Blockchain y sus aplicaciones

Benjamin Yahari Navarro

Universidad Católica Nuestra Señora de la Asunción,
Asuncion, Paraguay
benjaminyahari@outlook.com
http://www.universidadcatolica.edu.py/

Abstract. Artículo que trata sobre la tecnología Blockchain y las aplicaciones que esta teniendo en la actualidad en el mundo de las finanzas y en la sociedad en general.

Key words: Blockchain, criptomonedas, tecnología, transacciones digitales, criptografía, economía.

1 Introducción

Esta tecnología tuvo su origen como soporte para las transacciones con bitcoin, fue originalmente utilizada por figuras que se oponían al sistema y que querían conseguir independencia del control central. Pero la idea en si, como forma de almacenar los datos tiene antecedentes muy anteriores, en la década del 70: el modelo relacional y las base de datos SQL; las grandes organizaciones pagaban mucho dinero por grandes bases de datos y colocaban todos sus activos de datos más preciados en estos sistemas: su memoria institucional y sus relaciones con los clientes. Y aun hasta hoy, el lenguaje SQL que alimenta la gran mayoría de los sistemas de gestión de contenidos que circulan por la web.

Un segundo antecedente es la World Wide Web, creando redes de computadoras, que permitían comunicarnos con protocolos como Telnet, Gopher, Usenet y Email que proporcionaban una interfaz de usuario para las primeras conexiones[1].

Sin embargo, las bases de datos y las redes nunca llegaron a entenderse completamente. Nunca se encontró un estándar común que les permitiera interoperar sin ningún problema. Interactuar con una sola base de datos es bastante fácil: a través de formularios y aplicaciones web como las que utilizas todos los días. Pero la dificultad es conseguir que las bases de datos trabajen juntas, de forma invisible, para nuestro beneficio, o conseguir que las bases de datos interactúen sin problemas con los procesos que se ejecutan en nuestros propios dispositivos. Esos problemas técnicos son enmascarados por la burocracia, pero sentimos su impacto cada día en nuestras vidas, muchas veces pagando un monto adicional a empresas que se dedican a que los distintos sistemas interactúen correctamente.

Veamos un ejemplo concreto, en este caso una transacción monetaria y el rol que el bitcoin podría tener. Pagamos un dolar por algún bien material. Esta

transacción se realizó porque el valor de un dolar está representado por un billete, el cual fue creado por un Gobierno en el que ambas partes confían, que se reconocen y aceptan. Cuando esta compra-venta se concrete, los detalles deben quedar escritos en un libro de cuentas.

En el caso de transacciones electrónicas entran en participación terceras partes fiables como bancos u operadores como Google Wallet o Paypal. Pero se sigue manejando una moneda centralizada como el dolar. Al final, las entidades financieras concilian las operaciones y obtienen sus beneficios correspondientes.

La situación cambia cuando la moneda es virtual y no la emite una entidad financiera o administración. En este caso se garantiza la integridad y fiabilidad basándose en el *consenso*. Aquí entra en juego el blockchain. El Blockchain (o cadena de bloques) es una base de datos compartida que funciona como un libro para el registro de operaciones de compra-venta o cualquier otra transacción.

Es un conjunto de apuntes que están en una base de datos compartida en la que se registran mediante códigos las transacciones realizadas. Al utilizar claves criptográficas y al estar distribuido por muchos ordenadores presenta ventajas en la seguridad frente a manipulaciones y fraudes. Una modificación en una de las copias seria inútil, ya que se debe realizar el cambio en todas las copias porque la base es abierta y pública [2]. La potencia de blockchains viene por la conjunción de sus tres grandes cualidades: irrefutable, irrevocable y distribuida.

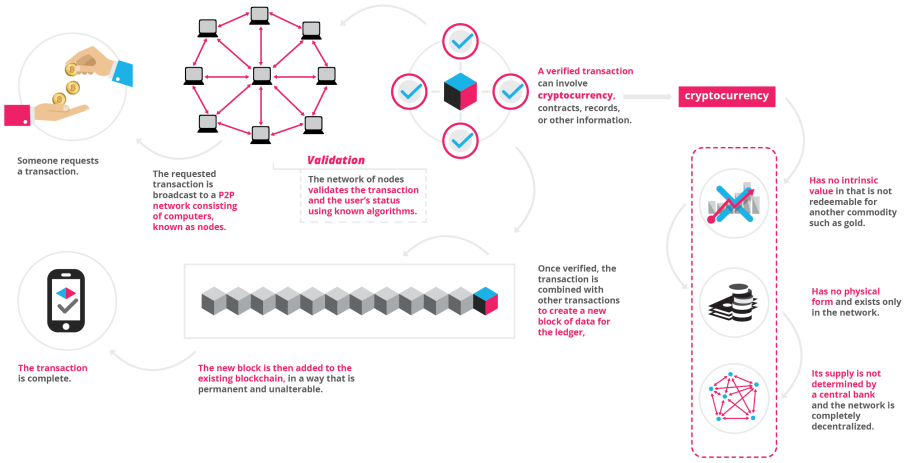


Fig. 1. Transacciones con criptomonedas.

Ahora bien, esta tecnología puede cambiar el mundo porque este modo de operar, en el que toda la información se distribuye con total transparencia por todos los nodos del sistema, puede terminar aplicándose a todo tipo de transacciones entre todo tipo de intervinientes, públicos o privados[3].

> "Todo sistema en el que haya algún tipo de compartición está sujeto a que una tecnología como blockchain pueda aplicarse".
> Pablo F. Iglesias, bloguero y analista de SocialBrains[1].

Se pueden clasificar según el acceso a los datos en dos tipos: públicas y privadas[4].

