recomendaciones que estaba recibiendo por la experiencia de terceras personas.

En un mundo donde la confianza en los sistemas informáticos se ve empañada debido a la proliferación de comunidades de hackers o intrusos que ingresan a los sistemas informáticos a cambiar la realidad de los hechos. La búsqueda de alguna alternativa, que nos ayude a incrementar la confianza en nuestros registros, es quizás, lo que está motivando a que el mundo entero, todos los días, lea o hable algo referente a alguna solución donde se está utilizando la Blockchain.

La Blockchain es una red que ayuda a que muchas personas, empresas y/o gobiernos confíen en la información que utilizan para tomar decisiones o ejecutar acciones importantes. Para lograr que esa "confianza" se alcance entre todos los participantes, se requiere cumplir al menos estos requisitos:

- Utilizar testigos digitales: Las transacciones deben ser almacenadas en varios lugares al mismo tiempo, incluso en servidores donde el registrante no tenga acceso para modificar la información, a estos testigos se les conoce como nodos, y no son más que equipos conectado entre sí que reciben y guardan una copia de la información.
- Verificación que todos los nodos estén llevando la misma contabilidad: Usualmente se le conoce como consenso, lo que se pretende es asegurar que todos los nodos están almacenando la misma información, que ninguno de los testigos tenga una versión diferente de la realidad, y de ser así, se debe realizar un voto virtual donde los nodos que tengan la mayoría de esa votación, ganen, y copien la versión de la realidad en los otros nodos que contienen una versión distinta a la mayoría.
- Inmutar los datos: Como entenderán no se puede estar constantemente auditando que los datos no sean cambiados. Para confiar ciegamente en la información, es necesario contar con un mecanismo que asegure que una vez que los nodos hayan llegado a un consenso, los datos sean almacenados en un ambiente seguro, de tal manera que nadie tenga que volverlo a comprobar, a esto se le conoce como bloque y se entrelaza con los otros bloques para que sea imposible modificar la historia.

Por último, la Blockchain no solo atrae beneficios a las empresas, también añade transparencia mediante el registro y acceso a información confiable ya que fue firmado por el registrante y se puede verificar que realmente fue así. Por otro lado, haciendo uso de los llamados "contratos inteligentes" se puede garantizar el cumplimiento de un acuerdo gracias a su mecanismo de su auto-ejecución.

Otro ámbito de aplicación interesante es la investigación científica o creación de obras, donde Blockchain permite que los investigadores o sus autores publicar resultados de los estudios practicados u obras de su autoría, sin necesidad de esperar a que sean publicados en congresos o revistas, y sin peligro que otro pueda atribuirse la autoría (Leftherian.com es un caso peruano de ejemplo). La Blockchain permite demostrar sin lugar a duda quién es el autor original de la información y cuándo fue publicada dando fe a su pre-existencia en un momento del tiempo.

Desde la perspectiva más empresarial, en un futuro cercano, será posible codificar programas en Blockchain que permitan a los socios inversionistas reclamar dividendos, o indemnizaciones, o regalías a que tienen derecho las acciones, sin necesidad de intervención humana y con la garantía de un cálculo transparente, predefinido y aceptado por todas las partes.

Como veras, el contar con mecanismos de confianza, la agilidad de los negocios será una realidad, evitando procesos de conciliaciones, validaciones o auditoría.

Capítulo 2
La criptografía y su uso en la Blockchain

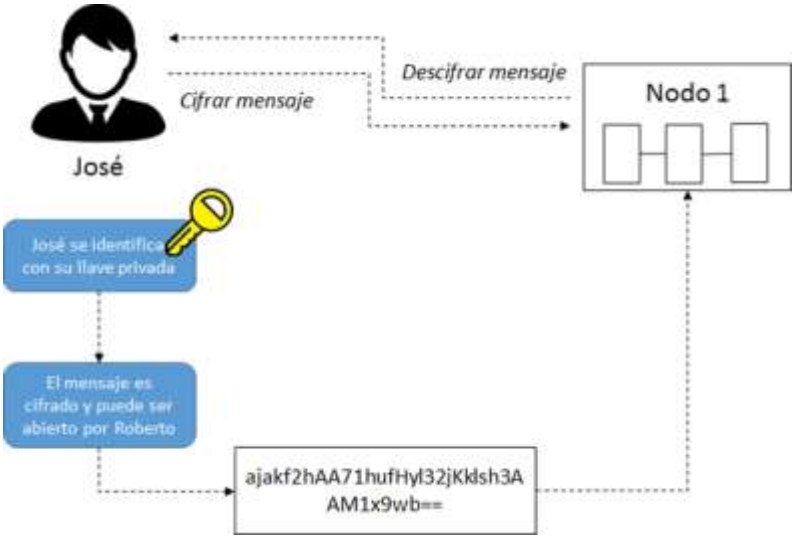
La palabra criptografía proviene de la unión de dos palabras griegas "kryptos" = *oculto*, y "graphia", = *escritura*, por lo que su definición sería: "Escribir algo oculto o secreto".

La criptografía ha sido estudiada por muchos informáticos y matemáticos desde décadas pasadas, incluso existen indicios que en la antigüedad se usaron métodos criptográficos que permitieron ocultar la información a quien no deberían verla. Uno de los primeros documentos cifrados de la antigüedad se descubrió en Irak en el siglo XVI a.C. donde un alfarero había grabado su receta secreta para fabricar tablillas en una tableta de arcilla, donde suprimió consonantes y alteró el orden de las palabras.

Como veremos en este capítulo, gracias a la capacidad de cálculo que tienen los ordenadores hoy en día se han creado técnicas más sofisticadas para cifrar y descifrar información. Actualmente, estas técnicas y/o algoritmos aseguran las transferencias de datos digitales a lo largo de todo el mundo.

Con la aparición de los computadores con una alta capacidad de procesamiento las técnicas criptográficas han evolucionado

mucho, siendo utilizada para brindar la seguridad necesaria en muchos niveles, desde la identificación y/o autenticación, la confidencialidad del registro y la inmutación de los datos.



La criptografía es uno de los pilares principales de la tecnología Blockchain, utilizando diversos algoritmos de resumen criptográficos se puede: demostrar la propiedad de un registro, transferir datos en la red de nodos, mantener la integridad de los datos en la cadena de bloques y para facilitar el proceso de consenso, entre otros ejemplos.

La criptografía busca crear métodos seguros para realizar la comunicación entre dos o más partes, garantizando:

- La confidencialidad de la información (cifrado de mensajes).
- La integridad del mensaje. (usando técnicas de hashing).

- Garantizar la vinculación con el emisor del mensaje. (Firma del mensaje).
- La existencia de mecanismos que permitan verificar la identidad del comunicador. (Firma del Mensaje, Firma ciega o pruebas de conocimiento cero)

En la Blockchain, el uso de los métodos criptográficos tiene tres propósitos específicos:

1. Identificar a la persona cuando se envía y recibe el mensaje.
2. Autenticar a las personas que envía el mensaje.
3. Comprobar la voluntad de la persona para aceptar una transferencia de un registro de la Blockchain.

Resumen criptográficos

Teniendo en cuenta que actualmente se calculan unos 60 trillones de hashes SHA-256 por segundo para minar Bitcoin en todo el mundo, quizá no es aventurado afirmar que puede ser el «algoritmo más popular del mundo».

- Matthew Weathers -

Conforme aumenta la popularidad de los diferentes proyectos donde se utiliza la Blockchain, se escucha mucho el uso de la palabra "Hash", la cual se refiere a una función de resumen criptográfico basada en un algoritmo matemático que transforma cualquier secuencia de caracteres alfanuméricos en una nueva serie de caracteres con una longitud fija. Independientemente de la longitud de los datos de entrada, el valor hash de salida tendrá siempre la misma longitud.

Existen varios tipos de algoritmos de hash, en la Blockchain por lo general se utiliza el del tipo SHA256, que genera una lista de 64 caracteres hexadecimales, es decir está conformado por las letras de la A a la F y los números del 0 al 9, por ejemplo si calculamos el hash del nombre: José, el Hash de tipo SHA256 dará como resultado:

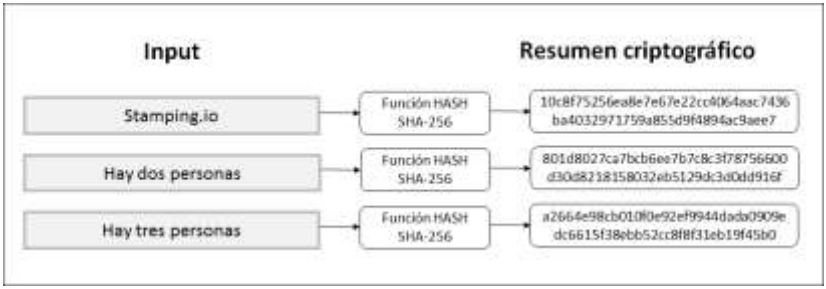
```
d3a309852d82a42f48c317174a8b35b7d3316b29ee63ebc
222527f10c113151e
```

Pero si se calcula el hash al nombre Jose (sin tilde) el resultado sería muy diferente:

```
ae978aa10c628b27427ff2615ad925abdf4171fc7b4d1f7
067bd35b23960d371
```

Si comparamos los resultados, una simple tilde generará una secuencia de datos completamente distinta al anterior, por lo que este método se utiliza para validar la existencia de un mensaje (documento, imagen, audio, video o secuencia de caracteres) dentro de la Blockchain ya que un mínimo cambio, por simple que parezca, adulteraría la secuencia de caracteres en casi su totalidad.

El siguiente cuadro muestra algunos ejemplos:



Colisión de hash

De acuerdo a Wikipedia: En informática, una colisión de hash es una situación que se produce cuando dos entradas distintas a una función de hash producen la misma salida.

Es matemáticamente imposible que una función de hash carezca de colisiones, ya que el número potencial de posibles entradas es mayor que el número de salidas que puede producir un hash. Sin embargo, las colisiones se producen más frecuentemente en los malos algoritmos.

En ciertas aplicaciones especializadas con un relativamente pequeño número de entradas que son conocidas de antemano es posible construir una función de hash perfecta, que se asegura que todas las entradas tengan una salida diferente. Pero en una función en la cual se puede introducir datos de longitud arbitraria y que devuelve un hash de tamaño fijo (como MD5), siempre habrá colisiones, debido a que un hash dado puede pertenecer a un infinito número de entradas.

Para entender el problema de la colisión del hash es importante recordar el principio de Dirichlet, conocido coloquialmente como "el principio del palomar" que dice:

"Si hay más palomas que casilleros donde puedan entrar, entonces existen algún casillero donde van a dormir más de una paloma"

Aunque el principio del palomar puede parecer una observación trivial, se puede utilizar para demostrar resultados inesperados ante un hecho que, a simple vista parece imposible. Por ejemplo, hay por lo menos 2 personas en Perú con el mismo número de pelos en la cabeza.

Demostración[6]: la cabeza de una persona tiene en torno a 150.000 cabellos y tener un millón de pelos requeriría de una cabeza gigante (nadie tiene un millón de pelos en la cabeza). Asignamos un palomar por cada número de 0 a 1.000.000 y asignamos una paloma a cada persona que irá al palomar correspondiente al número de pelos que tiene en la cabeza. Como en Perú hay 30 millones de personas, habrá al menos dos personas con el mismo número de pelos en la cabeza. Aunque parezca raro, se puede asegurar que en cualquier ciudad con más de un millón de habitantes nos encontraremos con 5 personas o más que tengan la misma cantidad de cabellera (por el "principio del palomar").

Ahora pensemos:

¿Cuántos documentos existirán en el mundo que comparte el mismo hash a pesar de tener contenido diferente?

Si aplicamos el principio del palomar, estaría demostrado que existe muchos, esta suposición se logra dado que la cantidad de hash del tipo SHA256 es finita y se pueden crear es calculada de la siguiente fórmula:

$$1.2 * 10^{115}$$

La siguiente tabla muestra la cantidad de posibles resultados que se obtienen dependiendo el algoritmo de hashing usado:

[6] Ejemplo basado en el ejemplo de Wikipedia: https://es.wikipedia.org/wiki/Principio_del_palomar

Bits	Salidas posibles
64	1.8×10^{19}
128	3.4×10^{38}
256	1.2×10^{77}
384	3.9×10^{115}
512	1.3×10^{154}

Como verás, por más grande que se vea el número, la cantidad de hashes posibles que se pueden obtener al aplicarse a cualquier entrada de datos es un valor finito.

El principio del palomar permite demostrar que las colisiones son inevitables en una tabla hash; porque el número de posibles valores que pueden tomar los elementos de un vector exceden a menudo el número de sus índices. Ningún algoritmo de hashing, sin importar lo bueno que sea, puede evitar estas colisiones.

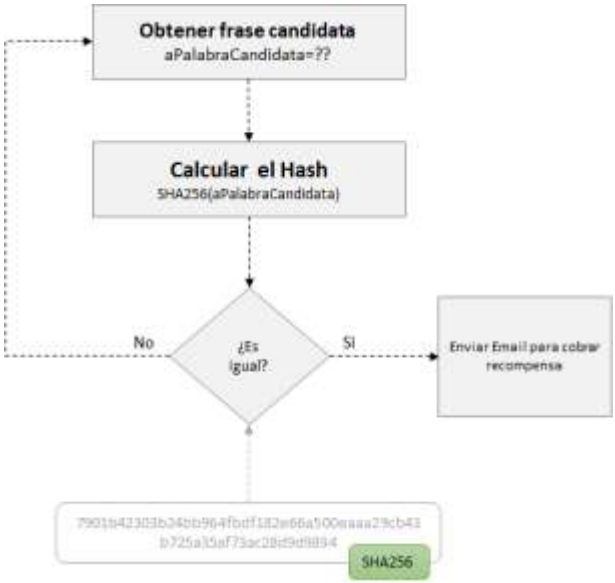
Una entrada de datos puede ser un documento, un archivo de sonido, una secuencia de datos, etc. No siempre será de tamaño infinito o al menos muy grande en cuanto a cantidad de bytes, por lo tanto, siempre existirá la posibilidad que dos entradas de datos generen el mismo hash de salida; sin embargo, debes procurar que no sea fácilmente revertir el valor del hash de salida para encontrar el valor de entrada. La forma de encontrar dos o más entradas que

den el mismo resultado, por ahora, no ha sido posible usando un algoritmo de ingeniería inversa (en el SHA256).

Para descubrir el valor de entrada que genera un determinado resumen criptográfico del tipo SHA256, por el momento solo se puede lograrse usando "la fuerza bruta", que consiste en realizar una serie de pruebas repetitivas con una lista de caracteres hasta lograr que en algún momento se logre el hash que se está buscando, por ejemplo: Si queremos describir cual es la letra, palabra, número, texto o símbolos de entrada que generan el hash del tipo SHA256:

`7901b42303b24bb964fbdf182e66a500eaaa29cb43b725a35af73ac28d9d9894`

Deberíamos comenzar a probar de la siguiente manera:



- Paso 1: Generar palabra Candidata
- Paso 2: Calcular el hash de tipo Sha256(<Palabra Candidata>)
- Paso 3: Si no es igual al hash buscado, regreso al paso 1,
    - Sino ¡Aleluya lo encontré!
- Es matemáticamente imposible que una función de hash carezca de colisiones, ya que el número potencial de posibles entradas es mayor que el número de salidas que puede producir un hash. Sin embargo, las colisiones se producen con más frecuencia en los algoritmos débiles o los que tienen salidas de menos bytes.
- A veces, se desea calcular el hash de una secuencia de datos de un pequeño número de entradas, que son conocidas de antemano, es posible construir una función de hash perfecta, asegurando que todas las entradas tendrán una salida diferente. Por ejemplo cuando se registran: transacciones de la Blockchain, facturas electrónicas, transferencia de propiedad, un registro de bytes o una secuencia de datos que utiliza una estructura conocida (JSON, XML, etc.).
- Pero en una función en la cual se puede introducir datos de longitud arbitraria, como es el caso de una imagen, un documento, un audio, video o cualquier archivo binario, y devuelve un hash de tamaño fijo, siempre habrá mayor probabilidad de encontrase colisiones, debido a que un hash dado puede pertenecer a un infinito número de entradas, a pesar que el atacante tiene el resto de buscar una entrada que no pierda el formato original y que genere el mismo hash de salida que el de otro documento que tiene el mismo formato.

El ataque de cumpleaños (Birthday attack)

La "paradoja del cumpleaños" establece que si hay 23 personas reunidas en un lugar, existe una alta probabilidad (50,7%), que al menos dos de ellos cumplan años el mismo día.

Para sesenta o más personas la probabilidad es casi certera (99%). Obviamente que si se tiene más de 366 personas la probabilidad será del 100%. (Teniendo en cuenta los años bisiestos).

Una paradoja es un dicho o hecho de la realidad que parece contrario a la lógica matemática. A pesar, que con la regla de Laplace se demostró que esa probabilidad es matemáticamente demostrable y por lo tanto, la paradoja del cumpleaños, no es una paradoja sino una lógica, a simple vista, parecería que fuera ilógico dado el siguiente motivo.

Si tienes 365 días del año donde cada persona puede nacer, como es que existe 99% de probabilidad que 2 personas cumplan años el mismo día solo con 60 personas, cuando la lógica haría creer que la menos se requiere la mitad de personas como días del año existe, es decir, al menos : "182 personas"

Las matemáticas demostraron que existe una alta probabilidad (>50%) de que 2 eventos sucedan el mismo día usando una cierta cantidad de intentos, para calcular la cantidad de eventos se usa la siguiente fórmula:

$$\#Intentos\ (50\%\ prob) = 1.1774 * RaizCuadrada\ (H)$$

Siendo H la cantidad de posibles resultados, por ejemplo para calcular cuantas personas se necesitan para tener el 50% de

probabilidad que 2 personas compartan el mismo día de cumpleaños sería:

*#Intentos (50% prob) = 1.1774 * RaizCuadrada (365) = 22.49*

(Es decir 23 personas)

El que dos hechos sucedan en un mismo momento se le conoce como colisión, es por ese que el ataque de cumpleaños es usando para detectar o generar colisiones, por lo tanto se puede determinar la probabilidad que existan colisiones (2 entradas distintas generen el mismo hash):

Bits	Salidas posibles	Probabilidad deseada de colisiones aleatorias							
		10^{-12}	10^{-9}	10^{-6}	0.1%	1%	25%	50%	75%
64	1.8×10^{19}	6.1×10^{3}	1.9×10^{5}	6.1×10^{8}	1.9×10^{8}	6.1×10^{8}	3.3×10^{9}	5.1×10^{9}	7.2×10^{9}
128	3.4×10^{38}	2.6×10^{13}	8.2×10^{14}	2.6×10^{16}	8.3×10^{17}	2.6×10^{18}	1.4×10^{19}	2.2×10^{19}	3.1×10^{19}
256	1.2×10^{77}	4.8×10^{32}	1.5×10^{34}	4.8×10^{35}	1.5×10^{37}	4.8×10^{37}	2.6×10^{38}	4.0×10^{38}	5.7×10^{38}
384	3.9×10^{115}	8.9×10^{51}	2.8×10^{53}	8.9×10^{54}	2.8×10^{56}	8.9×10^{56}	4.8×10^{57}	7.4×10^{57}	1.0×10^{58}
512	1.3×10^{154}	1.6×10^{71}	5.2×10^{72}	1.6×10^{74}	5.2×10^{75}	1.6×10^{76}	8.8×10^{76}	1.4×10^{77}	1.9×10^{77}

Esta tabla muestra el número de hashes que son necesarios para alcanzar la probabilidad de éxito dada, asumiendo que todos los hashes son igualmente probables (Extraído de Wikipedia)

Para entender el "ataque de cumpleaños", es decir, cambiar el contenido de algo que da como resultado el mismo hash que otro contenido, confundiendo al firmante sobre qué fue lo que realmente firmó, ya que ambos documento dieron el mismo hash.

Para firmar un documento o registro, ya sea en la Blockchain o un documento que se está firmando digitalmente, lo primero que se realiza es el cálculo computacional del hash del documento.

Supongamos que Ana quiere engañar a Bruno para que firme un documento fraudulento. Ana prepara dos documentos, ambos dan el mis o hash pero tienen contenido diferente. Para lograrlo primero calcula el hash del documento uno, el que espera que realmente firme Bruno, luego trata de modificar el segundo documento (documento falso), agregando párrafos sin cambiar el significado, colocando comas, espacios en blanco, usando sinónimos, o cualquier otro contenido que ayude a forzar una colisión.

Luego de una cantidad de intentos (millones), Ana finalmente podría crear una variación del documento que tendrá el mismo hash que el documento original.

Bruno firmará el documento original, pero Ana podría demostrar que también firmó el documento fraudulento, ya que ambos tienen el mismo hash.

Para impedir este ataque, la longitud de los resultados de la función hash deben ser lo suficientemente grande de manera que el ataque de cumpleaños se torne computacionalmente imposible, por ejemplo, unas dos veces más grande de lo que se requeriría para prevenir un ataque de fuerza bruta. También se ha recomendado que Bruno realice cambios menores en cualquier documento que le sea presentado para ser firmado. Sin embargo, esto no resuelve el problema, porque ahora Ana sospecha que Bruno intenta usar un ataque de cumpleaños.

Es por eso que muchas empresas utilizan stamping.io el cual orece tres soluciones, que en su conjunto evitan este ataque:

1. Cuenta con un sello de tiempo que evite este acto fraudulento. Ya que se podrá demostrar que los

documentos fueron creados en diferente momento del tiempo.

2. Usamos una técnica basada de repetición iterativa que pueden reducir considerablemente los requerimientos de almacenamiento de los ataques de cumpleaños.
3. También combinamos dos o más tipos de hashes dentro de una misma transacción que se ancla en la Blockchain, siendo muy baja la probabilidad que dos contenidos que colisionan usando SHA256, también colisiones en SHA1.

Usos de los códigos hash en la Blockchain

Los códigos Hash son usados para muchos propósitos, sobre todo para comprobar la existencia de una secuencia de datos, por ejemplo si usted desea comprobar que yo soy el dueño de un registro, solo debería indicar que "texto secreto" que permitió generar un código hash, si conozco ese "texto secreto", todos podrán comprobarlo con tan solo calcular el hash del valor que estoy mostrando.