- Las públicas son, por ejemplo, sobre las que trabajan bitcoin o ethereum, en donde el publico en general tiene acceso. Es aquella en la que no hay restricciones ni para leer los datos de la cadena de bloques (los cuales pueden haber sido cifrados) ni para enviar transacciones para que sean incluidas en la cadena de bloques. En ellas es fácil entrar y salir, son transparentes, están construidas con precaución para la operación en un entorno no confiable.
- En las privadas solo pueden entrar quienes digan los propietarios. Es aquella en la que tanto los accesos a los datos de la cadena de bloque como el envío de transacciones para ser incluidas, están limitadas a una lista predefinida de entidades.

Estos tipos de cadenas de bloques son los casos mas extremos pudiendo también haber casos híbridos o intermedios.

[1] SocialBrains es una consultora de transformación digital, smart data y ciber reputación con base tecnológica y medios de ingeniería social.

2 Componentes

La tecnología está basada en cuatro fundamentos: el registro compartido de las transacciones (ledger), el consenso para verificar las transacciones, un contrato que determina las reglas de funcionamiento de las transacciones y finalmente la criptografía, que es el fundamento de todo[5]. En esta sección veremos los componentes que hacen esto posible.

2.1 Bloques

Blockchain es un registro de todas las transacciones que se empaquetan en bloques que los mineros luego se encargan de verificar. Luego serán agregadas a la cadena una vez terminada su validación y distribuidas a todos los nodos que forman la red. En la actualidad, la cadena de bloques bitcoin ocupa unos 170 gigas aproximadamente)[6].

Un bloque es un conjunto de transacciones confirmadas e información adicional que se ha incluido en la cadena de bloques. Cada bloque que forma parte de la cadena (menos el primer bloque que inicia la cadena) está formado por:

1. Un código alfanumérico que enlaza con el bloque anterior
2. El "paquete" de transacciones que incluye
3. Otro código alfanumérico que enlazará con el siguiente bloque.

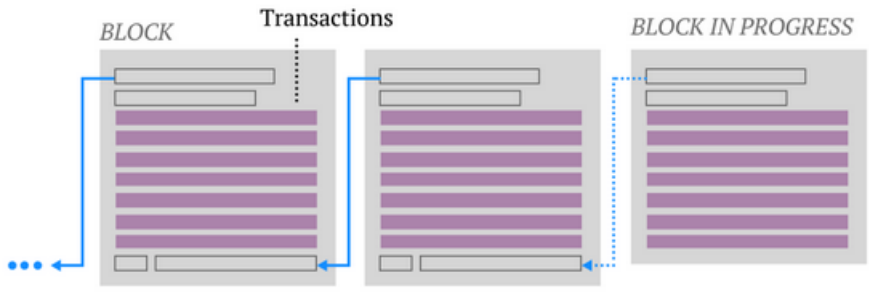


Fig. 2. Cadena de bloques

El bloque en progreso lo que intenta es averiguar con cálculos el ultimo punto. Los bloques son generados por los mineros

2.2 Mineros

Los mineros son ordenadores dedicados que aportan su poder computacional a la red para verificar las transacciones que se llevan a cabo. Son computadoras que se encargan de autorizar la adición de los bloques de transacción. Estos siguen los siguientes pasos[7]:

1. Las nuevas transacciones se transmiten a todos los nodos
2. Cada nodo de la minería recoge nuevas transacciones en un bloque.
3. Cada nodo minero trabaja en la búsqueda de una prueba de trabajo para su bloque.
4. Cuando un nodo de la minería encuentra una prueba de trabajo, este transmite el bloque a todos los nodos.
5. Los demás nodos acepta el bloque sólo si todas las transacciones son válidas y no se hayan gastado.
6. Los nodos expresan su aceptación del bloque trabajando en la creación del próximo bloque en la cadena, utilizando el hash del bloque aceptado como el hash anterior.

Cada vez que alguien completa un bloque recibe una recompensa en forma de bitcoins y/o por cada transacción que se realiza.

2.3 Nodos

Son computadoras conectadas a la red utilizando un software que almacena y distribuye una copia actualizada en tiempo real del blockchain.

Cada vez que un bloque se valida y se añade a la cadena, el cambio es comunicado a todos los nodos y este se añade a la copia que cada uno almacena.

Algunos, conocidos como mining pools o grupos de minería, se encargan ademas de escuchar nuevas transacciones y agruparlas en bloques para proponerlos como trabajo a los mineros,que luego de ser confirmados son propagados a la red y añadidos a la cadena.

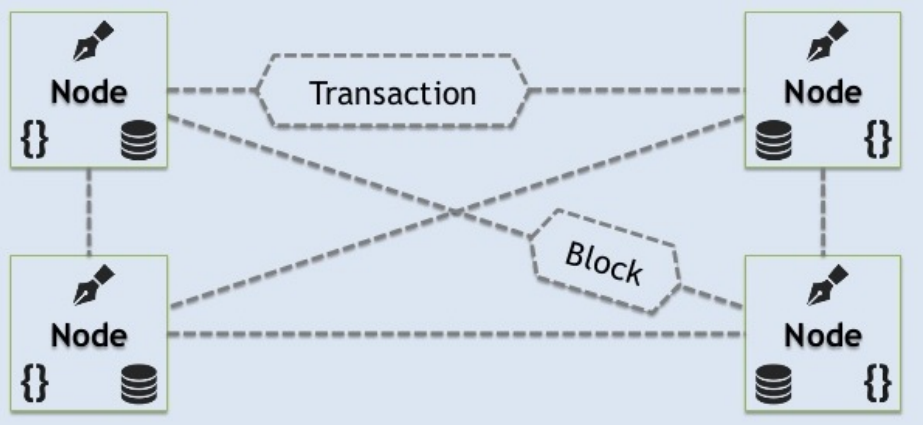


Fig. 3. Componentes blockchain

3 Características y funcionamiento

Las propiedades mas importantes para describir como funciona la tecnología blockchain son las siguientes: es de carácter descentralizado, pues esta no requiere un organismo o entidad central de confianza, es una tecnología distribuida y de consenso, porque que parte de unas reglas claras y un consenso sobre la validez de las transacciones y su estado, abierta tal que cualquier usuario puede hacer uso de ella y finalmente segura gracias a la verificación criptográfica [8].

3.1 Descentralizado

Expertos explican[9], que las redes blockchain son altamente escalables, descentralizadas y peer-to-peer. Es asi que, la integridad está basada en un mecanismo de consenso, en vez de una infraestructura basada en la confianza sobre un organismo central, como sería un banco u otra entidad financiera. La red P2P evita que un único participante o grupo controlen el sistema completo. Todos los integrantes de una red se adhieren, a los mismos protocolos, ya sean individuos, organizaciones o actores estatales. Las transacciones son irreversibles, por lo que una vez realizadas no pueden anularse, modificarse o revertirse.

Así, se eliminan los riesgos que vienen con los sistemas centralizados[10]. La red carece de puntos críticos o centrales de vulnerabilidad que podrían ser explotados. Los métodos de seguridad Blockchain incluyen el uso de la criptografía de clave pública: Una clave pública es una dirección en la cadena de bloque. Los tokens, como por ejemplo bitcoins, son enviados a través de la red y se registran como pertenecientes a esa dirección. Una clave privada es como una contraseña que le da acceso a su propietario a sus activos digitales.

Cada nodo o minero en un sistema descentralizado tiene una copia de la cadena de bloqueo. La calidad de los datos se mantiene mediante la replicación masiva de bases de datos[11]. No existe una copia oficial centralizada y ningún usuario es de más confianza que cualquier otro.

3.2 Sistema abierto

Es abierto porque cualquier persona puede formar parte tan solo con descargándose el programa. Luego ella podrá realizar movimientos y transacciones con monedas virtuales y acceder a los datos registrados en su cadena de bloques.

A veces los bloques se pueden producir concurrentemente, creando un fork temporal. La cadena de bloques tiene un algoritmo especificado para marcar diferentes versiones de la cadena para que una con un valor más alto pueda ser seleccionada sobre otras. Los bloques no seleccionados para su inclusión en la cadena se denominan bloques huérfanos[12], como se observa en la figura 4.

Los peers de la red pueden tener de vez en cuando versiones diferentes de la base de datos. Estas solo guardan la versión con la puntuación más alta que conocen. Cada vez que un compañero recibe una versión de puntuación más alta (usualmente la versión antigua mas un solo bloque añadido) extienden o sobrescriben su propia base de datos y retransmiten la mejora a sus pares. Por

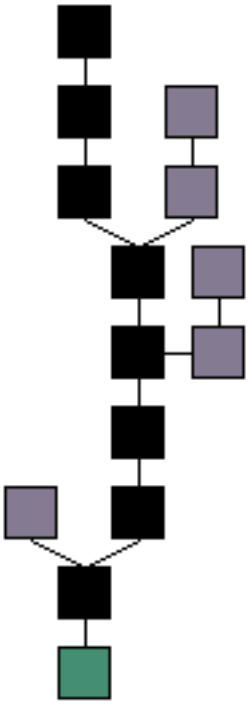


Fig. 4. Formación de cadena de bloque. La cadena principal (negro) consiste de la serie mas larga de bloques que surgen del bloque de origen (verde). Los bloques huérfanos (purpura) existen fuera de la cadena principal.

ejemplo, en una cadena de bloques utilizando el sistema de prueba de trabajo, la cadena con la prueba de trabajo más acumulativa siempre es la considerada válida por la red.

3.3 Seguridad

Los bloques que forman parte del blockchain son ordenados en la cadena por orden cronológico y tienen un código alfanumérico conocido como hash, que corresponde al bloque que los precede, gracias a ese hash todos están referenciados por el bloque que los creo, por lo que solo los bloques que contienen un código valido son introducidos en la cadena y replicados a todos los nodos. Es gracias a este método lo que hace virtualmente imposible modificar un bloque que ha sido introducido ya hace un cierto tiempo.

Los nodos mineros son los encargados de la creación de nuevos bloques de la cadena, computando y añadiendo luego a cada uno de ellos el hash y todas las nuevas transacciones correspondientes. Por lo tanto el blockchain nos permite llevar a cabo, una contabilidad publica de los movimientos realizados en la red

de manera transparente, minimizando la posibilidad de fraude, no permitiendo la perdida de datos y con un sistema totalmente trazable.