Por ejemplo:

Cuál es el valor que genera este hash SHA256:

```
267bd504a88a8c7c36da93c315cd0e285ba9e2378d11940
                bf9700f59ebf7aed6
```

Solo dos personas pueden realmente saben cuál es la frase que genera el código hash anterior, los autores de este libro:

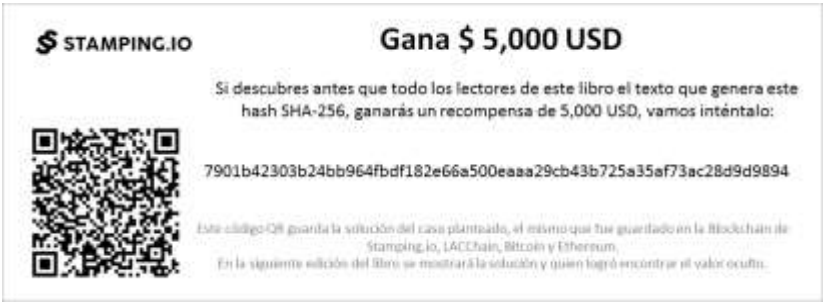
```
SHA256("Soy Jorge y José")
```

Resultado:

```
267bd504a88a8c7c36da93c315cd0e285ba9e2378d11940
bf9700f59ebf7aed6
```

¿Esto método es seguro, cómo para confiar la identificación de una persona?

Probablemente, es tan seguro como utilizar una contraseña pero, al menos tenemos la seguridad que nadie sabe el secreto que se esconde detrás de ese hash, más que el que la generó y créanme que utilizar la fuerza bruta no es tan fácil de lograr, sino atrévete a participar de este reto:



Firmas Criptográficas

Las firmas ciegas

Es un protocolo de firma digital creado por David Chaum que ha sido utilizada para esquemas dinero electrónico (por ejemplo ecash) y esquemas de voto electrónico. Este protocolo permite a una persona obtener un mensaje firmado por otra persona o entidad, sin revelarle información del contenido del mensaje.

David Chaum se motivó a crear este protocolo porque, cada vez que llamaba por teléfono para comprar un producto usando su tarjeta de crédito, o para suscribirse a una revista o pagar algún impuesto, se preocupaba por que esa información terminaba en alguna base de datos que se encuentra alojada en algún lugar del mundo, lo que trasgrede nuestro derecho a la privacidad y nos expone a ser víctimas de un fraude financiero.

Para tener una idea intuitiva del concepto de firma ciega podemos establecer una analogía con la firma del "documento de cargo", ese documento que firmamos manualmente cuando el mensaje nos entrega un sobre, sin saber cuál es el contenido interior del sobre, firmamos el cargo sin saber el contenido de dicho documento. Este tipo de firma permite comprobar que el documento firmado es el mismo que estaba en el sobre que se entregó sin conocer el contenido, de ahí viene el nombre "firma a ciegas".

Por ejemplo con este tipo de firmas manuales podríamos establecer el siguiente esquema de votación sin usar medios electrónicos:

- El votante toma su papeleta de votación y la envuelve en un sobre de manila que tiene papel de calco, para luego enviarlo en un sobre con su remitente al encargado del conteo.
- El encargado del conteo firma sobre el papel calco que se encuentra sobre el sobre de manila (sin ver que hay en el interior), y devuelve el paquete en otro sobre. Esta acción permitirá asegurar que el votante se encuentra autorizado para votar asegurando además el secreto del voto.
- Para el día de las elecciones, cada votante manda su papeleta con su voto marcado al contador de votos en un sobre sin remitente, para mantener el anonimato.
- Posteriormente estos sobres pueden ser abiertos y contados públicamente. Si cada votante recuerda algún elemento característico de su papeleta, como el patrón en las fibras del papel, podrá reconocer su voto en el conteo.

Capítulo 3
Tokenización de activos digitales

Muchas personas en el mundo están sobre exagerando acerca del verdadero uso de la Blockchain. Proponen a que todo proyecto que se les ocurra deba ser "Blockchainado" con el propósito de transparentar las transacciones o incrementar la seguridad de la información. En realidad la mayoría de los casos expuestos podrían ser resueltos utilizando una sencilla base de datos central y no dejaría de ser transparente y segura.

Entender el funcionamiento de una Blockchain es sencillo; detectar un correcto uso no lo es. Quizás porque a la fecha son muy pocas o nulas las aplicaciones donde se ha visto obligada a tener "la necesidad" de usar esta tecnología. Los emprendedores se motivan a forzar el uso de Blockchain con el objetivo de usarlo como estrategia comercial y no como una real necesidad tecnológica. No hay que olvidar que el objetivo de usar una determinada tecnología deber ser motivada para resolver un problema real, y no para impresionar a un mercado aprovechando su desconocimiento ya que esto podría traer como consecuencia un manoseo exagerado del término Blockchain que podría conllevarlo a su muerte prematura.

Hasta la fecha, se ha demostrado que los casos de uso donde se puede emplear la arquitectura Blockchain, son para el registro de pruebas de existencia (evidencias digitales) y pruebas de propiedad (tokenización). Te invito a conocer cada uno de estos tipos de usos.

Primer tipo de uso: "Las Evidencias Digitales"

Pruebas de existencias

Dado que la Blockchain cuenta con un servidor de sellado de tiempo descentralizado, donde varios nodos participantes están registrado simultáneamente la información y para su correcto funcionamiento se requiere que todos los relojes se encuentren sincronizados; éste simple hecho es aprovechado por muchas organizaciones para demostrar que "algo" ha existido en un momento del tiempo.

El uso de la Blockchain para registrar de evidencias digitales que permitan demostrar matemáticamente la existencia de una secuencia de datos o de un documento en un momento del tiempo, permite que muchas aplicaciones adopten fácilmente la Blockchain para un caso de uso real. Estas aplicaciones utilizan a la Blockchain como un *"Notario digital",* con un costo mucho menor y con un grado de eficiencia superior, al otorgado por las autoridades de sellado de tiempo o TSA. Además, no solo sirve para ´realizar una *prueba de existencia*, sino también, puede ayudar a demostrar su originalidad y que no ha sido adulterado desde su creación, es decir: permite hacer *pruebas de integridad* del contenido.

Los proceso de transformación digital que las empresas vienen adoptando, así como a digitalización de sus procesos ha generado

la necesidad de contar con un tercero de confianza que permita dar fe que algo sucedió en un momento del tiempo, sobre todo cuando hablamos de expresiones de voluntad. Vivimos en una etapa de la humanidad donde pequeñas aplicaciones de clase mundial están destronando a grandes corporaciones mundiales, muchos la llaman la nueva revolución industrial. El principal activo de las empresas es la información por lo que muchos ejecutivos exitosos le prestan su mayor atención a la calidad y validez de sus datos.

La forma como se transmiten datos desde una entidad u organización, hacia un tercero es utilizando datos y/o documentos, necesitamos garantizar la integridad de esa transmisión, así como la autenticidad de los mismos pero también poder demostrar la existencia de esa transmisión en un momento del tiempo, sobre todo cuando deseas integrarte con un desconocido. Para lograr esto, existe la figura del tercero de confianza o lo que es lo mismo, un notario digital, que custodia las comunicaciones entre las partes concediéndoles validez probatoria en los tribunales de justicia.

El tercero de confianza archiva las comunicaciones entre las partes, durante un plazo largo de tiempo, en el caso de la Blockchain es inmutado de por vida, al menos eso es lo que prometen los creadores de esas redes. En estas bases de datos distribuidas se guarda una copia de la fecha y la hora de las mismas, el contenido o una marca criptográfica que permite demostrar la existencia del contenido y por supuesto, dando fe de la creación, verificación y validación de su existencia. Como veremos más adelante estas soluciones se apoyan de tecnología de criptográfica asimétricas, firmas electrónicas, cifrados digitales, certificados, webhooks, sellos, entre otras.

Cuando un negocio mueve transacciones en el ámbito electrónico, necesita enfocarse y gestionar tres puntos importantes que le ayudará a garantizar la seguridad legal de sus operaciones digitales. No sólo es suficiente enviar o recibir datos y/o documento, sino que además debes tener constancia de otros puntos como:

- Integridad del contenido: Contar con un mecanismo que asegure que la información transferida no ha sido modificado desde su envío hasta su recepción.
- Autenticidad: Que el emisor y receptor son quien dicen ser y que no se vulnere la seguridad del sistema, además de garantizar la confidencialidad y privacidad de la información.
- Trazabilidad: Que se conozca fehacientemente su estado. Es decir, si ha sido recibido, abierto, leído, rechazado, etc. Pero lo más importante, que se pueda demostrar para evitar el repudio de alguna de las partes.

Los principios anteriores son esenciales pero muchas organizaciones no son capaces de demostrar evidencias de su existencia, por ejemplo, delante de algún juez, que, efectivamente, el documento realmente se ha enviado, firmado, recibido, tratado, etc. y qué, quién dice que eso se ha producido. La Blockchain actúa como un "tercero de confianza" descentralizado, a pesar de no ser parte activa en la reclamación nos ayuda a demostrar que alguien miente en caso de necesitarse.

Para contar con un mecanismo seguro que ayude a funcionar como un tercero de confianza para demostrar pruebas de existencias, autenticidad e integridad de los datos utilizando una

base de datos distribuida o descentraliza se necesita al menos estos tres requisitos claves:

1. Un lugar seguro donde se guardan los datos

La búsqueda de una piedra la suficientemente confiable donde se pueda registrar las transferencias que se realizaron en un momento del tiempo, no es tan fácil de encontrar, como cuando los escribes en un papel. Estarás de acuerdo conmigo que cuando el mundo no era digital, dejar evidencias de algo, era más sencillo, solo tenías que escribirlo en un papel y firmarlo por los participantes. Aunque guardar el papel por muchos años siempre ha sido un reto que la sociedad tenía que afrontar.

Desde la digitalización de las operaciones empresariales, algunas cosas han cambiado. Las empresas se encuentran enfocadas en la constante búsqueda de mecanismos que le ayuden a agilizar sus operaciones, todas innovan para ganarle al reloj, las empresas modernas no se pueden dar el lujo de esperar ya que hay cientos o miles de startup listas para ganarles clientes con productos cada vez más enfocados y especializados a ciertos nichos del mercado. Cómo vamos a dejar sentado que algo paso en un momento del tiempo si tratamos de hacer las cosas cada vez más rápido y menos engorrosas, además que tenemos el reto de garantizar que los datos no se cambiaran por nadie desde su creación, tan igual como antes lo hacíamos guardando el papel donde todos firmaron.

La Blockchain no solo actúan como los testigos digitales que necesitan para dar fe que algo paso en un momento del tiempo, nos referimos a esos nodos que se encuentran conectados entre sí. Sino que también nos ayuda a demostrar la autenticidad y veracidad de una evidencia digital sin recurrir a firmar un documento físico – haciendo uso de firmas digitales y criptografía.

Las firmas de criptografía asimétrica no son nuevas en el mundo, la Blockchain no las inventó, hace años que se utilizan en todo el mundo, por lo general son usadas para firmar documentos con el propósito de identificar a los participantes y expresar la manifestación de voluntad, la ley lo ampara y evita el repudio legal de alguna de las partes firmantes.

La Blockchain usa ese mecanismo para firmar las transacciones y evitar que alguien se haga pasar por otra persona con el afán de mentir o hacer un acto malicioso.

Ejercicio: Orden de compras

Antecedentes

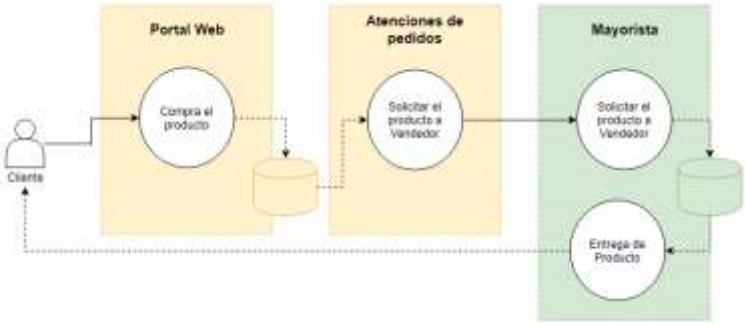
Imaginemos que tenemos dos organizaciones que tienen un vínculo comercial bajo la modalidad de mayorista-minorista. El minorista desea enviarle una orden de compra a la empresa mayorista para atender un pedido.

Cada una de las empresas cuenta con su propio control de inventarios y sistema ERP. Sin embargo deben intercambiar información entre ellas para atender el pedido.

En minorista ha creado un portal web que permite que sus clientes puedan solicitar cualquiera de los productos que ofrece y promete hacer la entrega en menos de 24 horas.

El minorista no cuenta con almacenes sino aprovecha los almacenes de los mayoristas. Cuando recibe un pedido emite una orden de atención al mayorista para que realice la entrega del producto, a fin de mes se realiza una liquidación de su deuda.

A continuación se muestra este proceso de negocios:



El problema

El negocio ha comenzado a generar en promedio 2,000 transacciones mensuales, el minorista está pensando en agregar nuevos productos del mayorista a su plataforma pero ha surgido en varias ocasiones discrepancia con respecto a los pedidos solicitados. Por lo que están buscando una alternativa segura que permite que ambos estén 100% seguros que el pedido ha sido realizado, entregado, facturado y cobrado. De solucionar el problema podrá atender agregar nuevos productos y nuevos mayoristas.

¿Cómo se puede solucionar el problema haciendo uso de la Blockchain?

Este problema a simple vista parece ser sencillo de solucionar usando una plataforma de intercambio electrónico de datos o usando micro-servicios, sin embargo, el problema de la automatización no es el tema central de la problemática dado que:

1.- El mayorista puede recibir pedidos a nombre del minorista, pero se trata de un fraude cibernético, el mayorista procederá a hacer la entrega del producto al supuesto cliente, sin embargo, se

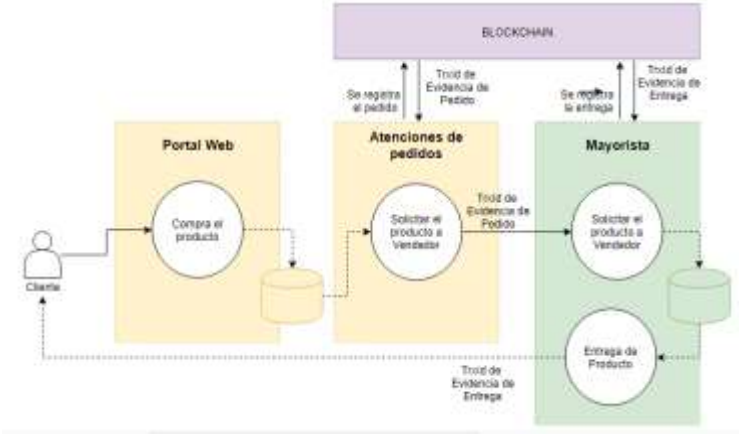
trataba de un fraude, finalmente en el momento de la facturación entre ellos surgirá un inconveniente.

2.- El mayorista puede "equivocarse" en el momento de la entrega o sencillamente ser engañado por el servicio de entrega de productos, nuevamente generando un inconveniente comercial entre ellos.

3.- El cliente puede realizar pedidos al mayorista y luego negar que estos pedidos fueron realizados, para evitar la gestión de cobranza.

Podemos seguir enumerando problemas típicos de una plataforma de integración de datos, sin embargo el problema entre ellos radica en que ambos cuentan con sistemas contables distintos. Por lo que cada uno, podría tener una versión distinta de la verdad o negar la existencia de algo confiando en que el otro participante no lo puede validar.

La solución

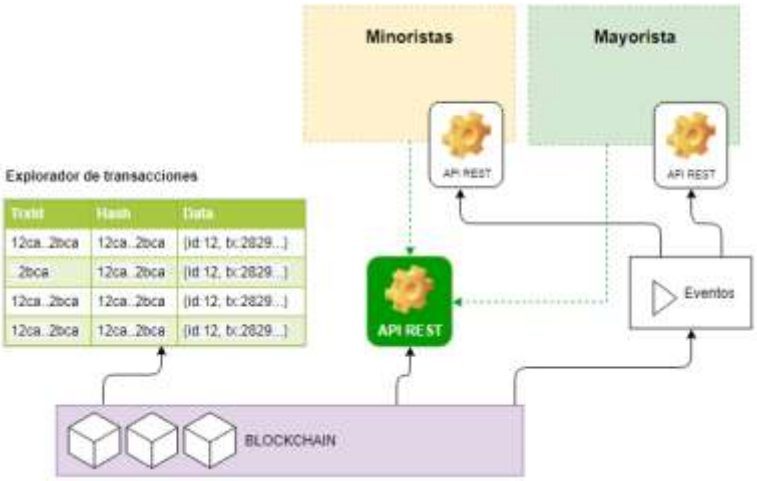


Si deseamos una solución sencilla recurriendo a las evidencias digitales, se puede resolver el problema creando un log compartido entre el minorista y mayorista de tal forma que ambos no nieguen

ni repudien la existencia de algo, por ejemplo: Cuando el minorista coloque una orden de compra, registrará en la Blockchain los datos de la orden, de tal forma de dejar constancia del pedido y evitando que luego pueda modificar los datos en sus sistemas ERP. La Blockchain le retorna un identificador de la transacción al que le llamaremos "TrxId", ese código es asociado en el ERP del minorista a la orden del pedido, el mismo que se envía al mayorista junto a los datos de la orden, pudiendo el mayorista comprobar que los datos se encuentra en la Blockchain, al menos los datos más importantes como: Fecha de pedido, fecha de entrega esperada, cantidad por ítem, lugar de entrega, condiciones y características de despacho, entrega y configuración del item.

Del mismo modo, cuando el mayorista planifica y realiza la entrega del producto al cliente, lo registra en la Blockchain con la finalidad de alertar y dejar evidencia de la realización de dicho acto comercial.

2. Mecanismo para localizar Transacciones



Existen varias formas de explorar los datos dentro de una Blockchain, una herramienta de visualización que nos permite encontrar o localizar cualquier transacción dentro de la Blockchain se llama explorador de transacciones o explorador de bloques, esta herramienta es una aplicación web que da acceso a los bloques, funcionando como un motor de búsqueda que se encuentra conectado a la cadena de bloques. Su función principal es permitir que cualquier persona con una conexión a Internet pueda seguir en tiempo real todas las transacciones realizadas en la red, da igual el nivel técnico y profundo conocimiento del usuario.

Por lo general el explorador de bloques muestra información de los bloques y las transacciones que la red está anclando en tiempo real, dando un fuerte énfasis en los nuevos bloques que se están agregando y confirmado en la cadena. Generalmente, se muestra la siguiente información:

- **Altura del Bloque**: La cantidad de bloques creados, se cuenta desde que se generó el primer bloque llamado *génesis*. Cada nuevo bloque aumenta este número en uno. También se indica la fecha de cuándo fue creado el bloque, el nodo responsable de su creación y las transacciones que lo componen.
- **Antigüedad**: El momento en que los mineros aceptan el bloque.
- **Confirmación**: La información más importante es el estado de transacción. Si una transacción es «sin confirmar» o «pendiente», esto significa que se encuentra en la cadena, pero ningún minero la ha aceptado aún. En Bitcoin demora en promedio diez minutos en confirmarse las transacciones, las transacciones se envían a un nuevo

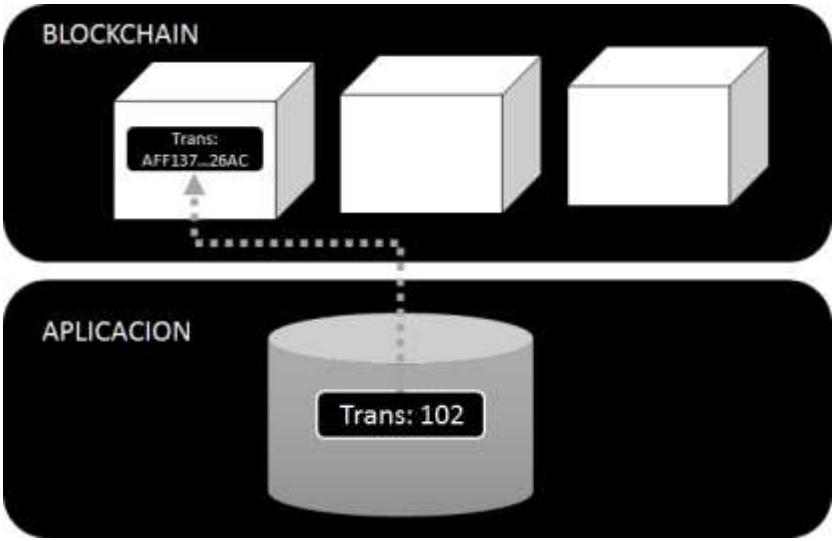
bloque. Consideramos que una transacción de BTC ha sido realizada con éxito después de al menos 6 confirmaciones.

- **Lista de transacciones** (TX): lista de las transacciones incluidas en el bloque.
- **Recompensa**: comisión que será utilizada para el pago de los mineros. Tenga en cuenta que no todas las Blockchain brindan recompensas a los mineros.
- **Resuelto por**: El grupo de mineros trabajando en conjunto para terminar los bloques.
- **Tamaño**: El tamaño de la transacción obtenida al agregar el tamaño de cada transacción incluida en el bloque. Estos datos están siempre en bytes.

Si bien existen muchos exploradores, observamos que existen muchas similitudes entre ellas. Sobre todo, la mayoría de ellas permite localizar una transacción en base a su identificador; por lo que se recomienda asociarlo con el registro anclado de la base de datos.

Al igual que con un motor de búsqueda, el usuario debe ingresar obligatoriamente una consulta de búsqueda. Por ejemplo, el hash de una transacción, comúnmente conocido como el TXID (un único código de 64 letras escrito en hexadecimal, es decir está confirmado por números del 0 al 9 y letras de la A a la F. Este código es utilizado para identificar unívocamente una transacción dentro de la Blockchain. Al buscarlo en el explorador, automáticamente, una página con detalles de la transacción se muestra al usuario, pudiendo validar su registro. La mayor parte del tiempo, una transacción contendrá varias entradas (input) y salidas (output), en la medida en que permite ahorrar tiempo y dinero. El siguiente gráfico muestra la forma como se registra la

transacción 102 y se genera el código de la Blockchain: AFF137…26AC



Otra forma de validar una transacción es haciendo uso de las API Rest que la mayoría de Blockchain exponen, donde a través de este micro-servicio se puede registrar o consultar el estado de una transacción. Por lo general, estas APIs de consultas usan el identificador de la transacción (TXID) para localizarla, en unas pocas, como es el caso de stamping.io se puede realizar consultas desde el hash que representa la evidencia registrada, aunque son muy pocas las que permiten esta funcionalidad.

Otras plataformas Blockchain permiten hacer consultas haciendo uso de llamadas a procedimientos remotos (RPC) o usando SDK de desarrollo. En realidad, existen variadas formas de automatizar

las consultas de las transacciones con el objetivo de integrarlas a sus aplicaciones.

Los eventos es otra forma de automatizar las consultas, aunque en este caso el que ejecuta el servicio es la Blockchain, haciendo una llamada a un servicio que los participantes expongan ante un evento determinado que se registra en la Blockchain. La forma como se utiliza esta funcionalidad es muy similar a las técnicas de webhook o alertas que se usan para integrar plataformas, con la diferencia es que el log de integración es compartido y aceptado en consenso por todos los participantes, evitando de esta manera que en el futuro exista el repudio del registro por alguno de ellos.

3. Comprobación

De qué sirve almacenar algo con la esperanza de validar su existencia en un momento del tiempo, si es imposible de demostrarlo. Te imaginas hacer un contrato firmado en un papel que se desvanece en el tiempo. La demostración de la existencia de un registro es quizás la parte más débil que por ahora tiene la Blockchain, ya que se necesita recurrir a las matemáticas pero, a muchos eso les da miedo. Hagamos un ejemplo:

Imaginemos que deseamos usar la Blockchain de Bitcoin o Ethereum para demostrar la existencia de un documento en el futuro. Por si no lo sabias, no se puede registrar un documento ni ningún archivo binario en la Blockchain, dado al poco espacio que se asigna a un transacción, si alguien guardara un documento binario eso conllevaría a crear un bloque bastante grande y todos los nodos que almacenan una copia de la cadena de bloques necesitarían un ancho de banda grande para la transferencia de la información y un disco enorme para almacenarlo, definitivamente por ahora, eso es inviable. Por lo tanto, para hacerlo se debe

recurrir a las matemáticas y la criptografía. Lo primero que se hace es convertir un documento en algo que lo represente. Por muchos años los seres humanos nos hemos registrado en una base de datos usando nuestras huellas digitales y/o firmas, esos datos son los que nos representan y que de alguna manera nos ha permitido demostrar nuestra identidad, de la misma forma se requiere buscar una huella digital que represente al documento que deseamos registrar.

Para identificar al documento no podemos crearle un código cualquiera porque, eso impediría demostrar en el futuro que ese documento está asociado al código. Por más que asegures que ese código le corresponde, nadie necesariamente tendrá que confiar en tu palabra, recuerda que la confianza se debe depositar en el mismo sistema y no en las organizaciones ni en las personas. No puedes ser juez y parte al mismo tiempo, ni mucho menos centralizar la verdad. Incluso si optaras por colocarle el código dentro del documento, sería en vano, nadie tiene la garantía que el código no haya sido reutilizado en otros documentos o que no lo haya colocado recientemente.

Para lograr una correcta identificación se necesita buscar un código que permita identificar inequívocamente al documento, que sea único o al menos de difícil duplicación, que sea confiable y matemáticamente o científicamente demostrable, como las huellas digitales de tus dedos que permiten te identificarte. En la práctica se crea un valor único desde el mismo documento usando el valor del hash del tipo SHA2[7], este valor es el más usado en las Blockchain y firmas digitales.

[7] Si no sabes de que se trata el hash SHA2 por favor ver el capítulo 3.

Imaginemos que para nuestro ejemplo se genera el código SHA2 del código binario de un documento PDF que deseamos registrar como evidencia digital, el valor que ese algoritmo nos genera nos da un valor hexadecimal de 256 bits (64 caracteres):

```
SHA256:
b5d2081efaac14527f60d15146acf84e653e1df817f0cfa95f222a422d8c220d
```

Ya contamos con la primera parte del reto, si te das cuenta cualquiera podrá comprobarlo con tan solo calcular el hash del documento, y si alguien modifica su contenido, el nuevo documento generaría un nuevo hash, alertando que el documento ha sido adulterado o es falso.

El hash de un documento es similar a la huella digital de tu dedo, aunque como veremos más adelante, existe la posibilidad que dos documentos generan el mismo hash, la probabilidad que ambos tengan contenidos similares y un mismo patrón es muy remoto, al menos, hasta la fecha no ha podido demostrarse que existe una forma de hacerlo en forma intencional, aunque la casualidad podría jugar una mala pasada.

Pruebas de registros de evidencias digitales

La necesidad de registrar una evidencia digital en la Blockchain es demostrar la existencia, propiedad, originalidad o integridad "de algo" cuando se necesite o para evitar el repudio de alguno de los interesados. En este caso, la Blockchain funciona como una plataforma de notariado virtual que permite dar confianza entre los participantes del sistema.

También se utiliza para demostrar públicamente, que una secuencia de datos no se ha cambiado en el tiempo, tiene un propietario y que es real, las pruebas que se pueden realizar basándose en un registro en la Blockchain son cuatro:

- Prueba de existencia
- Prueba de integridad
- Prueba de propiedad

Prueba de existencia

Es una prueba que se realiza con el objetivo de demostrar que "algo" existió en un momento del tiempo. Para que se pueda realzar esta prueba se debe calcular el hash del contenido que se registró en la Blockchain, luego se busca en la Blockchain para comprobar que existía en un momento del tiempo, si existe, se observa la fecha de creación y con eso se demuestra la fecha en que fue registrado, caso contrario no se podrá comprobar su existencia en un momento del tiempo. Recuerda que nadie puede entrar a la Blockchain a cambiar la fecha de un registro ni ingresar un registro que no existía.

Prueba de integridad

Es muy parecida a la prueba de existencia, solo que esta vez se necesita que el contenido este asociado a un registro de la transacción de la Blockchain, con la finalidad de validar que el hash del contenido es similar al valor que se encuentra registrado en ese registro de la Blockchain, de tal forma que se puede validar que el contenido de la transacción o documento no ha sido modificado.

Prueba de propiedad

Para probar la propiedad de un documento o secuencia de datos, solo se debe verificar la dirección del dueño (owner) que registro el

activo digital en la Blockchain. El owner es el único que puede transferir el registro o la propiedad de algo que se ha registrado en la Blockchain, para hacerlo hace uso de su llave privada, demostrando de esa forma que es el dueño o propietario del registro.

Algunos ejemplos de evidencias digitales

Una entidad gubernamental emite un documento que contiene un certificado que autoriza a una empresa para realizar ciertas actividades comerciales que requieren de ese consentimiento previo. El documento es emitido en formato pdf.

Para evitar las falsificaciones de documento, la entidad puede guardar en la Blockchain la "huella digital" del documento (Hash), de tal forma que cualquier cambio del contenido, por mínimo que sea, el valor del hash cambiará.

El algoritmo de hash del tipo SHA256 es muy común que sea utilizado para obtener esta huella digital, además que es muy fácil demostrarlo ya que si se aplica el cálculo sobre el archivo digital siempre dará como resultado los mismos 64 caracteres hexadecimales, más adelante vamos a profundizar el tema del "hash".

Este código hash se guardará en la Blockchain con la finalidad de demostrar que existió ese valor en ese momento del tiempo, los nodos serán testigos de su existencia y nadie podrá negarlo.

Cuando este hash sea registrado se retorna un código de transacción que permite buscar los datos dentro de la Blockchain, el mismo que será asociado al documento para facilitar su comprobación, es común que muchos desarrolladores usen un

código QR dentro del documento para facilitar las pruebas de existencia e integridad del contenido.

Tipos de inmutación de evidencias digitales

Una evidencia digital es una cadena de caracteres conformados por un resumen criptográfico basado en el algoritmo de hashing, por ejemplo para esta secuencia de datos:

ID	Date	Time	Product	Status	Price	Quantity	Customer
1	12/11/2018	12:11:21 PM	PR013	Ok	19	1	8r9Gw

Calculando el valor hash de la evidencia digital de los datos expuestos:

SHA1('143445.507881944443445.5078819444PR013Ok1918r9G')
Valor: 8b0aa31e88a68c93f3cffe50aeb97fb4f88adee1

Cada empresa puede transferir las evidencias digitales a la plataforma de registros descentralizada basada en la Blockchain, en un punto de inmutación, siendo ideal que cada organización cuente con un nodo instalado en su red local, en ese caso, se puede delegar el registro de cada log que actualmente se encuentra en la base de datos para que sea gestionado por la plataforma de contabilidad distribuida.

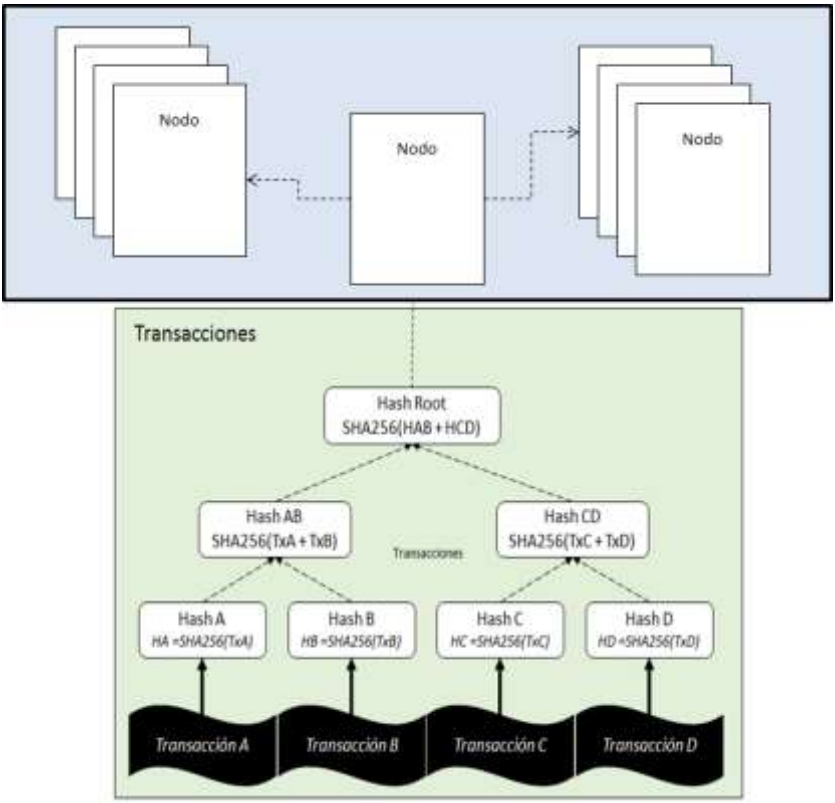
Si no se cuenta con un nodo Blockchain dentro de su red local, y se requiere usar un nodo que se encuentra en la nube, el problema, por supuesto, es evitar que las empresas tengan que transferir todos los registros, evitando "latencia de datos" producto de estar enviando constantemente información por internet.

La red de nodos de evidencias digitales, donde cada empresa que utiliza la solución es parte del consorcio, constituye una autoridad central de confianza descentralizada, que verifica que cada transacción sea registrada correctamente, emitiendo un certificado de evidencia forense cuando se requiera, dando fe de la existencia de una secuencia de datos en un momento determinado del tiempo.

Agrupando evidencias digitales

En algunas ocasiones se realizan múltiples transacciones por segundo, y registrarlas en la Blockchain podría ocasionar problemas de rendimiento, debido a que los nodos requieren sincronizar los datos con los otros nodos de la red, por lo tanto, en muchos casos es recomendable solo guardar un hash que represente un conjunto de transacciones, y que se pueda demostrar su existencia e integridad cuando se necesite. Existen tres métodos que se utilizan para realizar esta agrupación:

Método 1: Arbol de Merkle



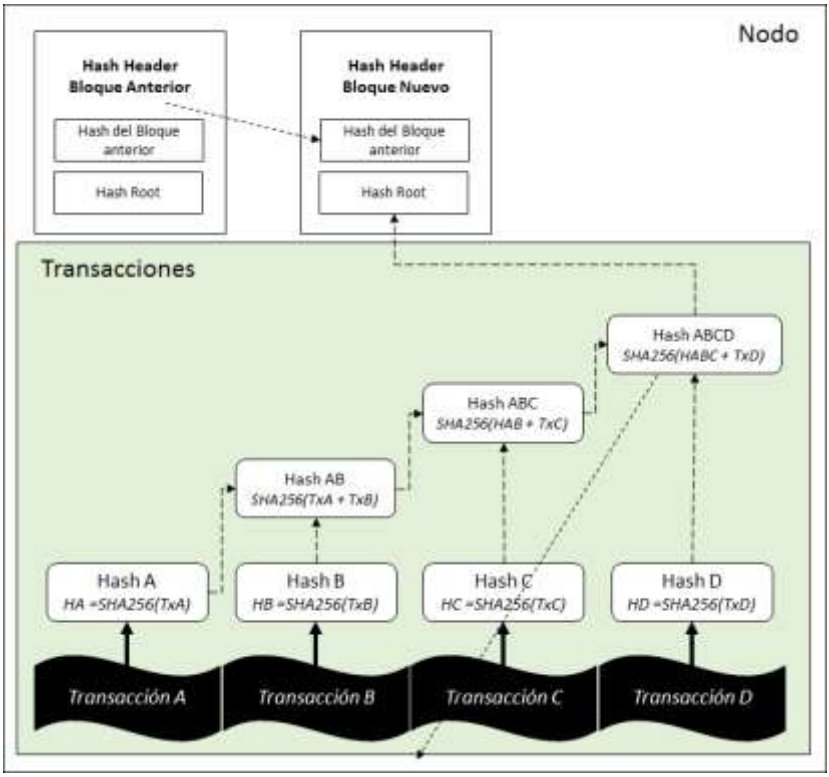
El árbol de merkle o árbol hash fue creado en 1979 por Ralph Merkle, consiste en crear una estructura de datos que contiene en cada hoja el valor de un hash que representa a una determinada transacción. Cada par de registros se calcula un nuevo hash en forma recursiva hasta que al final se obtiene un hash raíz que representa a todos los hash agrupados. Esta técnica permite que gran número de datos separados puedan ser agrupados en un único valor. Lo más importante es que esta forma de agruparlos proporciona un beneficio al momento de verificar el registro,

siendo un método seguro y eficiente, sobre todo cuando se trata de grandes estructuras de datos.

Cuando se utiliza la Blockchain de Stamping.io, normalmente el hash de cada raíz va firmado por un agente automatizado, para asegurar su integridad y que la verificación sea totalmente confiable. Además cada 30 minutos se agrupan todas las transacciones que se han recibido en ese lapso de tiempo, al calcularse un hash que representa el árbol, este es enviado a Blockchain públicas como Bitcoin, Ethereum o evidenChain.

Para demostrar la existencia de una transacción o documento, se calcula el hash y con tan solo tener los hash de sus vecinos se puede demostrar el registro en la Blockchain. No se necesita contar con todos los hash que forman el árbol sino solo con los vecinos, por ejemplo en el gráfico adjunto, veremos que si deseamos mostrar la transacción A solo se requiere e hash de B y luego el hash que compone CD, de este modo se puede llegar al hash raíz que es finalmente el hash que se encuentra anclado en la Blockchain. Si bien es cierto en el árbol de ejemplo solo existen cuatro transacciones pero, en el caso de ser miles o millones de transacciones se verá que solo se requiere una cantidad limitada de los hash para hacer la demostración, siendo un método extremadamente eficiente para comprobar la existencia de una secuencia de datos, ya que si un árbol está compuesto por N elementos, se puede comprobar si cualquier elemento de datos está incluido en el árbol con un máximo de *2*log2(N)* cálculos, por ejemplo si tenemos cien mil transacciones solo necesitaremos menos de treinta y cinco combinaciones para demostrar su existencia, en un millón menos de cuarenta y en cien millones de transacciones, solo necesitas menos de cincuenta y cuatro combinaciones.

Método 2: El hashlink (Hash Entrelazados)



Es un método de agrupación de hashes creado por Arson Group, fue publicado por primera vez en el año 2012, cuando se necesitaba demostrar la existencia la secuencia de los datos en un proyecto para una empresa de telecomunicaciones. A diferencia de los árboles de Merkle, no se necesita realizar un corte para empezar a calcular el hash raíz. Por lo que este método es muy útil cuando se requiere anclar transacciones en línea y se desea contar con un mecanismo de inmutación.

En toda base de datos existen registros que en el eventual caso que sean eliminados se perderían evidencias de transacciones, seguridad o autorizaciones importantes, por lo que siempre ha sido un reto importante para los administradores de base de datos, jefes de seguridad informática o directores de sistemas, evitar que estos datos puedan ser eliminados o modificados.

El uso de hash para evitar que los datos de una fila puedan ser modificados, proporcionando una parte de la solución. Estos hash son algoritmos de resumen criptográficos que permiten obtener una secuencia de caracteres que representan a una secuencia de datos pero, los beneficios principales se pierden si una persona realiza la modificación de un registro y re-calcula el hash de validación, por lo que se requiere entrelazar con los siguientes registros, obligando a re-calcular toda la secuencia de datos y registrar cada cierta cantidad de filas el hash entrelazado para evitar que sea modificado.

Pretender hacer un registro por cada fila en una plataforma externa para evitar la modificación de los datos, es una solución que técnicamente podría generar problemas de rendimiento, además generaría un problema de seguridad por lo que se requiere conexión a Internet en forma permanente.

La solución que proponemos es crear link enlazados entre los hash que representan cada registro de a tabla que se desea inmutar (HashLink), y cada "x" filas el valor del hash entrelazado se registra en una red de igual-a-igual (Blockchain), evitando que los datos puedas ser adulterados con el consentimiento del DBA o encargados de entregar credenciales de acceso.

Si resumimos la seguridad de muchas base de datos se centra en ciertas tablas de trazabilidad o auditoria (comúnmente llamadas

logs de transacciones), que prácticamente se encuentran en todas las bases de datos corporativas y fungen de ser una tabla con la suficiente autoridad para ser considerada como la verdad absoluta y extrema de las transacciones o registros que un proceso ha realizado.

Es cierto que el sistema funciona suficientemente bien para la mayoría de las transacciones, aún se sufre las debilidades inherentes del modelo basado en la confianza al administrador de la base de datos, eficiencia de los desarrolladores, responsabilidad del encargado de la seguridad informática, entre otros. Si nos fijamos bien, la confianza no se encuentra en las tablas de auditoria sino en las personas que las administran.

El reto de crear registros o transacciones completamente no reversibles (inmutables) no siempre es logrado en la mayoría de las compañías, por más que existan mecanismos de seguridad y privilegios, se cuenta con la posibilidad de reversión, la necesidad de confianza se extiende a tener una tercera entidad que evite que eso suceda con la finalidad de evitar que la historia real de las transacciones, sean registradas tal como sucedió.

Una solución simplista sería enviar toda la tabla de auditoria a un tercero de confianza basada en Blockchain, donde una red de nodos puedan certificar que una secuencia de datos fueron creadas en un momento del tiempo y no han sido adulterados, sin embargo no todas las compañías, por ahora, cuentan con un nodo de Blockchain interconectado con otros nodos para generar la confianza que se necesita para evitar la adulteración.

En caso de utilizar un nodo de confianza en la nube, el reto de evitar el problema de rendimiento por la latencia de conectividad se suma a la complejidad de la solución, para que la solución este

completa se requiere evitar que todos los registros sean enviados uno por uno al nodo descentralizado, por lo que se deberá diseñar un mecanismo que entrelace los hash que representan a cada fila de la tabla de transacciones y a través de un algoritmo de resumen criptográfico que se entrelace con el registro anterior, forzando a un intruso que desea realizar un cambio, a realizar una serie cálculos de las nuevos hash para las filas siguientes.

Establecer de un canal de comunicaciones como un tercero de confianza que permita validar que los datos, basado en pruebas criptográficas en lugar de basarse en la confianza a las personas, permitirá que los datos registrados en esas tablas de auditoria sean considerados como pruebas forenses con valor probatorio legal, sin la necesidad de tener que contar con un notario, fedatario o autoridad de sellado de tiempo.

En éste documento, proponemos una solución al problema de inmutación de registros mediante el uso de un servidor de marcas de tiempo distribuido para generar la suficiente prueba matemática del orden cronológico de las transacciones. El sistema es seguro dado que todos los nodos de la red son honestos, dado que la red Blockchain implementada es permisionada, evitando que cualquier persona sin autorización pueda instalar nodos en nuestra red de alta confianza.

Por ejemplo, en el sistema financiero los datos de "originación" de una operación de crédito fueron utilizados para calcular el rating y por consecuencia la tasa de interés, se imaginan que pasaría si luego de otorgar el crédito, esos datos se modifican, en el caso de una auditoria el personal de riesgo estaría expuesto en un caso de fraude. Los pagos de amortización de un crédito, imagínese que por error o en forma intencionada estos sean alterados, no

cuadraría el saldo de la deuda con los movimientos de las amortizaciones.

Las operaciones o movimiento de una cuenta pasiva, los otorgamientos de privilegios de acceso a un determinado sistema, los logs de operaciones fraudulentas, las operaciones que deben ser reportadas por el oficial de cumplimiento para evitar lavados de activos, los bloqueos de cuentas o tarjetas, los reclamos reportados por los clientes, las atenciones a los pedidos de cobranzas coactivas, etc.

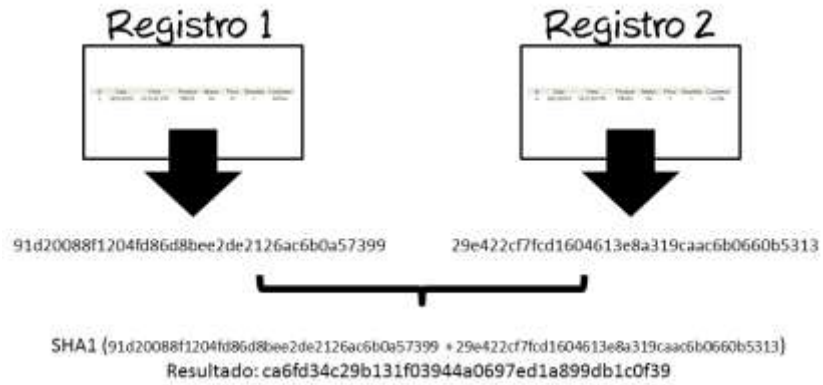
En las entidades gubernamentales las cobranzas por servicios de procedimientos TUPA, la lista de documentos electrónicos, digitales o digitalizados que han sido recibidos por mesa de partes, las orden de compras, las conformidades de servicios, las vistas de funcionarios, los pagos de viáticos, las denuncias y reclamos, etc. Podrían ser fácilmente modificados en el sistema, el uso de un hashlink inmutado en la Blockchain reduciría muchos de los fraudes y a la vez transparenta los procedimientos.