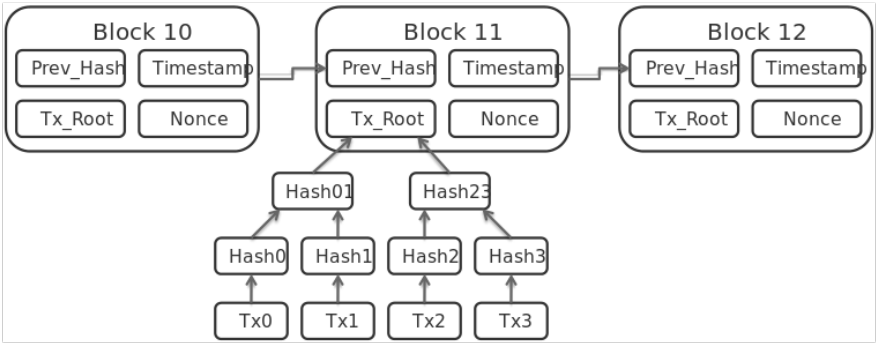


Fig. 5. Ejemplo de esquema blockchain

Es necesario que los nodos que integran la red estén sincronizados manteniendo almacenada la cadena de bloques correcta, es decir la que esta actualizada. Como también observamos anteriormente, cada bloque contiene información sobre las transacciones de un periodo concreto, estas son almacenadas en una estructura denominada Merkle Tree (en honor a su creador: Ralph Merkle), también la información criptográfica del bloque precedente es decir, el código hash (Las funciones de hash, permiten parear strings de un tamaño cualquiera a strings de tamaño fijo en una cantidad de tiempo razonable, en el caso de la moneda virtual Bitcoin se emplea la función hash criptográfica SHA-256, siendo sus apuntadores hash de un tamaño fijo de 256 bit), y un número único llamado *nonce*, el cual es un valor arbitrario que puede utilizarse una sola vez, es generado por los mineros mediante la prueba de trabajo (Proof of Work o PoW) y sirve como método sencillo para autenticar un bloque en caso de una posible modificación o reutilización de su contenido, sin tener que volver a procesar toda la cadena, ahorrando así mucho trabajo computacional.

Esta estructura de árbol binario, reúne pedazos de información y da como resultado un hash por cada uno de ellos, que vuelven a agruparse en pares y generan un nuevo hash que es agrupado con otro y así sucesivamente hasta alcanzar un único bloque raíz que se conoce como root hash, y es registrado en la dirección del bloque actual con el fin de reducir el espacio ocupado por cada bloque. Se puede observar un ejemplo en el gráfico 6:

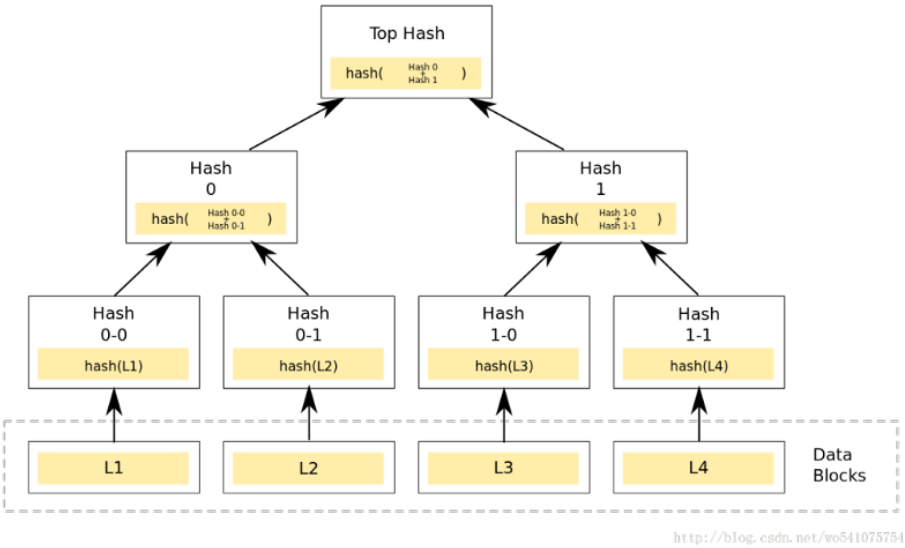


Fig. 6. Estructura merkle tree

Esta estructura permite recorrer cualquier nodo del árbol para la verificación de que ningún dato ha sido falsificado o adulterado.

Un bloque se verifica cuando el nonce, un número aleatorio que es utilizado una única vez, se encontró que, pasado por una función hash, proporciona un resultado menor que el valor objetivo. Una vez que el esfuerzo computacional satisface la prueba de trabajo, no se puede cambiar sin hacer de nuevo todo el trabajo, y, como los bloques están encadenados juntos, se deben calcular todos los bloques después de él también. Las pruebas de trabajo son esencialmente un sistema de una CPU, un voto. La decisión de la mayoría esta representada por la cadena mas larga, que tiene el mayor esfuerzo de pruebas de trabajo invertido. Para modificar un bloque pasado, para intentar robar bitcoins, un atacante debe rehacer todas las pruebas de trabajo y todos los bloques después de el y luego alcanzar y sobrepasar el trabajo de los nodos honestos[7].

Las cadenas de bloque también pueden utilizan otros esquemas de consenso, para serializar los cambios. Los métodos de consenso alternativos incluyen Proof of Stake y Proof of Burn.

4 Aplicaciones

Blockchain tiene un gran potencial de transformar los modelos de operación de negocios a largo plazo. Es una tecnología fundacional con la capacidad de crear nuevas bases para la economía global y para los sistemas sociales. Su uso promete traer incrementos significativos a la eficiencia de la cadena de suministro, transacciones financieras, libros de activos, y a la conexión social descentralizada.

Esta tecnología puede ser integrada en múltiples áreas y a continuación veremos algunas de ellas:

4.1 Monedas digitales

Una de las aplicaciones mas populares del blockchain son las cryptomonedas o monedas digitales, bitcoin siendo la mas conocida de todas.

A principios del 2009 nació el Bitcoin de la mano de Satoshi Nakamoto, seudónimo que identifica a la persona o equipo que crearon la criptomoneda, que en la actualidad es la moneda digital más famosa, se crea, se transfiere y se deposita de forma electrónica, además está protegida criptográficamente.

Esta divisa digital es una moneda descentralizada, nadie pueda controlarla. Está fuera del alcance de gobiernos o bancos centrales. Esta independencia de un organismo central es la principal característica respecto al resto de monedas convencionales.

Fig. 7. Logo de Bitcoin

Funcionamiento de Bitcoin

Para empezar utilizar bitcoin, primeramente se necesita de una billetera Bitcoin, donde se almacena las claves privadas que necesitamos para acceder a nuestras monedas. Estas billeteras pueden ser aplicaciones móviles o cuentas online en plataformas especializadas, algunas opciones disponibles son Bitcoin Core, Multibit, Armory, Blockchain.info, entre otras.