En este capítulo se ha demostrado que la mejor forma de evitar la latencia en el registro de la plataforma de registro de evidencias digitales, es manejar una red secuencias de hash entrelazadas entre sí, tal como se plantea en el siguiente gráfico:

ID	Date	Time	Product	Status	Price	Quantity	Customer	Hash
1	12/11/2018	12:11:21 PM	PR013	Ok	19	3	Br9Gw	[illegible]
2	12/11/2018	12:11:24 PM	PR038	Ok	9	1	LvJDk	[illegible]
3	12/11/2018	12:12:11 PM	PR035	Ko	33	1	Lz7Wn	[illegible]
4	12/11/2018	12:12:22 PM	PR035	Ko	12	1	eVhah	[illegible]
5	12/11/2018	12:12:25 PM	PR014	Ok	12	2	pExT7	[illegible]
6	12/11/2018	12:13:02 PM	PR019	Ok	3	2	x6v5F	[illegible]
7	12/11/2018	12:14:01 PM	PR013	OK	2	1	HVHI	[illegible]
8	12/11/2018	12:14:35 PM	PR013	Ok	12	2	aBGxh	[illegible]

En la figura anterior se muestra una lista de transacciones donde se ha calculado el hash de cada registro, utilizando el algoritmo de resumen criptográfico SHA1, pudiéndose utilizar cualquier de los que el cliente desea, incluso SHA256 o SHA512.

Si nos fijamos en los dos primeros registros, se obtienen dos hash diferentes, que representan a sus correspondiente filas, sin embargo, en caso que uno de ellos sea adulterado se podría volver a calcular el hash, siempre que este no se encuentre registrado en otro lugar seguro, para evitar que el hash pueda ser modificado se propone crear un sistema de entrelazamiento de hash, donde el segundo registro calcule un hash basado en el hash anterior y el hash de la fila, evitando que las filas puedan ser modificadas sin que se deba calcular todos los hash consecutivos.



En la tabla de transacciones nótese que el hash entrelazado es calculado utilizando el resumen criptográfico SHA1 del resultado de concatenar el hash del primer registro con el segundo registro, retornando un nuevo hash con el valor:

ca6fd34c29b131f03944a0697ed1a899db1c0f39

Si hacemos este cálculo en todas las filas de la tabla de transacciones nos daría como resultado la siguiente tabla:

ID	Date	istomer	Hash	HashLink
1	12/11/2018	r9Gw	91d20088f1204fd86d8bee2de2126ac6b0a57399	91d20088f1204fd86d8bee2de2126ac6b0a57399
2	12/11/2018	vJDk	29e422cf7fcd1604613e8a319caac6b0660b6313	ca6fd34c29b131f03944a0697ed1a899db1c0f39
3	12/11/2018	d79n	f02025ab68ab83ea5320ce7b175258eb7b88d186	20ab49da776731781981258a104bf42a35cb0e0a
4	12/11/2018	Vhah	[illegible]	f5715396b26f22d5dd6d345854d35cc009157096
5	12/11/2018	EvT7	64650c8629aa984dea6c9c8da082d57998b4c06	17efecaa24a0b072b5243d20d5d691348a6bd74f
6	12/11/2018	x6v5f	191c6b1a6061aa1b9b34c7288915c14afdd1699	0674fcd947fb63be8c230cad793eefd39ecfe037
7	12/11/2018	HVHI	4e1b44dbead2002bdb86bb73f3b1f346e4da2890	c4825099efd6f0f690fd872684f68080141ba9d2
8	12/11/2018	BGxh	5b3c5d62f3628a804a2e3995dbe686670aa29ac3	ed30e444ea4cc7798126a975e80926f3128809b3

La solución contempla que cada vez que se registre un nuevo registro en la tabla se calcule el nuevo hash entrelazado, de tal manera que cualquier alteración de un registro anterior, toda la cadena de hash entrelazadas deberá ser modificada, el siguiente ejemplo pretende hacer un cambio en el cuarto registro donde se procede a cambiar el precio de 12 a 14, el resultado de del hash del registro 4 va a ser cambiado, pero deberá "recalcularse" todos los registros siguientes por están entrelazados entre sí, si se realizará ese proceso la tabla y las evidencias digitales se modificaría de la siguiente forma:

ID	Dcomer	Hash	HashLink
1	12/11Gw	91d20088f1204fd86d8bee2de2126ac6b0a57399	91d20088f1204fd86d8bee2de2126ac6b0a57399
2	12/11Dk	29e422cf7fcd1604613e8a319caac6b0660b6313	ca6fd34c29b131f03944a0697ed1a899db1c0f39
3	12/11'9n	f02025ab68ab83ea5320ce7b175258eb7b88d186	20ab49da776731781981258a104bf42a35cb0e0a
4	12/11ah	a50aa0f8c5a4c4f9d0e444990c93caca574ee699	3ccaca64b5b7921b80c0e7dd6dc33cd46bc9e238
5	12/11T7	64650c8629aa984dea6c9c8da082d57998b4c06	a5bdebc0e00ef5c150b29059e2f7bb1ab1585ca5
6	12/11r5f	191c6b1a6061aa1b9b34c7288915c14afdd1699	dde1505b5ebafc7908e15ac7acbc8c7e276edcde
7	12/11HI	4e1b44dbead2002bdb86bb73f3b1f346e4da2890	c728106da57adb805d641c5b9134c71615dbaf65
8	12/11xh	5b3c5d62f3628a804a2e3995dbe686670aa29ac3	5723e754109e46955d094a577668d6511d28e294

Al cambiar el registro #4, los datos de los hash de evidencias se modifican a partir de esa fila, alterando también la cadena de hash entrelazados, alertando que un dato fue modificado, para evitar que alguien pueda volver a cambiar toda la cadena de transacciones, es importante que cada "x filas" o "x tiempo", los datos puedan ser enviados a un nodo Blockchain de redes públicas

como Bitcoin, Ethereum o Stamping.io. En algunos casos, podría ser adecuado el uso de redes permisionadas como Rastrar.com, LACChain o Alastria.

Es resumen, este tipo de uso permite demostrar la propiedad, existencia, originalidad e integridad de una transacción, archivo o documento oficial en un momento del tiempo.

Anclándolo en la Blockchain las transacciones agrupadas

Bitcoin

Para explicarte como se ancla en Bitcoin una evidencia digital basado en un hash del tipo SHA256, necesito que veas esta pantalla con detenimiento, aunque te parezca raro ahí esta ese hash que deseamos guardar, ¿ya lo viste?:

A simple vista no se ve, pero voy a demostrarte matemáticamente que si existe, solo que está transformado.

Si quieres verlo desde el explorado de Stamping.io puedes leer este código QR:

Pasos

Paso 1: Convertir el valor hash SHA256 a 20 caracteres, hacemos uso del hash del tipo RIPEMD160, es similar al SHA256 pero retorna solo 20 caracteres.

Calcular:

```
RIPEMD160("b5d2081efaac14527f60d15146acf84e653e1df
817f0cfa95f222a422d8c220d")
```

Resultado:

```
6CFC29F7BA23ED605B8D90306339C017EC4E2496
```

Paso 2: Al resultado AGREGAR 6F[8]

Calcular:

```
6F                                                +
6CFC29F7BA23ED605B8D90306339C017EC4E2496
```

Resultado:

```
6F6CFC29F7BA23ED605B8D90306339C017EC4E249
6
```

Paso 3: Se calcula un CHECKSUM de comprobación, se usa los primeros ocho valores del doble sha256 del valor anterior. Te en cuenta que el cálculo se realiza usando el valor Binario en el primer SHA256 (ejemplo: en PHP debes usar: pack("H*", <resultado del paso 2>)).

Calcular:

```
Substr(Sha256(Sha256(pack("H*","resultado
paso 2"))),0,8)
```

Resultado:

```
E5F66B59
```

Paso 4: Se concatena el valor obtenido en el paso 2 y paso 3.

[8] Cuando se usa la red de pruebas de Bitcoin se agrega 6F si fuera MAIN NET se agrega 00

Calcular:

6F6CFC29F7BA23ED605B8D90306339C017EC4E2496
+ E5F66B59

Resultado:

```
6F6CFC29F7BA23ED605B8D90306339C017EC4E2496E
5F66B59
```

Paso 5: El último paso es convertir el resultado anterior en una dirección aceptada por Bitcoin, se necesita expresar el valor anterior en base58 (similar al base64 pero se excluye los caracteres cero, uno, ele en mayúscula o la letra O (en mayúscula), también se excluyen caracteres especiales como el slash) .

Calcular:

```
base58Check("6F6CFC29F7BA23ED605B8D90306339
      C017EC4E2496E5F66B59")
```

Resultado:

```
mqTDMRqw7jQbV8pSamWvLqaz66nJ2XwH7E
```

Ahora te invitó a volver a ver la pantalla de la transacción bitcoin (testnet):

Voy a hacer un zoom para que te percates en la dirección a donde se realizó la transferencia de unos pocos satoshi's (0.0000061 BTC):

Si nos damos cuenta cuando se calculó el base58Check, en realidad se creó una dirección válida de bitcoin donde podrá recibir monedas digitales, siendo aceptadas, minadas y validadas por los nodos de la red. Por otro lado dado que ningún nodo tiene la menor idea de los usuarios que participan de la red, no pueden determinar si en realidad existe algún usuario que pueda reclamar ese pago.

En el caso de Stamping.io o cualquier otra plataforma que ancla evidencias digitales en la Blockchain de Bitcoin, hacen este artificio para dejar inmutable en la red algo que es matemáticamente demostrable. Es por eso, que cuentan con mecanismos simples de comprobación visual donde si ingresas el hash, realiza el cálculo y te dice, si existe o no existe. Pero siempre estará la opción de comprobarlo manualmente. Para concluir, quería comentarte que

esta forma de registrar evidencias en bitcoin no es la única, también existe otra manera usando OP_RETURN.

Preguntas de repaso:

- ¿A quién le pertenece el dinero que se ha transferido a la dirección donde se ancló el hash del documento?
- ¿Quién va a reclamar ese pago?

Ethereum

En caso de Ethereum, no es necesario hacer todo este proceso, ya que se puede hacer una transferencia de tu walllet a tu wallet y registrar el hash en un campo llamado data input.

Veamos cómo se ancla un documento cuyo hash SHA256 dio este resultado:

Viendo la transferencia realizada en Ethereum verás que en el campo Data Input se encuentra el hash en valor hexadecimal.

….

Segundo tipo de uso:
"Tokenización de Activos digitales"

La Blockchain es una base de datos distribuida que registra activos de valor que pueden ser de dos tipos:

Fungibles

Que pueden ser gastados y dividido en pequeñas cantidades, ejemplo: Las monedas digitales. Aunque existen diferentes casos de usos como por ejemplo:

- Token de utilidad: Sirven para realizar actividad dentro de la red, son token que permite ser gastado dentro de la red para realizar ciertas tareas. Pueden ser similar a tener créditos.
- Token de equidad: Sirven para ser usado como votos, donde a cada usuario tiene un saldo que permite manifestar su voluntad y que esta pueda ser computarizada.

No fungible

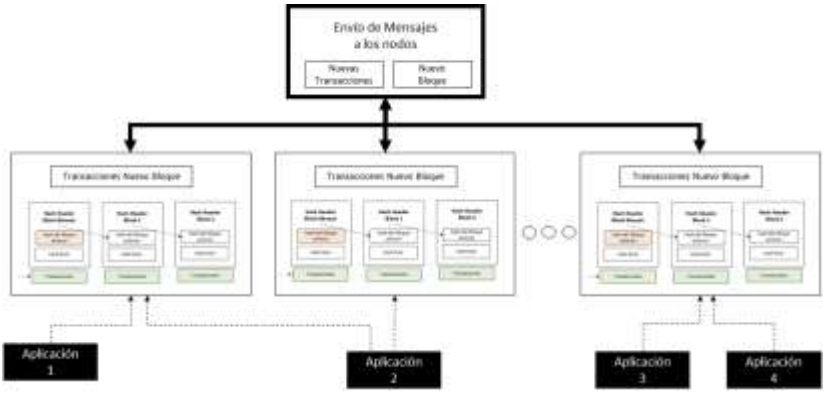
Que no puede ser gastado ni dividirse en pequeñas cantidades, estos tipos de activos representan algún producto tangible o intangible en particular, su uso es para generar trazabilidad en el cambio de los valores de sus atributos, gestionar y controlar los cambios de propiedad, así como llevar un registro certero de la fecha de creación del activo, por ejemplo: Registro de propiedad intelectual, el registro de un certificado o documento, el registro de

una orden de compra, la producción de un bien o servicio, el registro de un reclamo, etc.

Por lo general, la tokenización permite demostrar la propiedad de algo, registrar la transferencia de propiedad (incluyendo trazabilidad) y la existencia de ese activo de valor en un momento del tiempo.

En proceso de tokenización está siendo explorado y utilizado por muchas industrias, para poder darle vida en un mundo real a cosas que existen o no existen en nuestro entorno, por ejemplo: Una votación electoral, el registro de propiedad vehicular, el registro de las garantías de compras de productos, la propiedad intelectual, la receta médica, el reclamo de un servicio, la orden de compra, un certificado de acreditación, etc. Si eres desarrollador, es aquí donde están los mayores desafíos.

El siguiente diagrama muestra la arquitectura de funcionamiento de una Blockchain:



En su esencia, la Blockchain incorpora los siguientes conceptos:

- Una red distribuida de nodos computarizados interconectados entre sí (en el caso de las criptomonedas son comúnmente conocidos como *mineros*), estos equipos de cómputos cuentan con un software especial que permite:

  Recibir: Las transacciones que se envían a la red.

  Validar: Que las transacciones que se han recibido coinciden con las registradas en los otros nodos.

  Consenso: Realizar una prueba que permita garantizar que todos los nodos llevan el mismo registro, en el caso de las criptomonedas muchas de ellas otorgan un incentivo a los mineros, con el objetivo que ayuden a crear más nodos; se usa un algoritmo de prueba de trabajo que incluye un reto matemático, el primero en resolverlo gana un cantidad de criptomonedas que luego, si desea, podrá cambiarlo por dinero fiduciario.

- Un registro público o libro mayor conformado por un grupo de bloque entrelazados entre sí. Este registro es un libro contable que se encuentra público entre todos los nodos o testigos que conforman la red. Cada bloque contiene las últimas transacciones que son agregadas a la cadena de bloques una vez que todos los testigos hayan confirmado. Por lo general, este libro es público y se encuentra disponible para todo el mundo.

- Un algoritmo de firmas criptográfica con cifrado asimétrico, que se utiliza para autorizar las transacciones y en algunos casos para conformar la identidad de las personas que reclaman o desean demostrar la propiedad de un activo en una dirección determinada.

Todos estos conceptos son importantes y contienen cierta complejidad, por lo que exploremos cada uno con mayor detalle.

Proceso de tokenización de activos digitales fungibles

Para entender los activos digitales fungibles o conocidos como dinero digital o criptomonedas, se debe comprender ¿cuál es el problema que se resuelve? El uso de una plataforma Blockchain para gestionar dinero digital es evitar que alguno de los participantes pueda gastar más dinero que el que dispone. Considerando que se puede usar registrar dos transacciones diferentes en dos nodos distintos, se debe contar con un mecanismo que asegure que nadie realice un doble gasto o que se cree "dinero" de la nada.

El doble gasto[9]

Es un defecto potencial del dinero digital el cual podría gastarse más de una vez. Esto es posible porque cada moneda consta de un archivo digital que puede duplicarse o falsificarse[10]. Al igual que los billetes falsos, el doble gasto conlleva inflación dado que se crean nuevas monedas que anteriormente no existían. Esto devalúa la moneda en relación a otras unidades monetarias, y disminuye la

[9] Basado en Wikipedia: https://es.wikipedia.org/wiki/Doble_gasto
[10] Ryan. «Digital Cash». School of Computer Science, University of Birmingham. Consultado el 27 de mayo de 2017

confianza de los usuarios, así como dificulta la circulación y posesión de la moneda.

En el caso concreto de la mayoría de las criptomonedas utilizan la Blockchain para protegerse contra los ataques de doble gasto, anclando cada transacción de transferencia en esta base de datos (la Blockchain) y que pueda ser verificada después (durante el consenso).

Hacerlo a través de un intermediario o tercero de confianza que lleve la contabilidad de cada transacción (libro mayor) y el saldo de cada cuenta no es fácil de hacerlo, hace años que así funcionan los sistemas de pagos online o transferencias interbancarias; hacerlo en un sistema descentralizado, basado en una gran red de nodos interconectados entre sí y que no se conozcan ni confíen entre ellos, ese es un resto que antes de la existencia de bitcoin, a nadie se le hubiera ocurrido hacer o proponer. ¡Felicidades Satoshi Nakamoto por atreverte a hacerlo!

El momento más vulnerable que tiene cualquier Blockchain para que se pretenda registrar un doble gasto, es durante la creación de un bloque en la red y por eso, a más nodos que lo confirmen, menos probable será el riesgo de sufrir un ataque. Más adelante veremos que la cantidad de confirmaciones dependerá del tipo de consenso que tiene cada Blockchain del mercado, incluso si deseas tener una propia red, es algo que deberás definir al crearla.

El ataque del doble gasto

Para ejecutar un ataque de gasto con éxito han de seguirse los siguientes pasos:

1) El atacante realiza un pago a una persona o empresa para recibir un servicio o producto, en el "backend", en

realizada se está registrando una transacción desde la billetera (Wallet) del comprador hacia la del vendedor, esta transacción la están registrando en un nodo de la red Blockchain que soporta la criptomoneda que se está usando como medio de pago. Ojo que el nodo es probable que sea de un tercero o del vendedor.

2) El atacante cuenta con su propio nodo conectado a la Blockchain, en ese nodo incluye una transacción en la que trata de transferir el dinero que tenía la cuenta con la que pago la transacción al vendedor, considera que cambiará la dirección destino (cuenta que recibe el dinero) hacia una nueva que ha sido creada por el atacante. A penas haya registrado la transacción fraudulenta, el atacante comienza a minar el bloque para tratar de registrarlo en la Blockchain. Su objetivo es que se confirme e incluye en la cadena de bloques antes que la transacción que utilizó para pagarle al vendedor.
3) El atacante continuará minando la rama fraudulenta hasta que esta sea convierta en la rama más larga que la rama del otro nodo que tiene la transacción original.
4) Como el proceso de minado toma algo de tiempo (por ejemplo diez minutos en bitcoin), el vendedor otorgará el servicio o producto al ver la transacción en el libro público (ledger), aunque aún no esté confirmada o tenga pocas confirmaciones.
5) Pero, si el atacante ha tenido éxito en el paso 3, la rama fraudulenta será publicada y considerada válida, recuperando la moneda gastada en la otra transacción. Ya que la cuando se trate de anclar la transacción correcta, esta será rechazada puesto que el dinero ya fue usado y la dirección ya no tiene saldo.

Este ataque se concreta cuando el vendedor no espera hasta la confirmación de la transacción en la cadena de bloques antes de entregar el producto o servicio. ¿Pero, vas a hacer esperar diez minutos a clientes hasta qué se confirme la transacción? Justamente, por este motivo, muchas empresas que ofrecen productos o servicios de entrega inmediata no están aceptando dinero digital o utilizan mecanismos alternativos para evitar este ataque.

Prevención del ataque de doble gasto

La base del ataque de doble gasto es que una moneda o partes de ella puedan usarse más de una vez, lo cual en teoría es algo que debería ser imposible, pero si el vendedor no espera a la confirmación de su transacción podría estar expuesto a un fraude.

Para solventar este problema se han desarrollado sistemas de verificación que siguen básicamente la siguiente secuencia:

1) Se lleva a cabo la transacción.
2) Se incluye la transacción en el bloque.
3) Se confirma la transacción. Hasta que no se ha confirmado por lo menos seis veces, el estatus de la transacción no pasa a legítimo. Este número concreto se debe a que según la teoría de la probabilidad, el éxito de una operación de ataque de doble gasto no superaría el 0.1%.
4) La transacción ya confirmada y legitimada se finaliza.

Proceso de Tokenización de activos digitales no fungibles

La tokenización de activos digitales es un proceso "relativamente" sencillo de realizar, solo se necesita crear un hash que represente al activo y registrarlo en la blockchain. Es muy simular a registrar una evidencia digital, solo que esta vez no solo se ha creado para demostrar su existencia, sino para que este activo pueda ser transferido entre varios usuarios, ya sea en forma parcial o total.

El hash que se genera al registrarlo en la Blockchain es lo que comúnmente se le conoce como "token", el cual representa el valor de un activo o bien digital, algunos pueden dejar el token estampado directamente en un smart contract, o un una base de datos externa (offchain) o dentro de la misma Blockchain (onchain).

Aunque cada caso tiene sus particularidades, no debems olvidarnos qie la Blockchain es una solución que permite brindar confianza entre los participantes. Cuando se crea un token que representa algo que tiene valor para los participantes de la red, es la misma red, el garante de la existencia de dicho registro y que solo se ha creado uno. Al ser una red pública entre todos los participantes, cualquiera de ellos podrá auditarlo incluso sin tener la necesidad de contar con un nodo. En el caso de stamping.io, cada vez que un token es creado, estos se publican en nuestro explorador, permitiendo ser validado por los interesados.

A partir de la creación de ese token, se podrá realizar la transferencia de su propiedad a otras personas, siendo nuevamente la red Blockchain quien de la garantía de la voluntad de su propietario en realizar la transferencia, pudiendo demostrarse en cualquier momento que la transacción fue realizada y asegurando

que nadie lo pueda hacer si no cuenta con la respectiva llave privada, al mismo tiempo evita la posibilidad que el propietario repudie dicha operación.

Se puede tokenizar cualquier cosa, pueden ser datos o documentos que presenten bienes tangibles o intangibles, a pesar que suene absurdo, cuando tratamos con bienes físicos el proceso se complica enormemente con respecto a los bienes intangibles. Por ejemplo:

"Ana es propietaria de una vaca, y quiere vendérsela a Bruno utilizando la Blockchain, por lo que primero deberán tokenizar la vaca en una Blockchain donde ambos confíen y que por lo general todos los ganadores también lo hagan. Ambos pueden generar un contrato que diga que si Bruno le paga a Ana el precio de la vaca, ella le transfiere la propiedad de su vaca a penas se confirme la trasferencia"

Transferencia de propiedad del token

Bruno lee el chip que tiene la vaca, el cual cuenta con un código del token de la Blockchain, en ese registro de la cadena de bloques se cuenta con los datos o atributos asociados a la vaca.

Ana puede hacer una prueba de propiedad demostrando que tiene la llave privada y que puede modificar el propietario si ingresa dicha llave privada para que este a nombre de Bruno, pero si realiza la transferencia antes de recibir el dinero, corre el riesgo que Bruno no le pague y de esta manera sería estafada, porque no existe manera de revertir la operación que se registró en la Blockchain.