Como ya estábamos mencionando la tecnología que hace posible su funcionamiento es la cadena de bloques, todas las transacciones validas se agregan a la cadena, cronológico del Blockchain facilita la seguridad que aporta la criptografía.

Una transacción en la red bitcoin es una transferencia con bitcoins que va de una billetera a otra, por lo tanto, cada transacción se incluye en la cadena de bloques. En los monederos (o billeteras) aparece una clave de firmas que valida la transacción. Estas transferencias suelen ser confirmadas rápidamente, mediante el proceso conocido como minería.

Este es un sistema de consenso distribuido que sirve para verificar los movimientos pendientes y agregarlos definitivamente a la cadena. Este proceso impide que un bloque anterior sea modificado o anulado, ya que produciría la corrupción e invalidez de los bloques posteriores.

Características de Bitcoin

- Utiliza blockchain como tecnología base.
- Pagos rápidos P2P a nivel mundial.
- No tiene el problema del double-spend.
- Bajos costos de procesamiento.
- Decentralizado
- Disponible a cualquiera, abierto.
- Anonimato.
- Transparente.

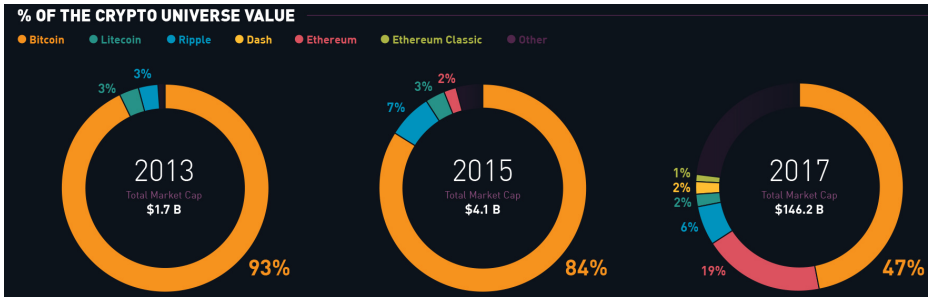


Fig. 8. Comparación de crecimiento de las criptomonedas.

Existen otras monedas virtuales, todas ellas de menor magnitud que Bitcoin:

- **Litecoin** tiene una tecnología parecida a bitcoin. Sus tiempos de confirmación son más reducidos. Es una criptomoneda mucho más joven por lo que está menos extendida, tiene un algoritmo criptográfico mas simple, mayor rapidez en la generación de bloques, las transacciones se procesan mas rápidamente.
- **Ether** está basada en el sistema ethereum, que es una plataforma para aplicaciones blockchain. Su aplicabilidad va más allá de las monedas digitales a través de los contratos inteligentes, tiene muchos usos en la industria. Al igual que Litecoin, es menos reconocida al ser una moneda creada en el 2014.
- **Dash** es un intento de mejorar el bitcoin en dos áreas: la rapidez de las transacciones y el anonimato. Para hacerlo posee una arquitectura de doble-capa con mineros y también nodos maestros que realizan funciones avanzadas tales como transacciones casi instantáneas y coin-mixing para proveer mas privacidad.

– **Ripple** es la tercera criptomoneda más usada del mundo. Esta respaldad por muchas entidades bancarias como la Royal Bank of Canada, Santander, UBS y UniCredit, es un sistema de conversión donde puedes intercambiar cualquier tipo de unidad de valor o moneda donde no hay minería involucrada.

Podemos observar en los gráficos la ventaja que aun lleva el bitcoin por sobre las demás competidoras, aunque es cierto que todas aun ido creciendo a lo largo del tiempo[13].

Fig. 9. Capital en el mercado

4.2 Smart Contracts

Una de sus aplicaciones emergentes más relevantes tiene que ver con lo que se conoce como "contratos inteligentes" o smart contracts.

En 1994, Nick Szabo, un jurista y criptografo, se dio cuenta de que un libro mayor descentralizado podría ser utilizado para realizar contratos digitales. En este formato los contratos pueden ser convertidos a código, guardados y replicados en el sistema y supervisados por la red de computadoras que corre el programa blockchain.

Los contratos inteligentes nos ayudan a intercambiar dinero, propiedades, activos o cualquier bien de valor de una manera sencilla, evitando los gastos por el servicio de intermediarios y sin revelar ningún tipo de información confidencial sobre las partes y/o naturaleza de la transacción.

Un ejemplo seria la venta o alquiler de un automóvil. Se podría hacerlo a través de blockchain pagando con monedas digitales. El comprador obtiene el recibo que es un smart contract, y la llave digital que llega a este en la fecha especificada. Si la llave no llega a tiempo, se le reembolsa el dinero. Si llega ambas partes reciben lo acordado a tiempo. El sistema funciona con la premisa de Si-entonces y tiene como veedores a mucha gente, así que se puede esperar un delivery sin inconvenientes. Si te doy la llave, de seguro obtengo mi pago, si enviás cierto monto de bitcoin por ejemplo, recibirás la llave del automóvil. El documento es automáticamente cancelado después de la fecha, y el código no puede ser interferido por ninguno sin que que el otro sepa ya que todos los participantes son alertados simultáneamente.