Si bruno le transfiere el dinero a Ana, corre el riesgo que Ana en realidad no cuente con la llave privada y se niegue a transferirle la propiedad. Claro que siempre podrá llevarse la vaca pero, Ana podría demostrar que la vaca sigue siendo de su propiedad y denunciar a Bruno de hurto.

La creación de un contrato inteligente (Smart contract) ayudaría a que esta operación pueda realizarse siendo la Blockchain el garante de dicha operación.

El funcionamiento seria el siguiente, Bruno compra unas criptomonedas que la Blockchain reconozca como token, luego firma un contrato con Ana donde dice que en el caso de recibir la propiedad de la Vaca, las criptomonedas serán transferidas hacia Ana, en caso que Ana no transfiera la propiedad del bien en menos de un tiempo definido, el Smart contract se encargará de devolver las criptomonedas a Bruno, quien podrá volverlo a convertir en dinero legal (Fiat).

Capitulo 4
Identificando casos de uso de la Blockchain

No todos los protocolos Blockchain que existen en el mercado son iguales, dependiendo el propósito para el cual fue creado puede contar con ciertas particularidades, por lo que nos vamos a concentrar únicamente en los componentes más importantes que una Blockchain necesita para funcionar.

Identificando las necesidades

Definitivamente la Blockchain es útil para muchas cosas, pero debes entender que no es una panacea que ayuda a solucionar todos los problemas informáticos.

La Blockchain soluciona un problema de confianza entre varios participantes que desean registrar algún activo que tiene valor para ellos.

Existen una serie de criterios que pueden ayudarte a determinar si tu sistema necesita implementar la Blockchain en alguno de sus

procesos. Ten en cuenta que la Blockchain es una arquitectura de software que propone el uso de un mecanismo de almacenamiento de datos que fue creado para dar soporte a crear registros entre varios participantes que no se conocen y/o no confían entre sí. Este mecanismo puede tener múltiples aplicaciones que van mucho más allá de las criptomonedas.

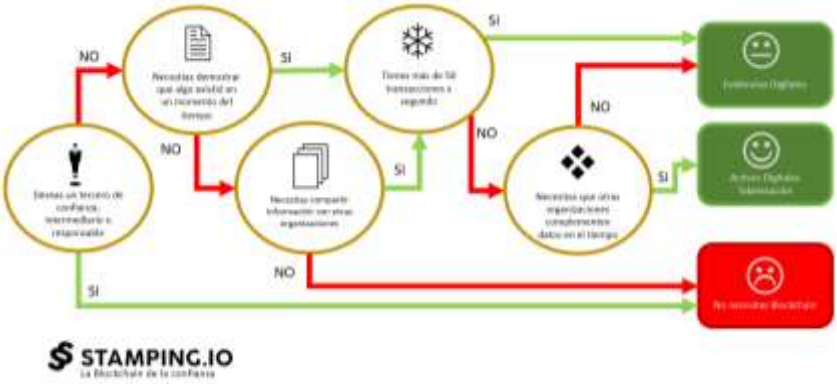
Hace unos años que las cadenas de bloques han cobrado importancia en el mundo tecnológico y muchas organizaciones han comenzado a explorar su uso. El problema es que el uso de una cadena de bloques no siempre es una buena decisión. El 90% de los proyectos basados en Blockchain, lanzados entre 2016 y la primera mitad de 2017, fracasaron en un lapso de 24 meses. Por esta razón, muchos especialistas remiendan que antes de comenzar un proyecto basado en esta tecnología, se tome el tiempo para analizar las necesidades y evaluar la factibilidad si la solución podrá ser cubierta por un sistema de bases de datos tradicional o bien es necesario recurrir a las cadenas de bloques o en una solución mixta.

"La tecnología no debe ser usada por moda, sino porque te ayuda solucionar un problema real"

En este artículo presentamos una serie de criterios que ayudan a determinar cuándo tiene sentido almacenar datos en una Blockchain, ya sea como una evidencia digital o una Tokenización de algún activo digital.

Tipos de usos

El siguiente diagrama muestra una metodología que puede ayudar a determinar el caso de uso que puede darse a la Blockchain:



Este árbol de decisiones, te ayudara a determinar si necesitas usar Blockchain y que tipo de caso de uso es el más recomendable, los pasos son los siguientes:

Pregunta 1: ¿Deseas un tercero de confianza, intermediario o un responsable?

Antes de responder esta pregunta, te invito a analizar más detalladamente como funciona un intermediario. Por la falta de confianza en la humanidad desde los años más remotos, nos hemos visto obligados a la necesidad de confiar como testigos en terceras personas, que no solo pueden ser seres humanos, sino también pueden estar conformados por otras empresas u organizaciones, cuyo propósito es dar fe que algo sucedido, existió o se realizó en un momento del tiempo; a estos intermediarios se les conoce como "tercero de confianza", por ejemplo a través de

los bancos, podemos realizar transferencias de dinero a cuentas, incluso de otros bancos o países; también les damos nuestro dinero para que lo guarden, teniendo la confianza a ciegas, que nadie realizará movimientos en esa cuenta sin mi autorización.

A pesar que la descentralización es una de las palabras que más seduce a las empresas cuando hablamos de la Blockchain; sin embargo, pocos se reparan a pensar si realmente necesitan que alguno de sus procesos no sigan recayendo en manos de un intermediario, que de alguna manera, me ayuda a tener fe que un cierto proceso funciona, funcionará y que los datos están seguros. Tenga en cuenta que existen algunos procesos comerciales, que se necesitan contar con un responsable para el éxito del negocio; ése responsable, es probable, que sea el intermediario.

Si decides no depender de un tercero de confianza, sino de una red de testigos digitales; deberás ser consiente que ya no tienes un responsable del proceso. Por ejemplo, en las transacciones financieras, de alguna manera el banco, no solo garantiza que ciertas operaciones se realizaron con éxito, sino que se encuentra regulado por entidades gubernamentales que tratan de evitar fraudes; sin embargo, cuando abandonas esos intermediarios por usar un sistema descentralizado, es un punto importante que deberías considerar antes de tomar la decisión.

Muchas veces, debido a la responsabilidad que los intermediarios tienen para generar confianza en determinadas transacciones, necesitan ciertos procesos adicionales de verificación, en muchos casos son manuales, generando retardo en el procesamiento y aprobación. En el caso de utilizar la Blockchain, los registros se actualizarán automáticamente en todos los nodos, sin posibilidad que alguien modifique o adultere la información, con lo que se logra una forma más eficiente y segura de realizar transacciones sin

perder tiempo extra en verificarlas haciendo que el costo por transacción sea muy inferior con respecto a los sistemas tradicionales centralizados en un intermediario responsable.

A simple vista, el decidir hacer algo, sin alguien que se responsabilice por dar la confianza para que sea transacción se realice en forma veraz, podría verse como algo absurdo; sin embargo, si lo vemos con detenimiento, casi siempre los intermediarios responsables, hacen todo el intento por dar la confianza necesaria a los participantes pero, en el caso de un engaño o fraude, es el momento, donde descubres que la responsabilidad era limitada. Por ejemplo, cuando descubres que alguien falsifico tu firma en una notaría o incluso vulneró el sistema de identificación biométrico, el notario se hace responsable del perjuicio ocasionado. Quizás la responsabilidad limitada de muchos intermediarios, es lo que está obligando a que la sociedad busque un mecanismo distinto en donde depositar su confianza y la Blockchain se está ganando un espacio, para resolver este problema social.

Todos los procesos de negocio tarde o temprano tienen la necesidad de demostrar que algo sucedió o se creó en un momento del tiempo, el no contar con un sistema centralizado sino depender de una red de nodos conectados entre sí, que en cualquier momento podrían ser desconectados, como se podría demostrar algo en el futuro, por lo que una de las barreras que se deberá romper para la adopción de la Blockchain es lograr confiar en esta tecnología que promete descentralizar la confianza, y no depender de un único responsable, es definitivamente la primera barrera que hay que romper para poder ingresar al mundo de la Blockchain.

Pregunta 2: ¿Necesitas de demostrar que algo existió en un momento del tiempo?

Si lo que estás buscando registrar, solo requiere tener una fuente certera que demuestre que: una secuencia de datos, documento, archivo digital, audio, video o imagen ha existido en un momento de tiempo y que desde esa fecha no ha sido alterada, puedes utilizar la Blockchain ya sea como registro de evidencias o como registro de token de activos digitales, la diferencia se dará en función a la cantidad de transacciones y uso que le quiera dar.

En el caso que la respuesta sea no, es probable que no necesites Blockchain salvo que necesites compartir información con otras organizaciones; donde necesitas un sistema que resuelva el problema de la confianza entre el proceso de intercambio de información entre todos los participantes.

Pregunta 3: ¿Necesitas compartir información con terceros?

Es difícil pensar que una organización puede operar sin la necesidad de intercambiar información con terceros pero, como lograrlo en un ambiente donde no siempre existe la confianza mutua. Si vas a implementar un proyecto donde debes intercambiar información con otras organizaciones y no deseas centralizarla en una de las empresas o en un tercero de confianza, puedes usar la tecnología de Blockchain en modo "peer To peer"; es decir, donde cada uno de ellos cuente con un nodo interconectado entre sí, con la finalidad de crear una red suficientemente confiable, que pueda operar sin la necesidad de un intermediario y que nadie pueda repudiar o negar en un futuro.

Pregunta 4: ¿Tienes más de 50 transacciones por segundo?

En un ambiente de alta concurrencia es probable que tal como está la tecnología Blockchain puedas tener inconvenientes de rendimiento, por lo que no está mal hacer una prueba de concepto para ver si es que funciona alguna solución para un caso de negocio en particular, a pesar que hay muchas organizaciones que aseguran realizar transacciones mayores a 500 por segundo, es mejor probar, antes de depositar su confianza en la red.

Si la alta concurrencia es un problema en la red, se puede realizar un simple proceso intermedio, que se trata de unir varias transacciones en una sola, de tal manera de reducir la latencia y se registre en la Blockchain como una evidencia digital, que se puede demostrar la existencia e integridad de los datos pero, no puede realizar trazabilidad ya que esta, solo se consigue cuando se crean token de activos digitales y se necesita crear un registro por cada transacción.

Pregunta 5: ¿Tienes otras organizaciones que desean complementar la información?

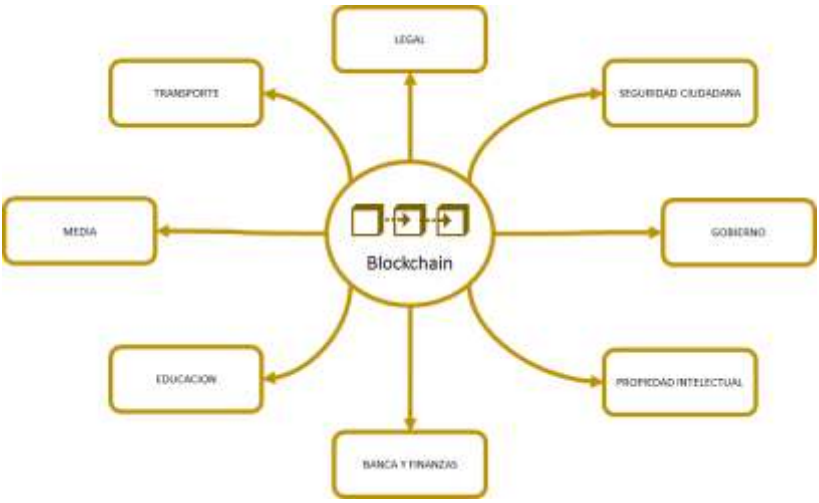
En la Blockchain, al proceso de complementación de información, se le conoce como trazabilidad digital; que consiste en dejar una traza de algo que se modificó en algún atributo del activo digital que se registró en la Blockchain. Lo ideal para crear trazabilidad digital de un activo digital, es que una de ellas la crea en la Blockchain y otras organizaciones participantes, que cuenten con la autorización respectiva, complementen la información en el tiempo; sin la necesidad de contar con una infraestructura centralizada que conlleve a que alguna de ellas se convierta en un intermediario; además se debe contar con mecanismos que

aseguren a los participantes que ninguno de los actores repudie algo que registro en la Blockchain.

En el caso que se requiera de alta concurrencia y la tecnología utilizada no permite crear un token por cada registro, puede evaluar la posibilidad de crear evidencias digitales que garantice que una traza existió en un momento del tiempo. Aunque la creación de una red Blockchain privada o DLT, cuando existen pocos actores, puede ser una excelente solución para manejar una alta concurrencia de registros, dado que la existencia de pocos nodos que sincronicen la información ayudará a tener un mejor desempeño.

Casos de usos

Existen muchas industrias que están explorando diferentes casos de uso de la Blockchain, siendo algunas de las más avanzadas las siguientes:



Exploremos algunas de ellas:

Blockchain en el área Legal

En al área legal de muchas empresas, se está utilizando la Blockchain para:

- Registro de existencia: Demostrar que algo existió en algún momento del tiempo y usarla como prueba en los tribunales de justicia; convertir los registros informáticos

en evidencias digitales con valor probatorio en los tribunales de justicia.

- Evitar repudio: Utilizando técnicas de confirmación criptográfica, se puede evitar que un participante de la red repudie alguna transacción que haya realizado.
- Evitar adulteración: Alertar algún uso inadecuado de un producto o servicio, como modificar la fecha de vencimiento, falsificar algún documento oficial, etc. Que evite alguna continencia legal a la empresa en el futuro.
- El uso de los Smart Contract o contratos inteligentes, permite que pueda auto ejecutarse; es decir, respetarse cada acuerdo del contrato, evitando el incumplimiento de alguno de los firmantes.

Blockchain para la seguridad ciudadana

En algunos países se está probando el uso de la Blockchain para mejorar la seguridad de los ciudadanos, por ejemplo:

- Rastreo de armas: Permite llevar un control de la cadena de abastecimiento, desde la importación o fabricación de armamento hasta la asignación de la arma a un ciudadano (civil, policial o militar).
- Control de incumplimiento de requisitos: Cuando una entidad gubernamental emite un certificado de autorización, existen requisitos que deben cumplirse, y se valida antes de emitir el certificado, sin embargo, existe la posibilidad que luego de haberse emitido dicho documento uno de los requisitos sea revocado o vencido, por lo que sería lógico que la autorización que fue dada como consecuencia de dicha evaluación quede también revocada

hasta que actualice el documento necesario para acreditar su cumplimiento, la Blockchain podría ayudar y alertar a las organizaciones involucradas (Entidad que emite el documento de requisito, la entidad que emite el certificado de autorización, las autoridades de fiscalización y supervisión, la empresa autorizada y los clientes o proveedores de la empresa autorizada).

- Evidencias forenses: El uso de la Blockchain facilitaría a la policía en el proceso de investigación, ya que se contaría con pruebas de sellos de tiempos, cadenas de custodia, cadena de hechos, huellas digitales que permita evidenciar un hecho ocurrido, etc.

Blockchain en el gobierno

Si hay alguna industria que puede ser beneficiada con el uso de Blockchain es el sector de gobierno, algunos gobiernos de países ya están demandado su uso, por ejemplo:

- Transparencia: Permite que ciertas operaciones que solo se encuentran registradas en los sistemas de los organismos gubernamentales puedan ser públicas, ayudando a que los ciudadanos puedan validar y controlar la gestión pública, como por ejemplo: voto electrónico, compras estatales, evaluación de funcionarios públicos, etc.
- Autenticidad de documentos: Permite validar que los documentos emitidos son originales y no han sido adulterados desde su creación.
- Inmutación de datos: Cuando se realizan registros en los sistemas gubernamentales estos no puedan ser modificados por el personal que cuenta con acceso a las base de datos

de tal forma de no ocultar información en procesos de auditoria.

- Interoperatividad segura: Crear mecanismo que evite el repudio de alguna de las partes dado que cada vez que una entidad realice la consulta, esa transacción se registra y firma en la Blockchain, y la entidad que responde valida que la consulta este guardada en la Blockchain y luego firma la respuesta, de tal forma que la entidad que realiza la consulta pueda validar que la respuesta que se registra en la Blockchain coincide con los valores que se enviaron.
- Fiscalización: Muchas entidades estatales tienen el objetivo de controlar y supervisar a un sector de la industria como minería, hidrocarburos, casinos, medio ambiente, telecomunicaciones, fármacos, animales, importaciones, etc. La Blockchain permite crear una red segura entre las e
- mpresas supervisadas y la oficina de fiscalización con la finalidad de intercambiar información y agilizar los procesos de autorizaciones.

Blockchain para el registro de propiedad intelectual

Muchos países firmaron el acuerdo en la convención de Berna para la Protección de las Obras Literarias y Artísticas, donde el derecho moral y de propiedad se basa en tres principios:

- Las obras literarias y artísticas de autores de los países de la Unión, o publicadas por primera vez en uno de dichos países, podrán recibir en cada uno de los demás estados contratantes la misma protección que estos otorgan a las obras de sus propios ciudadanos.

- Esa protección no debe estar condicionada al cumplimiento de formalidad alguna.
- Esa protección es independiente de la existencia de una protección correspondiente en el país de origen de la obra. Sin embargo, si un estado contratante provee un plazo más largo que el mínimo prescrito por la convención, y la obra deja de estar protegida en el país de origen, la protección le puede ser negada una vez que cese la protección en el país de origen.

Sin embargo, en algunos casos podría existir algún tipo de controversia sobre la autoría de la creación de una obra, por lo que se requiere demostrar con pruebas fehacientes la existencia de la obra en un momento del tiempo; el uso de la Blockchain ayudaría a demostrar esa pre-existencia y por consiguiente la autoría. En Perú existe un proyecto llamado Leftherian.com que realiza el proceso de registro de obras gratuita basada en la Blockchain.

Blockchain en Seguros de Vida y Salud

Existen diferentes Blockchain que están implementando tecnología de registro digital en el sector de la salud como una forma de mejorar la prestación de servicios. En la asistencia médica, la tecnología se utiliza para asegurar los registros médicos ya que la seguridad cibernética es un punto muy importante en la actualidad. También se utiliza para la anonimación de los datos del paciente, donde solo él puede ver los resultados de sus exámenes y compartirla con un tercero, incluido el médico, cuando lo crea necesario.

En un cliente nuestro, estamos explorando el uso de la Blockchain para el registro de recetas médicas, con la finalidad, de mostrarla

en la farmacia para que pueda ser atendido, en caso de usarse, esta receta ya no podrá ser usada en otra farmacia para adquirir nuevamente el medicamento; sobre todo cuando estos fármacos cuentan con componentes que solo pueden suministrarse bajo restricción.

La tecnología está encontrando un gran uso en la obtención de ensayos clínicos, registros médicos de pacientes y registros de facturación. Alojar tales registros en una Blockchain garantiza que no se puedan manipular, explorando la posibilidad de crear una base de datos común de información de salud anonimizada a la que puedan acceder los médicos o científicos para realizar estudios donde se pueda aplicar análisis en datos de varias fuentes distribuidas pero, al tiempo que garantizan la privacidad de los pacientes que comparten dicha información.

Las compañías de seguros de vida también están aprovechando la tecnología para detectar el fraude en la industria, para validar la pre-existencia de enfermedades antes de tomar un determinado seguro, así como para facilitar la interoperación de las empresas prestadoras de salud, las aseguradoras y los pacientes.

Blockchain en Bienes Raíces

La Blockchain también puede ser usada en el sector inmobiliario, durante años ha lidiado con problemas asociados con corredores y las personas que ofrecen el inmueble. Algunos casos de uso de la Blockchain en el sector inmobiliarios son:

- Registro de los contratos exclusivos que se firman entre los corredores y los propietarios de los inmuebles. Evitando conflictos entre ellos, cuando se realiza una determinada venta.

- Crear plataformas de intercambio de propiedades entre diferentes corredores, con la finalidad de intercambiar en forma segura a lista de compradores y vendedores, evitando conflictos de distribución de comisiones entre ellos.
- Tokenizar las propiedades en pequeños fragmentos, con la finalidad de ofrecerlas como alternativas de inversión en forma fraccionada.
- Facilitar el proceso de alquiler temporal, donde se firma un Smart contract para activar la entrada de una determinada vivienda por un periodo determinado, siendo la Blockchain quien controla el pago y apertura de las puertas, sin necesidad de un intermediario.
- La implementación de Blockchain en la industria inmobiliaria también está preparada para lograr una reducción en los casos de fraude, ya que ahora los depósitos en garantía se realizarán de manera más segura y oportuna, evitando que el arrendador no devuelva el importe cuando termina el tiempo de arrendamiento. La tecnología también garantizará un registro público y verificable, lo que garantizará la transparencia de todo el proceso.

Blockchain en la Cadena de Suministro

Si una madre en época de lactancia un médico le prescribe antibióticos para curar algún tipo de infección. La madre, por seguridad deja de alimentar en forma natural a su bebé; sin embargo, cuando niños le damos la leche de la vaca sin tener la más mínima idea de que ha consumido ese animal. Todo lo que nos llevamos a nuestro cuerpo que proviene de la ganadería,

agricultura, farmacología e industria alimenticia, será en un futuro necesario registrar información certera de la trazabilidad del producto. Un simple código QR puede mostrar la información de la trazabilidad digital.

En agosto del 2019, un proyecto llamado rastar.com permitió enviar un contenedor compuesto por más de 1040 cajas, donde cada una de ellas se registró en la Blockchain con la finalidad de registrar la trazabilidad del productor del limón. Cuando un exportador debe atender un pedido, por lo general utiliza productos de varios productores. En el caso de detectarse alguna incidencia o alerta de salubridad en el producto, es necesario demostrar e identificar en cada caja quien fue el productor.

La Blockchain proporciona una manera fácil de garantizar que todos los registros que surgen en el envío de productos del productor al consumidor final, se almacenen de forma segura y se pueda acceder a ellos en cualquier momento.

Hoy en día el cliente requiere saber cada componente de lo que usa y consume, generando mercados en los que, por ejemplo, se está dispuesto a pagar más por un producto cultivado de manera orgánica, y donde demostrar tus procesos se vuelve necesario para fidelizar, convencer a clientes potenciales y diferenciarte de tu competencia. No solo basta con que lo coloques en tu página web o que hagas una campaña en medios, necesitas que esta información esté presente en cada uno de tus productos, que las personas puedan ingresar y ver en tiempo real qué está pasando en tu empresa, cómo está hecho el alimento que van a consumir y por qué deberían confiar en que lo que ofreces es lo que prometes. Adherir las características del Blockchain a nuestros procesos, como la trazabilidad, la inmutabilidad, la inamovilidad, la descentralización y la posibilidad de que no puedas modificar

información, porque todo lo que hagas queda completamente registrado demostrará la transparencia y responsabilidad con la que manejas tu empresa y, sobre todo, la calidad de tus productos

Blockchain en Finanzas

Al parecer, Blockchain ha encontrado un gran uso en el sector financiero debido a las aplicaciones que ya existen. Los ejecutivos de Blockchain han utilizado con gran éxito la tecnología para acelerar y simplificar el proceso de pago transfronterizo. La tecnología también ha reducido los costos incurridos en la transferencia de grandes cantidades de dinero en comparación con otras formas tradicionales de pago.

Mirando hacia adelante, los CIOs de blockchain están explorando la posibilidad de aprovechar la tecnología en el intercambio de valores, medio de pago ágil, en un intento por garantizar una mayor precisión del comercio y procesos de confirmación más cortos. Los contratos inteligentes permiten auto-ejecutar y respetar acuerdos facilitando el proceso de comercio exterior.

Blockchain en Testamentos digital y fideicomisos

El Derecho de sucesiones regularmente llamado "testamento" se encarga de determinar la forma como se van a repartir todos los bienes, derechos y las obligaciones de una persona física luego de su muerte.

En la herencia intervienen varias personas, siendo el principal la persona que transmite su patrimonio por causa de su fallecimiento. Puede dejar un testamento (sucesión testada) o no dejarlo

(sucesión intestada). Luego tenemos a los herederos que son las personas que reciben el patrimonio del fallecido.

Pero para que un testamento se pueda hacer efectivo, se requiere de un encargado de cumplir la última voluntad del causante y custodiar sus bienes, y ejecuta y vigilar la ejecución del testamento.

Desde un punto de vista técnico, la información sobre la herencia podría ser almacenada, perfectamente, en una plataforma Blockchain. El secreto de la tecnología de la cadena de bloques no está en el software sino en las posibilidades de demostrar la existencia de algo en un momento del tiempo. El uso de los contratos inteligentes tiene un poder legal que para muchos abogados es una excelente herramienta para que todo contrato sea auto-ejecutado, a fin de poder transferirlos automáticamente a los herederos.

Ethernal.io, es un proyecto Blockchain que permite registrar un testamento en base a pruebas de contenidos digitales, como Fotografías, audios y vídeos contenidos en el teléfono móvil. Donde el testador expresa su voluntad para el destino de su patrimonio en vida, y las almacena en la Blockchain para garantizar su privacidad hasta su muerte.

No obstante, la utilización de contratos inteligentes para ejecutar testamentos presenta problemas y riesgos de carácter técnico y legal que hay que tener muy claro, aunque el uso notarios y la creación de fideicomisos, podría brindar una solución legal en varios países.

Blockchain para trazabilidad de las pruebas de calidad de los fármacos

Algunas empresas por razones comerciales o regulatorias requieren realizar pruebas de calidad a ciertos productos que fabrican, por lo general las pruebas se realizan a ciertos productos que son seleccionados al azar dentro de un lote de producción como muestra.

Las pruebas de calidad pueden ser realizadas en forma manual o automáticas, los resultados son registrados en bitácoras ya sea usando almacenamientos físicos como libros de registros o usando equipos computacionales que los registran en una base de datos.

Las empresas que usualmente están reguladas a realizar dichas pruebas de calidad son aquellas que fabrican productos que son ingeridos por los seres vivos, por ejemplo: Laboratorios Farmacéuticos, Productos comestibles, Golosinas, etc. Por lo general las reguladoras gubernamentales o de certificación requieren que las empresas demuestren con pruebas fehaciente el cumplimiento de las normas, usualmente recurren a registros manuales o electrónicos los que es muy difícil demostrar la adulteración, perjudicando el proceso de auditoría o certificación.

Algunas empresas requieren realizar pruebas de calidad por temas comerciales como son pruebas de color, pruebas de durabilidad, pruebas de resistencia, pruebas de cumplimiento de especificaciones técnicas, pruebas de eficiencia o eficacia, etc.

En una cadena de distribución es probable que el producto por una cadena de abastecimiento hasta llegar al consumidor final, pudiendo ser la cadena la siguiente:

La calidad del producto antes de llegar al consumidor final puede ser afectada o adulterada en cualquier parte de la cadena, pudiendo

perjudicar a la marca del fabricante o a cualquier empresa que participa en la cadena de abastecimiento, por lo que en un mundo ideal sería genial en pensar que se puede crear una base de datos única y abierta (Open Data) que permita trazar todos las variables que puedan alterar la calidad del lote de producción hasta llegar al consumidor final.

Para lograr el objetivo de tener una trazabilidad de la calidad del producto, esta iniciativa debe ser liderada o iniciada desde el fabricante, por lo que esta propuesta permite que se logre este objetivo poco a poco, empezando por registrar los resultados de calidad de la muestra de cada lote de producción para luego llegar a el registro que afecta a la calidad de cada producto.

Se puede registrar también:

- Los lotes de producción que fueron dados de baja por no cumplir con los resultados del protocolo de calidad, evitando su comercialización.
- Los productos que fueron dados de baja por vencimiento.
- Alertar los lotes vencidos, evitando que alguien dentro de la cadena de valor pueda alterar la etiqueta.
- Alertar a la cadena de abastecimiento los productos dados de baja por robos.
- Alertar a la cadena de abastecimiento los productos que han sido vendidos a entidades gubernamentales, evitando que sean robados de sus almacenes y comercializados en el mercado formal.

Casos de éxito en el uso de la Blockchain

Antecedentes policiales/penales/Judiciales y laborales

Gestión de compras estatales

interoperabilidad

Roadmap para desarrollo de proyectos

Muchos ejecutivos de las empresas desean probar esta tecnología por lo que algunos expertos recomiendan hacerlo paso a paso, es mejor determinar el objetivo del proyecto, plantear algunos hitos importantes antes de iniciar un despliegue, este roadmap ayuda a entender cómo hacer tus primeros pasos en el uso de la Blockchain:

Paso 1: Determinar el objetivo del proyecto

Es decir debes definir si lo que deseas es crear evidencias digitales o un token de activo digital que permita la trazabilidad, es importante definir quiénes serán los responsables de los nodos, la forma como se resuelve el problema de confianza entre todos y la manera en que la información va a ser registrada. Existen muchos consultores, profesionales o empresas especializadas que pueden asesorarlos para lograr este primer hito, además muchos casos de referencia pueden ser utilizados como una guía de implementación.

Paso 2: Selecciona la tecnología

Puede parecer una tarea sencilla, pero no todos los productos funcionan igual, por lo que se tiene que decidir algunos temas como por ejemplo: si se necesita una Blockchain privada o una publica o ambos, si se requiere de muchos o pocos nodos, quienes

serán los responsables de los nodos, como se realizará en endose y anclaje de los registros, como se puede demostrar legalmente la existencia de un activo y su trazabilidad, etc. Una vez que hayas elegido la tecnología podrás hacer una prueba de concepto que ayude a demostrar la viabilidad del proyecto, en el caso de crear activos digitales se podría complicar por que la prueba involucra a otras organizaciones que no siempre estén dispuestas a cooperar.

Paso 3: Prueba de concepto (Testnet):

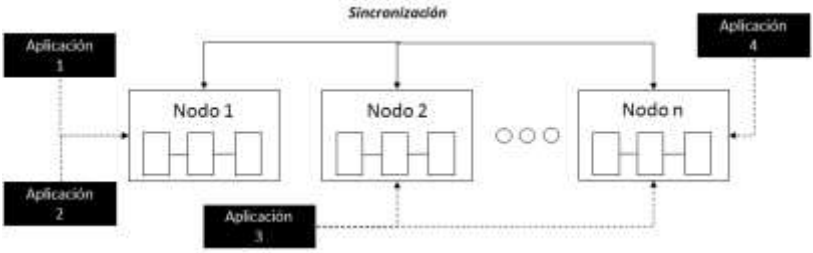
Es hacer un proyecto que no tome más de 60 días y que permita demostrar que la solución es viable, esto ayuda a reducir muchos costos innecesarios, hacer ajustes para satisfacer la necesidad del negocio y sobretodo tener la experiencia con la tecnología que se haya seleccionado, considerando que existen poca documentación, variedad de tecnología y muchas de ellas aún no son estables o maduras pero, si vale la pena probarlo por el potencial que prometen.

Paso 4: Despliegue (Mainnet):

Si la prueba de concepto funciona, no se hable más, el proyecto es viable y se debe desplegar y masificar en todo el ecosistema donde se había planificado. Es importante que se cuente con mecanismos de gobernanza, recuerde que por más que ustedes hayan sido la empresa que motivo a su creación, no son dueños de la red, la red es de todos los participantes y de los que van a participar, y deberá ser gestionada por todos en forma consensuada y no democráticamente, es decir una vez que se toma una decisión todos deben acatarla, así no hayan estado de acuerdo, por lo que tener una política clara de gobernanza ayudará a evitar conflictos y caer sin quererlo en la intermediación y centralización.

Capítulo 5
Los Nodos como testigos digitales

Los nodos, son programas de computadora que se encuentran conectados entre sí, todos los nodos en una red Blockchain se encuentran interconectados o al menos la mayoría de ellos y quizás sea eso lo que hace que sea una tecnología interesante de probar, porque todos los equipos funcionan en conjunto como testigos digitales para dar confianza a una red Blockchain.



El protocolo peer-to-peer (P2P, por sus siglas en inglés) es lo que permite que los nodos se encuentren constantemente comunicados dentro de la red, los nodos tienen algunas funciones específicas, como por ejemplo:

- Difundir información sobre las nuevas transacciones que crearán un nuevo bloque.
- Validar que la información no sea alterada, utilizando mecanismos criptográficos que aseguran que la información haya sido creada correctamente, y de acuerdo las reglas que los participantes han definido en consorcio. Ya los veremos más adelante este tema, cuando veamos cómo funcionan los contratos inteligentes.
- Avisar a los otros nodos cuando se ha creado un nuevo bloque.
- Guardar una copia de los datos para ser consultados o verificados.

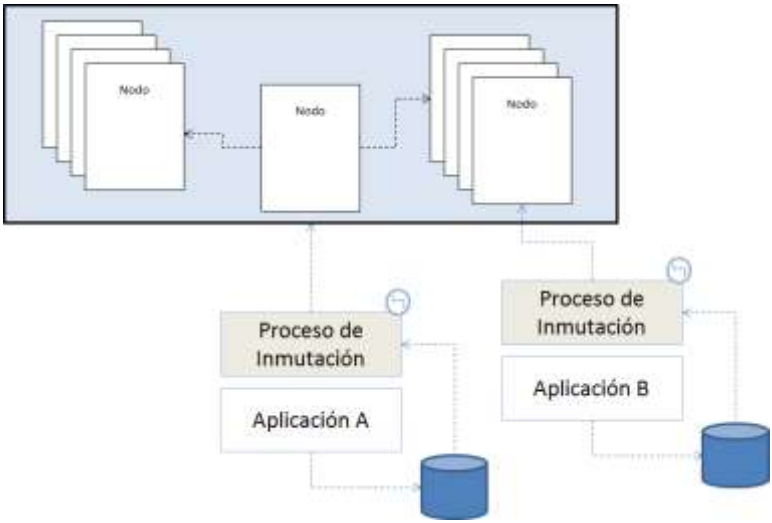
Imaginemos una red donde se reciben ciento o miles de transacciones por minuto, y cada diez minutos se guardan en un bloque, se imaginan la cantidad de información que va a existir en cada nodo, por lo que algunas redes cuentan con dos tipos de nodos:

Livianos o Regulares

Nodos solo se encargan de apoyar la validación de los datos para el nuevo bloque que va a crearse, una vez que se crea ese bloque, se aseguran que los datos se almacenen correctamente en los nodos Blockchain y proceden a eliminar los datos y solo se quedan con la información del bloque.

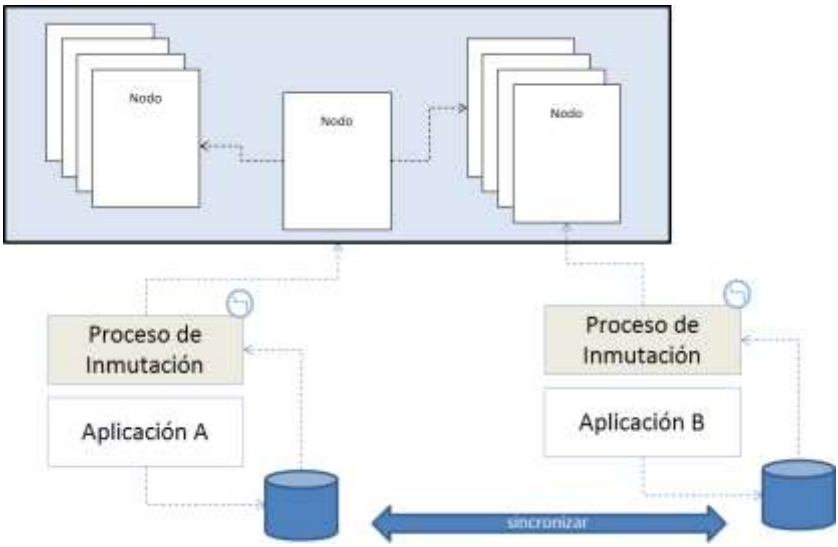
Algunas plataformas Blockchain no cuentan con este tipo de nodos, por lo que es responsabilidad de los desarrolladores colocar un repositorio intermedio con la finalidad de almacenar estas transacciones hasta que se ejecute el proceso de inmutación. Lo ideal es que si desarrollas esta funcionalidad fuera de la Blockchain (Offchain) coloques algún mecanismo de envío de mensajes, para que los otros participantes puedan recibir una copia de la transacción, así se incrementará la confianza de la red, dado que se está asegurando que en ese transcurso de tiempo no se está adulterando o eliminando los registros.

El siguiente ejemplo muestra la forma como se inmutan transacciones de una base de datos, donde no existe un nodo regular, por lo tanto las aplicaciones almacenan temporalmente las transacciones en una base de datos alterna a la red Blockchain, hasta que el proceso de inmutación de datos, tome esos registros, y los endose en un nodo de la red Blockchain:



Este tipo de soluciones se emplean, en procesos de notariado o inmutación de datos donde el objetivo es evitar que la información almacenada en la base de datos pueda ser modificada por alguien que cuente con los privilegios adecuados.

Como lo mencionamos anteriormente, el riesgo que presenta esta arquitectura de referencia, es que durante el tiempo de inmutación, los datos están expuestos en la base de datos, pudiendo ser alterados en forma maliciosa o por alguna falla del sistema. Una manera de mitigar el riesgo es creando un proceso de anclaje de registros dentro de la base de datos donde se almacenan las transacciones temporales y replicarlas en otras bases de datos de los participantes como una medida preventiva para evitar la adulteración de los datos, a continuación se muestra la arquitectura de referencia:



En este tipo de arquitecturas se puede utilizar Kafka o un API Gateway dentro de una capa de micro-servicios, que ayude a sincronizar la información entre las base de datos. Si se

encuentran en un caso de negocio, donde las transacciones son muy elevadas como en el caso de los movimientos de saldos de cuentas contables o el tráfico de llamadas, se puede hacer uso de los árbol de Merkle y/o Hashlink (Ver sección de agrupación de hash) y enviar el código de raíz en periodos más cortos, reduciendo el tiempo de posible sabotaje a casi cero.

Completos o Validadores

Son nodos que están completamente sincronizados con todas las transacciones de la red Blockchain, es decir, almacenan Cientos de Gb en alguna unidad de disco.

En una red Blockchain es común encontrarse que la mayoría de los nodos son livianos o regulares, sin embargo, los nodos completos forman su columna vertebral y sin ellos no existiría la posibilidad de comprobar la historia y por lo tanto la confianza en la red se perdería.

Características de los nodos

Recepción de mensajes

Los nodos reciben en tiempo real todas las transacciones que se están realizando en la red, algunas plataformas de Blockchain utilizan herramientas de mensajería para alta concurrencia (por ejemplo: Kafka), cada nodo que se encuentra suscrito a la red

recibe el mensaje, tan igual como un grupo de whatsapp, es decir, todos reciben el mismo mensaje y pueden llevar una contabilidad compartida entre todos. Solo que a diferencia del whatsapp, un proceso validará constantemente que todos los participantes siempre tengan la misma información, y que no modifiquen o eliminen ningún registro.

Comprobación

Los nodos también se encargan de comprobar que las transacciones que se están realizando dentro de la red cumplan con todas las reglas principales del protocolo. Algunas plataformas de Blockchain tiene reglas específicas como por ejemplo: validar que se puede crear una cierta cantidad de transacciones por cada bloque, las transacciones deben tener el formato de datos correcto, las transacciones deben estar firmadas correctamente, etc.

Si el nodo detecta que una transacción ha violado alguna de las reglas que se han definido y escrito en los Smart Contract o los procesos estándares que la red disponibiliza, por consenso la transacción será rechazada por completo, incluso si otros nodos de la red lo consideran válido se hará uso de un algoritmo que determina que hacer en ese caso, por lo general la mayoría de consensos se basa en lo que la mayoría determine, es decir, si el 50%+1 dice que es inválida, el resto de nodos acata la orden y rechazarán la transacción.

Los nodos no dejan de hacer lo correcto a pesar de que otros nodos piensen lo contrario, sin importar qué, garantizan un alto nivel de seguridad de los datos que se están almacenando y

siempre estando alerta que otros nodos podrían pretender engañar, es decir, guardar transacciones que no sucedieron en la realidad.

En realidad, la verdad absoluta no la tiene cada nodo, sino todos en su conjunto, por lo que cada momento se están realizando validaciones y comprobaciones para asegurarse que los datos que se están guardando en los nodos sea la misma. Por lo que se debe tener cuidado que si la transacción aún no se registra en un bloque, esta podría ser rechazada, incluso considere que un nodo podría modificarse a propósito para engañar que una transacción existe en un determinado momento cuando en realidad eso no sucedió. Esto puede ser usado para fraudes.

Por lo tanto, dependiendo la red Blockchain que desees crear, es importante definir el algoritmo de consenso que necesitas para asegurar la credibilidad de la red y evitar perder la confianza de los participantes.

Clases de redes Blockchain

Las Blockchain pueden ser clasificadas de diferentes formas, dependiendo del acceso a los nuevos nodos, se clasifican en:

Privadas o Permisionadas

Para ingresar a la red se requiere de un permiso especial para comenzar a registrar transacciones y/o para conectar nuevos nodos. Muchas de estas redes tienen políticas claras de gobernabilidad para evitar concentrar el poder en las personas, sino en las máquinas. Con este mecanismo se desea evitar la

centralización que podría conllevar, sin querer a la intermediación y control de la red.

Hay varias formas de gestionar el acceso, la más simple es que alguien coloque el identificador de tu nodo dentro de la red, para que comience a sincronizarse. De hecho, así es la forma como funcionan la mayoría, pero ¿qué pasa si esa persona le da acceso a alguien que no debería estar incluida en la red?. O por el contrario, no quiere darle acceso a otro participante motivado en rivalidades comerciales o personales. Es por eso que se ha creado algunos métodos de gobernabilidad, incluso muchos ya se están automatizando. Por ejemplo en Stamping.io, puedes crear un nodo y agregarte a la red enviando un email, un robot al recibir el correo lo envía a un operador para solicitar el "enode" (identificador del nodo en Ethereum) y lo agregará a la red de Stamping.io siempre y cuando sea reconocido como un cliente de la red, caso contrario se enviará un formulario de solicitud de acceso.

Públicas

Cualquier persona puede colocar un nodo y generar transacciones en la red, siguiendo sus reglas y su protocolo. Nadie tiene que dar acceso a ningún nodo,. Bitcoin y/o Ethreum están conformados por miles de nodos, no se pueda dar una cantidad exacta porque cada diez minutos entran nuevos nodos, así como se desconectan otros.

En el caso de Stamping.io también usamos redes públicas, en ese caso contamos con nodos conectados a las redes Blockchain de Bitcoin y Ethereum (Testnet y Mainnet), estos nodos reciben

nuestras transacciones y las envían a los otros nodos de la red para que sean confirmadas y ancladas a la Blockchain.

El problema de las redes públicas es que tienen algoritmos de validación y consenso que por lo general toman más tiempo en confirmar una transacción que las redes permisionadas, son limitadas en cuanto a agregar funcionalidad (salvo la permitida por los Smart Contract) y la creación de activos de valor están más orientados a trasferencia de dinero digital y acuerdos comerciales. Cuando desea crear algún proyecto de tokenización para trazabilidad de "algo" que tiene valor para un grupo de participantes, se vuelve un poco limitado e ineficiente. Además no hay que olvidar que el costo de transacción (Fee) es cada día más alto.

Tipos de algoritmos de consenso

Consenso

De acuerdo a Wikipedia: "Se denomina consenso al acuerdo producido por consentimiento entre todos los miembros de un grupo o entre varios grupos. La "falta de consenso" expresa el disenso.

El consenso se diferencia de una DEMOCRACIA porque cuando una mayoría se pone de acuerdo también hay una minoría que disiente, en cambio en el consenso no hay disenso, simplemente todos acatan la orden luego de la votación.

Una decisión por consenso, no obstante, no implica un consentimiento activo de cada uno, sino más bien una aceptación

en el sentido de "no oposición". En este tipo de modalidades de decisión encontró su fundamento la democracia griega.

Los algoritmos de consenso son procesos de toma de decisiones para una red, donde cada individuo dentro de la red construye y apoya la decisión que funcione mejor para ellos. Es una forma de resolución donde los miembros deben apoyar la decisión mayoritaria o de acuerdo como se haya definido el tipo de consenso, les guste o no les guste.

En un sistema informático donde los datos se encuentran distribuidos entre diferentes nodos, muchas veces puede verse afectado por un mal funcionamiento o por una falla intencional y pretender modificar la información en su base de datos, por lo que el consenso en una red Blockchain es el responsable de resolver esos conflictos. Los algoritmos de consenso solo pueden funcionar con éxito si todos los nodos y/o usuarios trabajan en forma orquestada. Sin embargo, incluso si uno de los componentes en de este sistema funciona mal o se trata de un nodo deshonesto que desea alterar la información de la red, todo el sistema no debería fallar. Esto es lo que justifica a que muchas redes Blockchain seleccionen un adecuado algoritmo de consenso.