Ventajas de los SmartContracts:

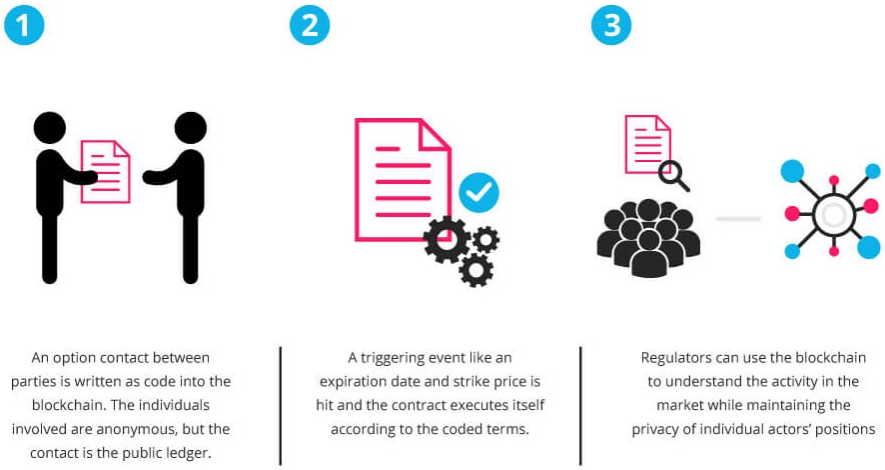


Fig. 10. Contratos inteligentes.

- Autonomía: Es uno mismo quien accede al acuerdo. No existen intermediarios, por lo que también se ahorra dinero.
- Confianza: Los documentos están encriptados en un shared-ledger. No pueden perderse.
- Backup: Todos los miembros de la red tienen los documentos duplicados.
- Rapidez: Ahorro de tiempo en el procesamiento de documentos, papeleos manuales, etc.
- Seguridad: Obtenida gracias a la criptografía.

4.3 Almacenamiento en la nube distribuido.

Anteriormente las compañías hosteaban sus propios servidores en sus instalaciones, esto les daba mas control pero repercutía en los costos, también necesitaban expertos para que instalen y mantengan los servidores, sin mencionar la inversión en servidores de redundancia.

Es por esto que las organizaciones han optado por la nube. Con tentadoras ofertas se pueden obtener servicios confiables de storage y backup sin mucha preocupación.

Pero esta comodidad también tiene sus desventajas. Cuando utilizamos servicios en la nube, ponemos nuestra confianza en terceros, les confiamos nuestra información muchas veces delicada y de mucho valor.

Existen paralelos entre la infraestructura del almacenamiento en la nube y la infraestructura financiera. Es por eso que también puede ser mas eficiente y menos costosa utilizando blockchain.

Blockchain permite la creación de un mercado de almacenamiento distribuido y descentralizado. Algunos hosts de la red pueden venden su capacidad de storage

sobrante y los que necesitan pueden pagar y subir sus archivos los cuales son encriptados, fragmentados y distribuidos inteligentemente por toda la cadena de bloques

Con blockchain se pueden obtener:

- Completa descentralización y verdadera redundancia: Los datos son almacenados en decenas de nodos distribuidos por todo el mundo, y difícilmente puedan ser afectados por ataques.
- Privacidad total: Terceros no controlan datos de usuario ni tienen acceso a ellos. Cada nodo solo almacena los fragmentos de estos datos, y los usuarios controlan sus propias llaves.
- Reducciones de costo: En comparación el almacenamiento por blockchain cuesta alrededor de 2 dolares por terabyte al mes comparado con Amazon que demanda 25 dolares por terabite[14].

Storj es otra de las empresas que esta incursionando en este sector, es una startup la cual esta realizando pruebas de un un prototipo un servicio que permite que el almacenamiento remoto se haga de forma distribuida utilizando una red basada en la Blockchain para así aumentar la seguridad.

4.4 Patentes/Registro de Propiedad.

La cadena de bloques también puede ser aplicada al registro de patentes o de protección intelectual, ya que en cada bloque se puede introducir todo tipo de información, incluyendo fechas o timestamps.

Una empresa como Apple, o un artista, podría probar que ha creado una tecnología o una música respectivamente, en una fecha concreta sin necesidad de hacer una aplicación formal para registrar la patente.

Podría vincular esos documentos internos al hash de una transacción realizada en ese momento y probar así que ellos han sido los primeros en desarrollarla. De este modo, el autor conseguiría controlar el uso de su obra en formato digital y garantizar que se le remunere adecuadamente

4.5 Internet of Things.

Existen billones de dispositivos inteligentes que pueden transformar la manera en que vivimos con el Internet de las cosas, pero también son fuente de vulnerabilidades y problemas de seguridad.

El modelo de seguridad centralizados tienen problemas de escalabilidad para soportar la demanda de muchos dispositivos. Es por eso que blockchain se muestra como una opción interesante, ya que esta construido con el control descentralizado en mente, un esquema de seguridad basado en ella es mucho mas escalable que lo normal[15].

Las protecciones brindadas contra la manipulación y alteración de datos pueden prevenir que un dispositivos extraño pueda conectarse a la casa, lugar de trabajo o sistema de transporte sin que sea detectado.

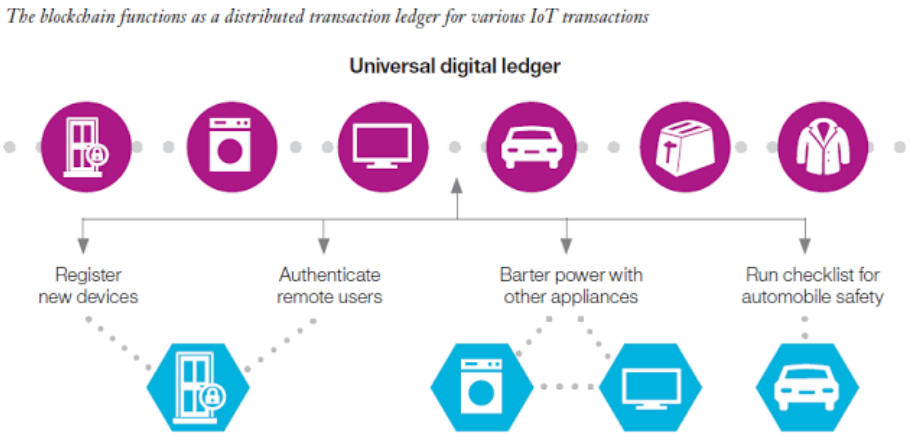


Fig. 11. Blockchain aplicado a IoT.

El sistema propuesto incluye capas de acceso que permite mantener fuera de la red a actores mal intencionados (como por ejemplo un dispositivo hackeado), es por eso que también se incluyen casos para remover dispositivos de la cadena de bloques.

4.6 Voto electrónico.

El costo de una elecciones es muy elevado, se tiene que crear papeletas, organizar toda la infraestructura necesaria para gestionar los voto y el posterior conteo de los mismos.

Aunque ya se han probados sistemas de voto electrónico, estas han sido incapaces de cubrir todas las vulnerabilidades de ataques de hackers y/o de asegurar un conteo preciso, cosas no menores cuando muchas veces de eso depende el futuro de un país.

La Blockchain puede ser una solución ya que permitiría un sistema de voto en el que las identidades de los votantes estuviesen protegidas, sean infalsificables y a un coste prácticamente nulo y de acceso público.

Convirtiendo los votos en transacciones podemos crear una cadena que lleve cuentas de los votos, de esta manera todos podemos estar de acuerdo en el conteo final porque podemos hacer las cuentas nosotros mismos y también verificar que ningún voto ha sido cambiado o removido y ningún voto ilegitimo ha sido agregado [16].

Los problemas de ciberseguridad podrían acabarse con el sistema criptográfico del blockchain, que permitirá sortear la suplantación de identidad de los votantes y mejorará la comodidad y la democratización del sistema electoral.

4.7 Gobierno transparente.

Haciendo uso de esta tecnología, cualquier institución gubernamental podría publicar como se encuentran sus cuentas en tiempo real. El gobierno solamente debería indicar cual es la dirección que ellos gestionan.

Desde ese momento todos los ciudadanos podríamos ver el estado de las cuentas, que es lo que se compra y lo que se vende, importaciones y exportaciones de todo lo que corresponde.

Si se diera el caso que un pago injustificable, o un monto exorbitante los auditores y la población entera lo vería al instante, lo que haría dudar a cualquiera con ganas de sacar algún provecho ilícito. Ademas de esto, la cadena de bloques sirve como un historial para ver como se ha manejado los fondos capitales en un gobierno determinado, para analizarlos y tomar mejores decisiones, y como ya conocemos es imposible cambiar datos de esta cadena e intentar falsear algunas cuentas del pasado.

4.8 Ecommerce.

Su uso en el comercio electrónico hará posible un intercambio mas directo de bienes y servicios, reduciendo los costos para las tiendas online, que ya no necesitaran la intermediación de un tercero. Blockchain posibilita que el flujo de productos y dinero esté disponibles para su control y comprobación, facilitando la facturación.

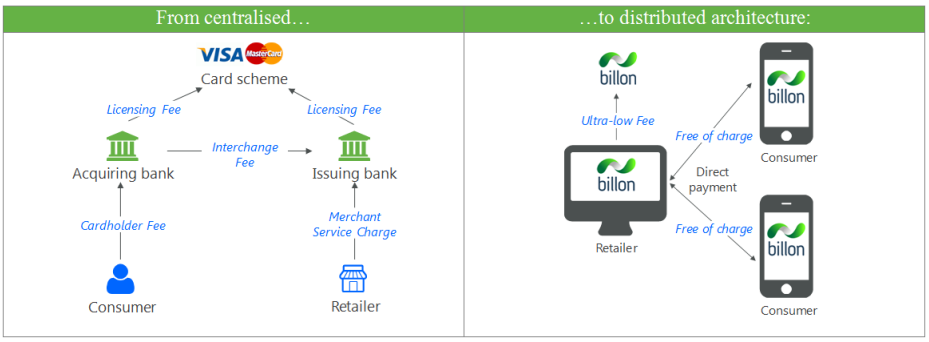
Billon, es una startup polaca[17], que presenta una *fintech*, que básicamente son tecnologías aplicadas al mundo de las finanzas, para realizar pagos fácilmente con costos muy bajos. Está diseñado para ser aceptado por las entidades financieras, y no hay necesidad de mineros ni terceros, es así que Billon ya ha sido aceptada por bancos de Polonia y esta incursionando al Reino Unido a modo de prueba.

La diferencia es que Billon utiliza tecnología blockchain propietaria y utiliza dinero real y no criptomonedas lo que facilita su adopción. También se tiene una integración total a la estructura bancaria existente permitiendo retiro de dinero desde las ATMs y puntos de pagos habilitados

El problema que trata de resolver es que las cuentas son costosas para los bancos, tan solo para abrir una cuenta los bancos les cuesta 100 euros y para mantener a un cliente otros 100 euros por año. Es así que muchas personas son perdida para estas entidades y no tienen acceso a los beneficios que estas pueden brindar

Billon trata de atacar esta problemática con proveyendo a los usuarios con una cuenta móvil, un servicio en el que es fácil de registrarnos obtenemos una cuenta corriente en nuestros smarthphones habilitandonos a realizar transferencias bancarias

Esta cuenta corriente móvil es una gran opción en el sector de método de pagos alternativos, es universal, que significa que cualquiera puede acceder a el -aun individuos sin cuentas bancarias, es simple y rápido. También es mucho



mas barato para las corporaciones y mercados, y virtualmente reemplaza a las tarjetas prepagas, gift cards, etc.