Las Blockchain descentralizadas, sobre todo las públicas, se definen como sistema abierto y distribuidos, debido a que no dependen de una autoridad central, sus nodos necesitan ponerse de acuerdo respecto a la validez de las transacciones. Aquí es donde los algoritmos de consenso entran en el juego, encargándose de asegurar que las reglas del protocolo son respetadas y garantizando que todas las transacciones tienen lugar de una forma fiable; lo que implica que todas las transacciones que

los nodos registren respeten las reglas, recordando que las transacciones se realizan en diferentes nodos, entre otras cosas se debe evitar el doble gasto o doble uso de un mismo activo digital, por ejemplo: Las monedas sólo podrán ser gastadas una vez, evitar la doble reserva hotelera de la misma habitación para el mismo día, evitar la doble venta de una entrada al cine en el mismo asiento para la misma película, etc.

Antes de sumergirnos en los diferentes tipos de algoritmos de consenso, es importante entender las diferencias entre un algoritmo y un protocolo.

Los términos algoritmo y protocolo a menudo se emplean de manera indistinta, sin embargo, no son la misma cosa. En términos simples, podemos definir un protocolo como las reglas primarias de una Blockchain; y el algoritmo, como el mecanismo a través del cual dichas reglas serán seguidas.

Una red Blockchain siempre se regirá sobre un protocolo que defina la forma del funcionamiento de los nodos. Por lo que todos los participantes de la red deberán respetar las reglas del protocolo. Mientras el protocolo determina cuáles son las reglas, el algoritmo le dice al sistema qué pasos seguir para cumplir con las mismas y producir los resultados deseados. Por ejemplo, el algoritmo de consenso de una Blockchain es lo que determina la validez de las transacciones y bloques. Así, Bitcoin y Ethereum son protocolos, mientras que Proof of Work (Pruebas de Trabajo) y Proof of Stake (Pruebas de participación) son sus algoritmos de consenso.

A fin de hacer una mejor ilustración, hay que tener en cuenta que el protocolo Bitcoin define cómo deben interactuar los nodos,

cómo deben transmitir los datos, así como cuáles son los requisitos para que una validación de bloque sea efectiva. Por otro lado, el algoritmo de consenso es el responsable de verificar los saldos de cada cuenta (balances de cada dirección) y que las firmas sean correctas, confirmar las transacciones y ejecutar la validación de cada bloque. Y todo esto, depende de un consenso de red.

El mecanismo de consenso utilizado en la redes Blockchain permite asegurar que los datos estarán guardados correctamente en los nodos, sin embargo, en algunas redes públicas se requiere generar un incentivo económico que sea lo suficientemente atractivo para motivar a los dueños de estos nodos a realizar estas validaciones, a quienes se les conoce como mineros. El objetivo del consenso es verificar si los datos se registraron correctamente durante la creación de un nuevo Bloque.

Todos los días nacen nuevas redes Blockchain, cada una muestra temas interesantes ya que se están especializando a propósitos específicos. Técnicamente, todas son muy similares, ya que cuentan con una contabilidad distribuida, tienen nodos que reciben datos en forma simultánea, tienen un protocolo y reglas que deben respetarse, tienen trazabilidad de las transacciones y movimiento de sus activos de valor, generan bloques cada cierto tiempo, los bloques se anclan con los anterior (haciendo una cadena de bloques) y habilitan una capa de micro-servicios para interactuar con las aplicaciones, o mejor dicho, que las aplicaciones interactúen con la Blockchain. Es decir, tiene aspectos técnicos muy similares entre sí pero, si hay algo que realmente las diferencia es su algoritmo de consenso.

Los principales algoritmos de consenso son:

- Prueba de trabajo (PoW)
- Prueba de participación (PoS)
- Prueba de participación delegada (DPoS)
- Prueba de participación arrendada (LPoS)
- Prueba de tiempo transcurrido (PoET)
- Prueba de actividad (PoA)
- Prueba de importancia (PoI)
- Prueba de capacidad (PoC)
- Práctica de tolerancia a faltas bizantinas
- Tolerancia a faltas bizantina simplificada
- Tolerancia a faltas bizantina delegada
- Proof-of-Burn
- Proof-of-Weight

Sin embargo, las implementaciones más comunes son PoW y PoS. Cada uno tiene sus ventajas y desventajas en lo que se refiere al equilibrio entre seguridad por un lado, y funcionalidad y escalabilidad por el otro.

Prueba de trabajo - Proof of Work (PoW)

PoW fue el primer algoritmo de consenso que se creó ya que se utiliza en Bitcoin y también ha sido adoptado por otras criptomonedas. Este algoritmo es una parte esencial del proceso de minado, ya que ayuda a determinar al ganador de la recompensa por minar y además permite que pueda ser confirmado por otros nodos de la red.

La prueba de trabajo implica realiza una serie de combinaciones de cálculos de hashing hasta encontrar un "hash block" que comienza con una cantidad de ceros especificados. Hay que considerar que cuanto más ceros se requieren, mayor dificultad de entrarlo ya que probablemente va a necesitar de más intentos hasta lograr la solución.

Cuando uno de los mineros dispone de más poder computacional significa que tiene mayores intentos por segundo y por lo tanto mayor posibilidad de encontrar el resultado antes que los demás, aunque no siempre es seguro. El algoritmo de consenso PoW se asegura de que los mineros sólo sean capaces de validar un nuevo bloque de transacciones y añadirlo a la Blockchain, si los nodos distribuidos de la red alcanzan consenso y aceptan el hash block provisto por el minero como una prueba de trabajo válida, pero antes de hacerlo van a confirmarlo, la forma de hacerlo es muy sencilla ya que el minero ganador provee un valor conocido como "nonce" que al calcular el hash de la combinación del hash raíz con el valor del *nonce* se obtiene el hash block, de esta forma es validado por cualquier nodo en forma automática. A pesar que es difícil calcularlo, la verificación de esa información es muy fácil, no

requiere de tiempo ni costos para hacerlo y comprobar que la respuesta es correcta.

Hay que considerar que la dificultad (cantidad de ceros) varía de acuerdo a la velocidad de cómo se vienen creando bloques, bitcoin se auto-regula, aumentando o disminuyendo la dificultad con el objetivo que se demore diez minutos en crear cada bloque. Es decir, se trata de un concurso entre los nodos para buscar un hash con un formato especial. Para hallar el hash esperado, se debe consumir muchos recursos computaciones que a su vez consumen mucha energía, por lo que se premia al primer nodo en encontrarlo.

El hashcash, el principio de la minería

El acertijo que debe resolverse en la Blockchain de Bitcoin es conocido como "Hashcash"[11], ese método fue publicado formalmente a través de un whitepaper de Adam Back el 2002 (mucho antes de la existencia de Bitcoin) para solucionar el spam de los email, ya se había hecho público en el mailing list del movimiento cypherpunk en 1997.

El objetivo principal de Hashcash era minimizar la recepción de grandes cantidades de correos electrónicos no deseados, utilizando la colisión de hashes para ello, Satoshi Nakamoto propuso usar esta técnica para realizar el consenso de los nodos en Bitcoin: *"Para implementar un servidor de marca de tiempo distribuido P2P, tendremos que usar un sistema de prueba de trabajo similar al Hashcash de Adam Back"*, se lee en el libro blanco publicado por Nakamoto en

[11] Creada por Adam Back

2009. El servidor de marcas de tiempo es lo que se conoce como la Blockchain.

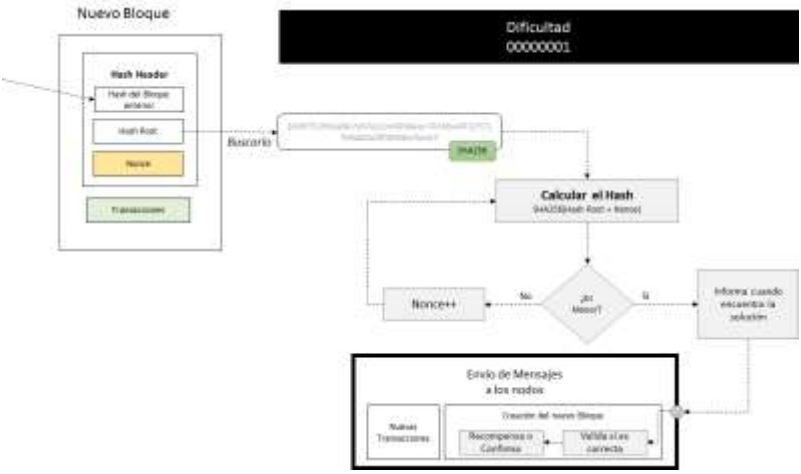
Compitiendo para descubrir el Nonce

El método del hashcash es sencillo de entender, para lo cual se trata de buscar a través de la "fuerza bruta" (prueba-error) un valor que al calcularle el hash de ese valor con el de otro hash dé como resultado un hash con ciertas particularidades, por ejemplo:

Tenemos un Hash con éste valor:

```
10c8f75256ea8e7e67e22cc4064aac7436ba4032971759a
855d9f4894ac9aee7
```

El objetivo es buscar el menor "numero", que se le conoce como *nonce*, que al realizar este cálculo: `SHA256(Hash+Nonce)` dé como resultado un hash que empiece así: `000001`. Este gráfico resume el cálculo:



Para lograr encontrar este resultado, se deberá utilizar un algoritmo similar al siguiente:

```
function getNonce(sGold, sNonce, sHashRoot) {
sHashWithNonce = Sha256(sHashRoot+sNonce)
    if (sHashWithNonce <=sGold) {
      return sNonce
    } else {
      sNonce++
      getNonce(sGold, sNonce, sHashRoot)
    }
}

sGold   = "0000000010000000000000000000000000000000000000000000000000000000"
sNonce  =1
sHashRoot = "10c8f75256ea8e7e67e22cc4064aac7436ba4032971759a855d9f4894ac9aee7"
getNonce(sGold, sNonce, sHashRoot)
```

Dependiendo el tipo de ordenador que tenga, este proceso puede tomar algunos segundos en encontrarlo, al final verá que ese valor va a ser encontrado, tal como se muestra en el siguiente gráfico:

Id	nonce	resultado	Estado
1	42945	0c36965049d2bd702e128a11a67f32f30be2bf82dac9572ce5b53cbf5b659b53	
2	42946	66b31ba19e57a46598f062066b7aae902ecb794c9fa79cb8c7244959a22f4fe4	
3	42947	834c96b3d2ab475dc4cc65502a2919bdd4f8ede9475799dae044574ce9bd9338	
4	42948	6171ed3ecd65792bf9ac75ed5455e594cee59b195447da3f752a37ea5176c2f8	
5	42949	00001dfb099a6af8da47ce942ebe61b6391ecbd12e5b1acf7a5f2d379b5ed8f1	Encontrado

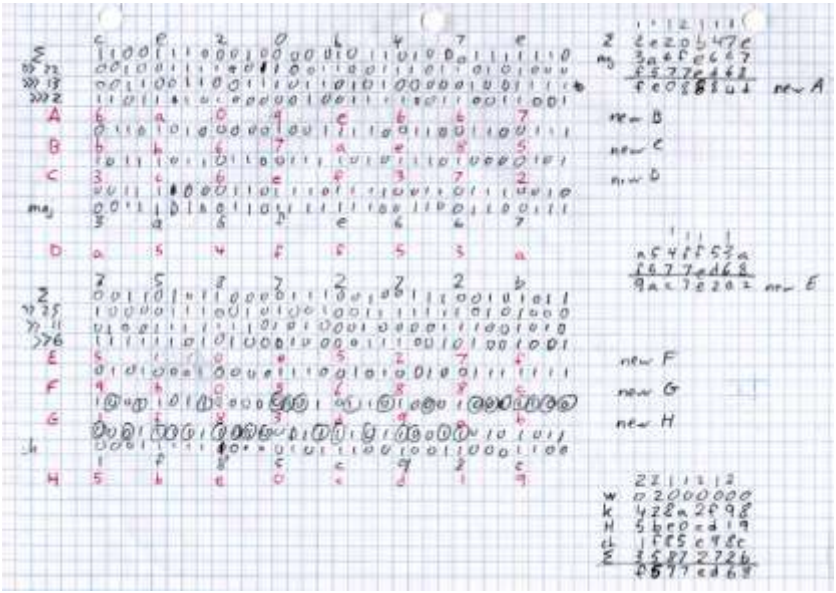
Sin embargo si usted desea comprobarlo solo debe calcular el valor de:

```
Sha256(10c8f75256ea8e7e67e22cc4064aac7436ba4032971759a855d9f4894ac9aee742949)
```

Como usted mismo se ha dado cuenta, es costoso encontrarlo pero sencillo de validar que el valor es correcto.

Si desea probarlo con un acertijo que tenga más ceros a la izquierda por ejemplo: 00000001, verá que el tiempo que tomará en encontrarlo puede ser mayor, por lo que las blockchain tratan que el tiempo sea constante entre la creación de cada bloque, ajustando la complejidad del acertijo cuando los mineros lo están encontrando muy rápido, en el caso de bitcoin, se trata de crear 2016 bloques cada quince días, ajustando la dificultad de la prueba de trabajo cuando no se está cumpliendo esta regla[12].

¿Sabes qué es esto?



[12] El método GetNextWorkRequired del main.cpp de Bitcoin tiene esta lógica.

El dibujo le pertenece a Mack, quién realizó una prueba de cómo se podía minar bitcoin a mano y descubrir cuanto podía tardar. Definitivamente rápido no fue, pero es meritorio que lo intentara y pudo calcular un hash en un cuarto de hora. Eso significa una interacción, recuerden que debe hacerse varias hasta encontrar el desafío, un hash que inicie con una cierta cantidad de ceros. En promedio toma 128 intentos para encontrar el *nonce*, por lo que necesitaría un día y medio (sin tener interrupciones) para lograr minar un bloque. Por lo tanto, el día que el mundo se quede sin energía eléctrica, ya sabemos cuánto tiempo va a tomar la creación de un bloque usando lápiz y papel.

Prueba de participación - Proof of Stake (PoS)

El algoritmo de consenso PoS fue creado el 2011 como una alternativa a la prueba de trabajo creada por Bitcoin. A pesar de que tanto PoS como PoW comparten objetivos similares, también presentan algunas diferencias y particularidades fundamentales. Especialmente, en lo relativo a la validación de nuevos bloques.

El algoritmo de consenso basado en la prueba de participación es realizada por el minero que cuente con la mayor participación en las transacciones del bloques a crear, en otras palabras, es realizada por el minero que cuente con mayor cantidad de monedas vinculadas en las transacciones. El acuñador o validador de cada bloque (forger), es determinado por la inversión en la propia criptomoneda, y no por la cantidad de poder computacional destinado. Cada red Blockchain basada en pruebas de participación puede ser implementada con distintas maneras, pero por lo general utilizan un proceso de elección pseudo-aleatoria que toma en consideración el capital del nodo y el tiempo que ha permanecido inmóvil la moneda (edad de las moneda - "staked"), aunque siempre se le agrega un factor de aleatorización.

La prueba de participación es un método de consenso que asegura que una transacción sea correcta por medio de una solicitación a los usuarios para que demuestren que son dueños de cierta cantidad de divisa. Es diferente a los sistemas de prueba de trabajo que funcionan haciendo hashing a los algoritmos para validar las transacciones electrónicas. Se utiliza con más frecuencia como un

suplemento de prueba de trabajo en Peercoin y unas cuantas otras divisas electrónicas.[13]

En el algoritmo de la prueba de participación con tan solo tener criptomonedas en tu poder eres recompensado. Es decir, tener criptomonedas en tu dirección es la única prueba que refleja que participas en la red. Los wallet de los usuarios se encargan de almacenar y validar bloques.

Los bloques se generan de manera semi-aleatoria, teniendo prioridad, quienes más monedas tienen almacenadas y durante más tiempo. Todos los que tengan monedas en su wallet, recibirán una recompensa, pero aquellos que más monedas tengan, recibirán una recompensa mayor.

Básicamente, el sistema Proof of Stake no necesita de potentes máquinas especializadas, vale cualquier equipo de cualquier usuario. Solamente se debe disponer de una wallet o cartera y una cantidad de monedas.

No obstante, no a todo el mundo le gusta Proof of Stake. Sus detractores opinan que es un modelo que potencia el acaparamiento. Cuantas más monedas tienen un usuario más recompensa recibe y, por tanto, se fomenta la aparación de criptomonedas. Esto provoca que descienda el número de monedas circulante y se aumente el precio de manera artificial.

La Blockchain de Ethereum se basa actualmente en un algoritmo PoW, están valorando adoptar un modelo mixto. Prueba de trabajo en los primeros años, para después migrar a prueba de participación, defendiendo que esto les permitiría quedarse con lo mejor de ambos modelos.

[13] https://es.bitcoinwiki.org/wiki/Prueba_de_participaci%C3%B3n

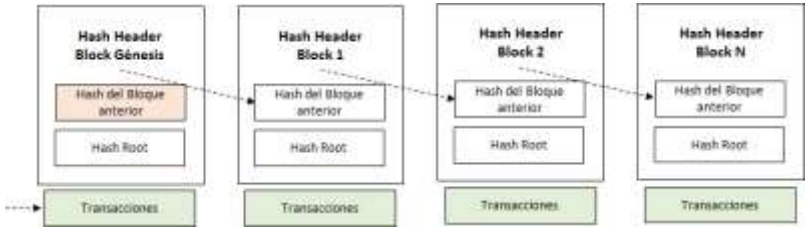
Para *Ethereum* , el protocolo *Clique* es un ejemplo de un mecanismo de consenso *de Prueba de Autoridad* más amplio, para aquellos que no saben cómo funciona PoA, es un protocolo muy simple, en el que, en lugar de que los mineros compitan para encontrar primero el "nonce" a través de una prueba de fuerza bruta (PoW), los firmantes autorizados en cualquier momento pueden crear nuevos bloques.

Este algoritmo se desarrolló por parte de Sunny King y Scott Nadal en 2011 y la primera vez que se implementó en una criptomoneda fue en 2012, cuando lanzaron PeerCoin (PPC), la primera criptomoneda basada en Proof of Stake (PoS).[14]

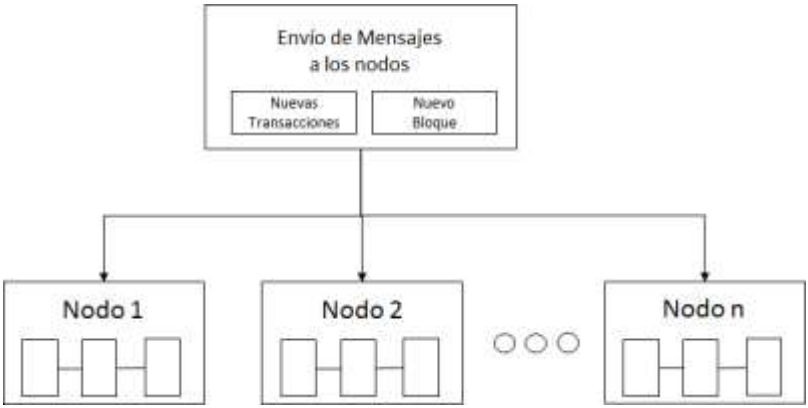
https://medium.com/coinmonks/private-ethereum-by-example-b77063bb634f

[14] https://academy.bit2me.com/que-es-proof-of-stake-pos/

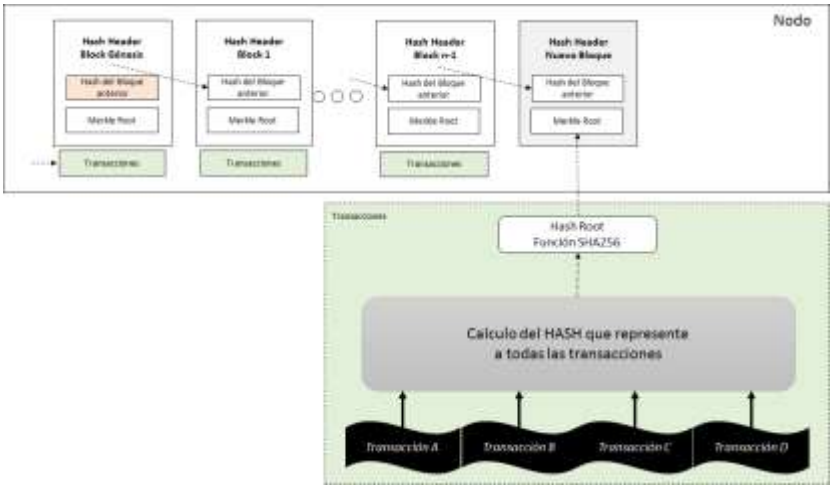
Capítulo 6
Los contratos inteligentes (Smart contract)



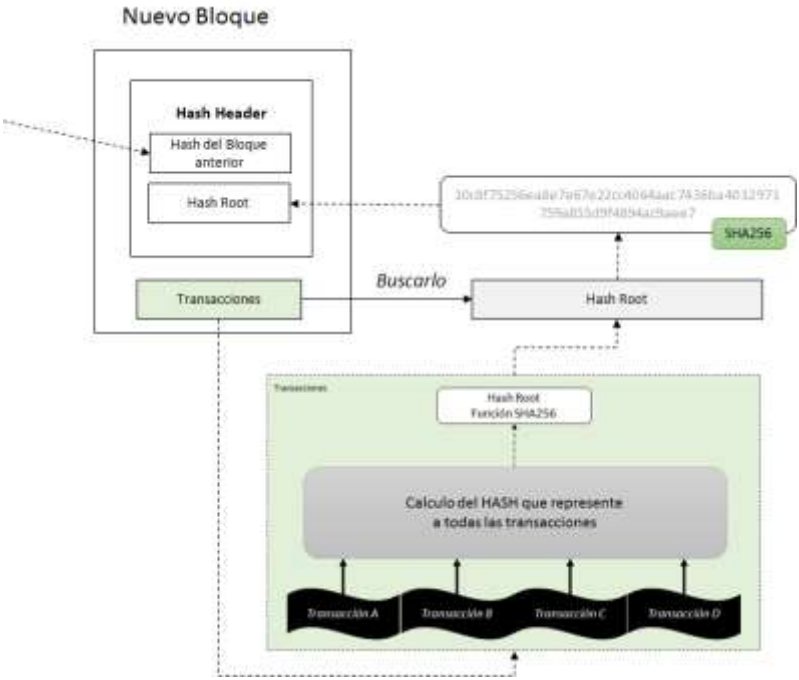
Endosar Transacciones - Envío de mensajes



Anclar Transacciones - Creación de bloques y consenso



Inmutación de datos – Hash Root



Algoritmos para generar el Hash Root

Hashlink

Capítulo 7
Creación de una Dapp

Medios de Pago

Capítulo 8
Las criptomonedas

Medios de Pago

Método de inversión

Transferencia de divisas

Stable coin/Coin.

La recompensa, el señoriaje y la inflación del 35%

Vamos a ver un caso típico de uso de hash para transacciones financieras, por lo que te pido que mires este diagrama:

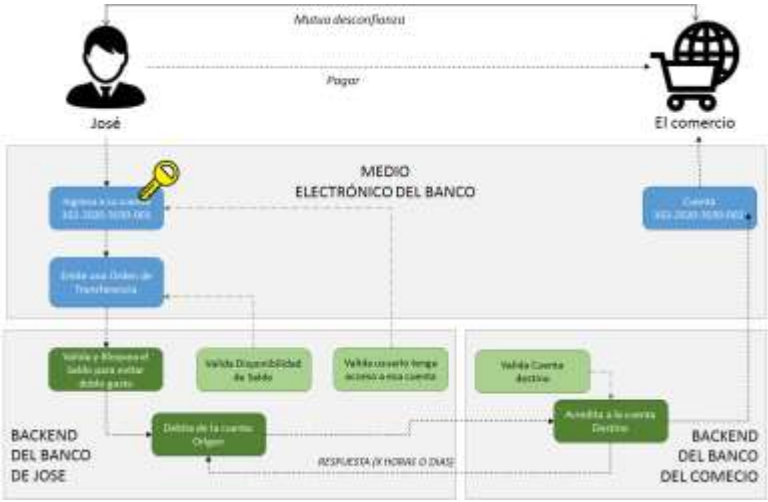
En este ejemplo se explica como José desea adquirir un producto a "el comercio", para lo cual deberá cancelar el importe de la cuenta,

una vez que "el comercio" compruebe que el pago ha sido efectuado transferirá el bien o servicio que el cliente haya adquirido.

Desde el punto de vista social, hay un pequeño problema de desconfianza mutua, que analizaremos paso a paso durante este capítulo, sin embargo para solucionarlo, al menos una parte de él, se puede usar un intermediario (el banco) que ayude a garantizar a ambas partes que el dinero ha sido enviado correctamente y que la contraparte no lo repudie; también te demostraremos como los hash pueden ayudar a resolver el mismo problema, utilizando una criptomoneda que sea validada por una cadena de bloques, pero sin intermediarios.

METODO 1: Usando la transferencia interbancaria

El siguiente gráfico muestra cómo se resuelve el problema si José realiza un pago utilizando una transferencia interbancaria, considerando que ambos utilizan bancos diferentes:



José se autentica en el portal web o la aplicación del banco que tiene instalada en su celular, si el banco determina que tiene el acceso respectivo ingresará a su cuenta, caso contrario será rechazado. Luego, tendrá que emitir una orden de transferencia, el banco debe asegurarse que el momento de emitir dicha orden el monto a transferir deberá ser menor al saldo total de su cuenta, caso contrario le mostrará un mensaje indicando que no cuenta con el saldo suficiente para realizar dicha transferencia.

Cuando la orden ha sido emitida correctamente, el banco bloquea el saldo en la cuenta del usuario para evitar que en ese momento haga otra transferencia, así evita que haga un doble gasto del dinero que dispone, un proceso automático del banco debitará de la cuenta del cliente el saldo que se va a transferir, además deberá registrar la transacción en la tabla de movimientos de cuentas y posteriormente acreditará el mismo saldo en la cuenta destino, es probable que dependiendo del tipo de cuenta y las opciones comerciales que el banco ofrezca a sus clientes se realicen otras transacciones asociadas como: el cobro de comisiones por la transferencia, el cobro del impuesto a las transacciones financieras, comisión por transferencia interbancarias, etc.

La transferencia sería enviada a otro intermediario que lo enviará al banco destino, salvo el caso que exista un convenio entre dichos bancos que la transacción iría directamente; El banco destino validará que la cuenta que va a recibir el dinero exista dentro de sus base de clientes, caso contrario le mostrará un error que esa cuenta no existe, en el caso que el cliente haya ingresado un número mal, es probable que su transacción se vaya a otra persona y corra el riesgo de perder su dinero, el banco no se hace responsable de ese error cometido por el cliente; Finalmente, luego de este proceso, el

dinero ya está disponible en la cuenta del "el comercio" y acto seguido podrá hacer entrega del producto o servicio a José.

La confianza en la transacción

Ambos bancos resuelven el problema de confianza para "El comercio" y también a José aunque nuevamente deberá confiar que "El comercio" es honesto y que entregará el producto o servicio ofrecido, caso contrario procederá a demandarlo en las entidades correspondientes pero, con la evidencia de haber realizado el pago (constancia de transferencia de dinero), que a su vez como ayudaría al juez.

Los puntos importantes en que los bancos ayudaron a generar la confianza son:

El banco de José

- Autenticó a José para garantizar que nadie ingrese en su nombre a hacer una transferencia sin su consentimiento.
- Permitió que José manifieste su voluntad de transferir su dinero a otra cuenta.
- Permitió que José confirme que la transferencia la realizó a la cuenta correcta, en muchos casos le muestra el nombre del destinario antes de aceptar la transacción.

El banco de "El comercio"

- Permitió que "el comercio" confirme que la transferencia (el pago) sea ha realizado con éxito.

Duración del proceso

A pesar que la transferencia del dinero fue rápida es probable que debido a la falta de confianza entre los bancos, generará como

consecuencia que "el comercio" disponga del dinero unas horas o días después, en caso de ser internacional el tiempo se incrementa. Hay que entender que los bancos necesitan confirmar que no se trate de un fraude, eso toma tiempo, además que el banco de "El comercio" debe asegurarse que el banco de José le va a dar el dinero que va a transferir.

Responsabilidad de ambos Banco

- Si alguno de los sistemas del banco no están disponibles, la transferencia no podrá ser realizada, por lo que ambos bancos deben asegurar que siempre estará en alta disponibilidad.
- Los bancos deberán evitar que se realicen fraudes pero, en el caso de ocurrir debe siempre guardar evidencias para delegar la responsabilidad al cliente o al "el comercio".

Responsabilidad de José

- No debe dejarse estafar de ningún modo, como por ejemplo: evitar que le clonen la tarjeta, evitar que le roben la clave de internet o cualquier otro método de fraude financiero pero, ¿cómo puede evitarlo si todo el control lo tiene el banco?, ya discutiremos este punto más adelante.

Responsabilidad de "El comercio"

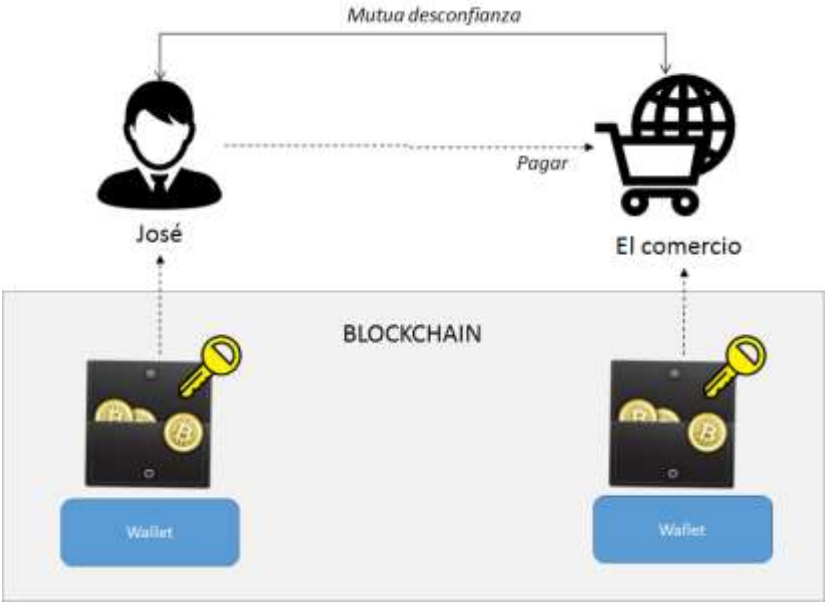
- No debe dejarse estafar de ningún modo, como por ejemplo: recibir transferencias fraudulentas, aceptar tarjetas falsas o evitar que usen tarjetas robadas pero, ¿cómo puede evitarlo?, este punto también lo discutiremos más adelante.

METODO 2: Usando criptomonedas

Quizás les pueda parecer muy raro el uso de los hash para este caso de negocio pero, es un ejemplo extraordinario la forma como se usa los hash para recibir transacciones de pagos y como reclamar el dinero sin recurrir a una entidad central que administre y evite el doble gasto, al entender este algoritmo descubrirá un nuevo paradigma que le ayudará a enviar o recibir evidencias, mensajes o transferencias de activos en forma descentralizada.

Te invito a ver el siguiente diagrama que muestra cómo se resuelve el problema en forma descentraliza, cuando José transfiere unos bitcoins a "el comercio" que equivalen al importe a pagar por el bien o servicio que "el comercio" le va a transferir:

:



Los wallet

Ambos tienen una billetera electrónica que contiene sus criptomonedas (wallet) registrada en la Blockchain, muy similar a lo que sería una cuenta del banco.

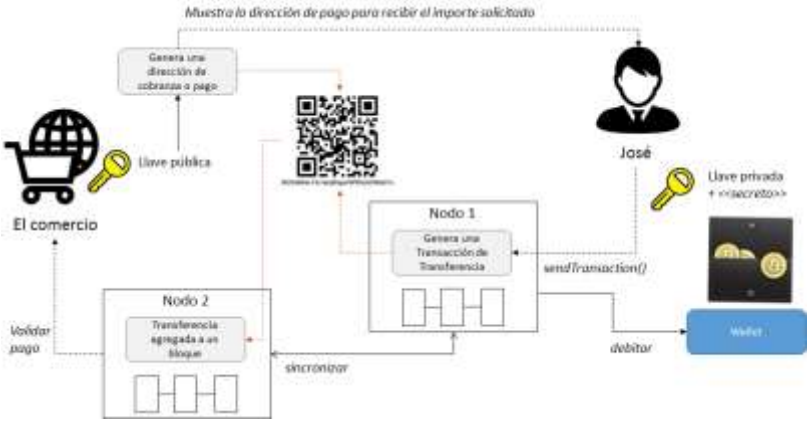
No importa en donde sacaron sus cuentas, ellos podrán transferirse entre sí, a diferencia que si sacan cuenta en un banco diferente. Ambos pueden demostrar que son los propietarios de esas billeteras utilizando sus llaves privadas y además manifestar su voluntad cuando deseen transferirlas a otras billeteras.

La realidad de las transferencias interbancarias

En el ejemplo anterior, vimos que José debe ser **autenticado** por el banco para garantizar que nadie ingrese en su nombre a hacer una transferencia sin su consentimiento, sin embargo, es probable que ante un fraude alguien suplante su identidad, y verás que en ninguno de los casos, José pudo realmente controlarlo.

Por otro lado, "el comercio" a pesar de haber recibido la confirmación de la transacción, el banco podrá decirle días después que se trató de un fraude y deberá asumir el riesgo a pesar de no tener control de esa situación.

Como funciona los pagos a través de bitcoin:



El comercio en base a su clave pública crea una dirección de cobranza, conocida como dirección bitcoin, para generarla no requiere de ningún nodo ni de alguna unidad central que administre las direcciones de pago. Para crear estas direcciones, bitcoin propone un protocolo basado en hash que analizaremos más adelante.

El cliente al recibir la dirección de pago, procede a generar una transacción en algún nodo que se encuentre conectado a la red de blockchain, donde se identifica y a la vez manifiesta su voluntad de hacerlo, utilizando su llave privada y un secreto que colocó cuando creó su billetera electrónica.

El nodo valida la transacción y se la comunica al resto de nodos para que sea incluida en el siguiente bloque, una vez que la transacción ha sido confirmada e incluida en un bloque, el vendedor podrá verificarlo usando cualquier explorador de transacciones o conectándose a cualquier nodo y haciendo la consulta.

Reclamar el pago

Una vez que el vendedor ha confirmado que la transacción ha sido realizada, deberá reclamar el pago, para hacerlo el protocolo de bitcoin se encargará

Para este reto se requiere

Ya que le permiten transferir esas criptomonedas a otras personas cuando ellos lo crean pertinente.

José desea pagar la cuenta en el comercio por unos productos o servicios que han adquirido, para lo cual se necesitará:

- El comercio debe indicar la cantidad de criptomonedas que José debe transferir.
- José deberá ingresar a alguna de sus billeteras y demostrar que es el propietario y emitir una orden de transferencia desde su billetera hacia "el comercio".
- "El comercio" deberá validar que José ha transferido la cantidad de monedas suficientes antes de realizar la entrega del bien o servicio.
- La cantidad de monedas que utilizó José deben ser reducidas de su billetera para evitar que pueda usarlas nuevamente.
- El comercio deberá poder utilizar en el futuro esas monedas recibidas en esta transacción.

en realidad esta genialidad . Voy a explicarte

emplean algunas criptomonedas bitcoin para recibir pagos es la creación de direcciones.

en el caso del protocolo Bitcoin para transferencia de dinero, un uso donde se mezcla muchos cálculos hash es para la creación de una dirección de pago, los creadores de Bitcoin creyeron conveniente hacer que cuando un comercio o sitio web desee cobrar una cantidad de Bitcoin por la venta de un determinado producto o servicio, se genere un dirección de pago, la misma que puede hacerse en forma descentralizada, sin necesidad de tener una unidad central que centralice las dirección de pago.

La confianza reciproca

Ernst fehr Michael kosfeld hormana oxitocina, reciprocidad. El juego de la Confianza pag 153

¿Qué es la trazabilidad?

La trazabilidad se define como una serie de procedimientos que permiten conocer el origen, la historia, la ubicación y la trayectoria de un producto a lo largo de la cadena de suministro en un momento dado, a través del uso de herramientas tecnológicas determinadas. Actualmente, la trazabilidad se realiza con medios informáticos convencionales gestionados centralizadamente, que carecen de la transparencia e inmutabilidad de la cadena de bloques. En este sentido, Blockchain representa un factor disruptivo e innovador tanto en la trazabilidad como en muchos otros ámbitos en los que se requiere de la documentación y la certificación de los procesos de una manera fiable e incorruptible. Los datos almacenados en una cadena de bloques no pueden ser modificados, borrados o censurados, por lo que la información que contiene goza de una dimensión de confianza por sí misma, y puede ser auditada y certificada en tiempo real sin la participación de intermediarios (autoridades, organismos certificadores, entre otros).

¿Por qué es importante la trazabilidad?

"La historia que cuenta un producto le agrega valor, proporciona al cliente motivos poderosos para comprarlo. La narrativa vende". – Juan F. Bolaños, CEO de Blochchain Andina

Ingresar la tecnología Blockchain a nuestros productos es una forma de demostrar que somos empresas responsables en nuestros procesos y comprometidos con nuestros clientes. Por ejemplo, las empresas dedicadas a la producción de vino español, vino chileno o vino argentino podrían mostrar la forma a través de la cual mantienen la calidad garantizada de sus uvas, el tipo de fertilizante o pesticida que están usando, cómo se labró la tierra en la que están cosechando, cuánta agua se usa o hasta temas que podrían ir hacia la responsabilidad con sus trabajadores. Otro ejemplo es demostrar cómo se obtuvo el Oro de una joya, siendo responsables en su producción y diferenciándose abiertamente de los que no lo son. Información que para muchos de nosotros como consumidores nos es difícil obtener, pero que como empresa debemos tener la seguridad, transparencia y disposición para brindarla.

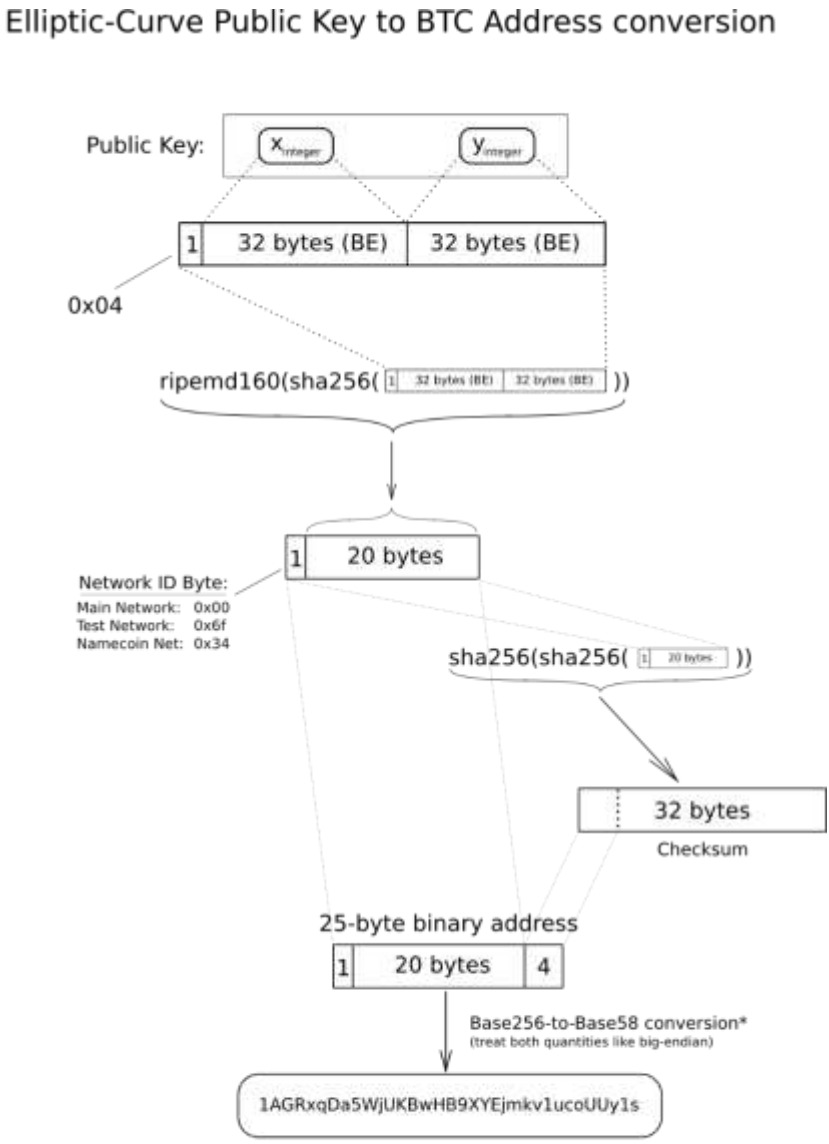
.

Tengamos en cuenta que esto es solo uno de los beneficios que podríamos obtener de esta tecnología, aplicarla continuamente nos permitirá sacar mayor provecho de nuestras certificaciones, pasar auditorías, obtener resultados de mercado en tiempo real e incluso identificar la ruta del delito de productos adulterados o de contrabando.

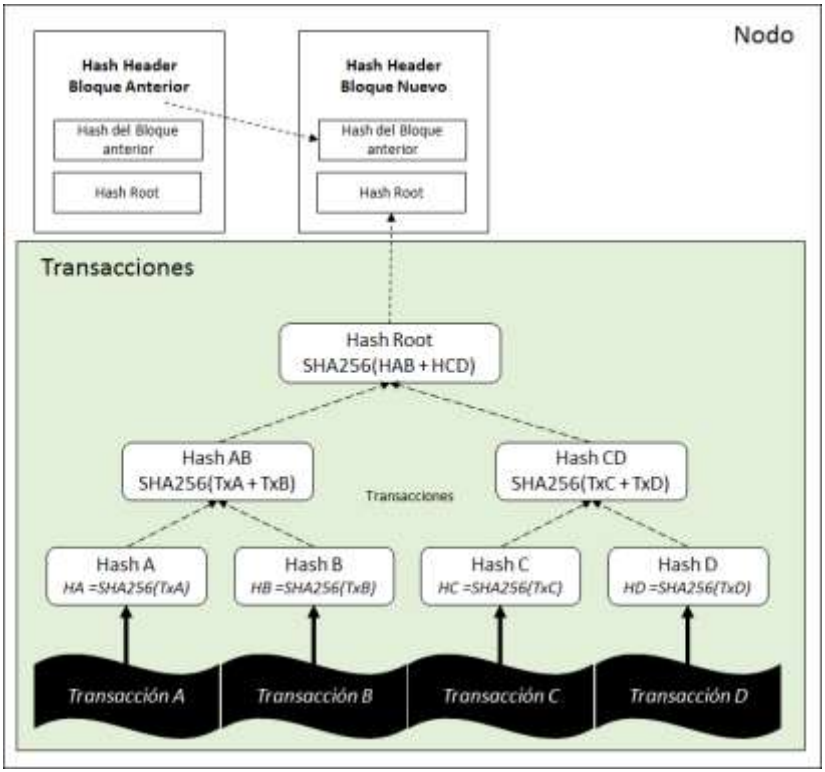
Los algoritmos inamovibles de la Blockchain dejarán registrados para siempre la información introducida en todos los procesos humanos. Nunca ha existido jamás en toda historia humana una herramienta más poderosa para garantizar el ejercicio y establecimiento de la "verdad". En buena parte, las aplicaciones empresariales de la Blockchain carecen de sentido si una empresa no está dispuesta a desnudarse en términos de transparencia. La empresa debe estar dispuesta a decirle a sus clientes: "Esto es lo

que soy. Estos son mis procesos, estos mis productos, y no tengo nada que esconder".

Así que, querido lector, siempre indague sobre el origen del pescado o langostino de su plato, que puede ser víctima de estafa o de intoxicación.


Elliptic-Curve Public Key to BTC Address conversion
Public Key:
x integer
y integer
1
32 bytes (BE)
32 bytes (BE)
0x04
ripemd160(sha256(
))
1
20 bytes
Network ID Byte:
Main Network: 0x00
Test Network: 0x6f
Namecoin Net: 0x34
sha256(sha256(
))
32 bytes
Checksum
25-byte binary address
1
20 bytes
4
Base256-to-Base58 conversion*
(treat both quantities like big-endian)
1AGRxqDa5WjUKBwHB9XYEjmkv1ucoUUy1s
*In a standard base conversion, the 0x00 byte on the left would be irrelevant (like writing '052' instead of just '52'), but in the BTC network the left-most zero chars are carried through the conversion. So for every 0x00 byte on the left end of the binary address, we will attach one '1' character to the Base58 address. This is why main-network addresses all start with '1'
etotheipi@gmail.com / 1Gffm7LKXcNFPrtxy6yF4JBoe5rVka4sn1

https://en.bitcoin.it/wiki/Technical_background_of_version_1_Bitcoin_addresses



Que es la Blokchain

https://onezero.medium.com/how-does-the-blockchain-work-98c8cd01d2ae