El concepto de Billon es simple, trata de reemplazar a los procedimientos de transacciones que son lentas y caras con pagos peer-to-peer rápidos y seguros

4.9 Identificación.

Es muy a menudo que nos encontramos en la siguiente situación: tenemos que llenar un formulario con nuestro nombre, email, tarjeta de crédito, numero de teléfono, contraseña y mas. Una alternativa es de conectarnos a través de Google + o Facebook como una forma fácil de identificarnos. Pero hay una razón por lo cual esto sucede, cuando uno no paga por el producto, es muy probable que uno mismo es el producto o mas bien los datos de uno. Pagamos por servicios gratuitos con nuestra privacidad e información, lo cual a mucha gente no le importa.

Pero existe una mejor manera, con blockchain es posible que cada uno posea su clave privada con sus datos y contenido. Seria algo así como nuestro pasaporte digital con el cual podemos acceder a productos y servicios como redes sociales, aplicaciones, e-commerces, en cualquier momento, manteniendo toda tu información contigo sin dificultades y al momento de darnos de baja de un servicio no dejar rastros [18].

Es tan solo así que los usuario podemos retomar el control de lo que nos pertenece y podemos avanzar hacia una Internet mas centrado y pensado en la privacidad y en el bien de los que la utilizamos.

4.10 Otras aplicaciones

- **Supply-chain:** Para conocer de donde provienen los productos. Con esta tecnología es posible identificar cualquier objeto con una huella digital única que seguirá todo su ciclo de vida desde el principio. Es por esta razón que resulta perfecta para su uso en la compleja cadena de suministro, algo que ya se ha probado para evitar la pesca ilegal, o Walmart, que se encuentra

en pruebas para asegurar la inocuidad de los alimentos. En la misma línea también está la gigante IBM, que está trabajando para resolver el problema de la última milla[19].

- **Entretenimiento**: Varios videojuegos y juegos de azar se han construido sobre una cadena de bloques o bien apoyándose en algún activo digital propio de ella. La velocidad, transparencia y, sobre todo, las recompensas, están aseguradas. Algunos ejemplos son: Spell of Genesis, un juego de cartas, Takara, una aplicación de realidad aumentada, y vDice, una plataforma de apuestas descentralizada que utiliza ethers.

- **Controles de dopaje**: En relación con el mundo deportivo, una de sus grandes dificultades es, sin duda, el dopaje. Para prevenir el mismo es necesario que los deportistas se sometan a controles periódicos, de cara a garantizar un deporte limpio.
  El uso del blockchain contribuiría a disponer de un historial completo e inmutable de los controles a los que se ha sometido un deportista.

- **Registros académicos**: Por medio de una de las características que ofrece la cadena de bloques, la seguridad, instituciones académicas podrían observar la disminución en los fraudes de obtención de títulos y se asegurarían de que los usuarios poseedores de diplomas u otro tipo de certificaciones académicas lo son de manera inequívoca. Se trataría pues de verificar la autenticidad de los certificados académicos mediante una rápida y sencilla consulta online, lo que supondría un importante avance, pues muchas veces no existe otra alternativa más que el contacto directo con la Universidad o su Secretaría para confirmar o no la validez de un título[20].

5 Conclusión

Claramente vivimos en una época donde la información equivale a dinero, el factor económico mas importante en la actualidad es el conocimiento, este nos da poder, así que necesitamos proteger la nuestra de la mejor manera. Son muy pocos los que realmente les damos la atención e importancia debida al cuidado y protección de nuestros datos, siendo que ya estamos bien adentrados en la era informática y somos conscientes de los peligros que existen. Blockchain nos provee una forma de darnos seguridad permitiendo que nuestros datos sean fragmentados y dispersados por toda una red de computadores, logrando así una redundancia real e impide la manipulación de esos datos.

Ademas de esto se están ideando y creando nuevas plataformas basadas en esta tecnología, servicios que son seguros y que buscan mejorar nuestra calidad de vida, tecnologías que se centran en las personas, y en donde estas personas son las que permiten que el sistema funcione. Se da así una relación simbiotica que permite que todos avancemos como una sociedad humana y tecnológica. En la era de la información las aplicaciones del blockchain son infinitas tan solo limitadas por nuestro ingenio y creatividad.

References

1. Consensys: Entendiendo la tecnologia blockchain (2016)
2. infotechnology.com: Que es blockchain la tecnologia que viene a revolucionar las finanzas (2016)
3. Vega, G., Bueno, O.L.: Blockchain: la tecnologia que va a cambiar tu vida (2017)
4. BitFuryGroup, Garzik, J.: Public versus private blockchains. - (2015)
5. da Silva, C.H.D.: Que es blockchain y como funciona? (2017)
6. blockchain.info: Blockchain size (2017)
7. Guggiari, J.: Blockchain: La tecnologia que descentraliza al mundo. Teoria y aplicacion de la Informatica 2 (2015)
8. Santibanez, F.: Todo lo que debes saber de las cadenas de bloques (2017)
9. IBM: What is blockchain (2017)
10. Economist, T.: Blockchains: The great chain of being sure about things (2016)
11. Raval, S.: Decentralized Applications: Harnessing Bitcoin's Blockchain Technology. O'Reilly Media, Inc (2016)
12. Boon, I.S.K.: Handbook of Digital Currency. Elvisier (2015)
13. DESJARDINS, J.: Comparing bitcoin, ethereum, and other cryptos (2017)
14. Herbert, Z.: Why blockchains are the future of cloud storage (2017) Sia Tech VP of Operations.
15. Compton, J.: How blockchain could revolutionize the internet of things (2017)
16. FollowMyVote: Blockchain technology in online voting (2017)
17. BillonTech: Billon technology overview (2017)
18. Tozzini, B.: Here is how blockchain could work as your identification (2017)
19. Cryptonoticias: Que es la tecnologia de contabilidad distribuida o blockchain (2017)
20. Finnopress: La revolucion del blockchain (2017)