Universidad del País Vasco Euskal Herriko Unibertsitatea
EKONOMIA ETA ENPRESA FAKULTATEA
FACULTAD DE ECONOMÍA Y EMPRESA

GRADO: ECONOMÍA

Curso 2020/2021

LA TECNOLOGÍA BLOCKCHAIN: SU IMPACTO EN DIFERENTES SECTORES ECONÓMICOS Y PROTOCOLOS DE CONSENSO

Autor/a: Gonzalo Hernández Chavarri

Director/a: Jose Manuel Zarzuelo Zarzosa

Bilbao, a 24 de junio de 2021

ÍNDICE

1. INTRODUCCIÓN

La tecnología Blockchain es un ejemplo más de cómo los avances tecnológicos están evolucionando y pueden cambiar la sociedad y la economía de manera nunca vista. Se trata de una tecnología capaz de ofrecer soluciones a problemas en campos tan diversos como pueden ser el financiero, el legal o el de la salud entre otros muchos. Los beneficios que aporta van orientados a reducir el tiempo de realización de transacciones, ofrecer una seguridad mucho mayor para el almacenamiento de datos o aumentar la transparencia en las transacciones.

Este trabajo tiene como objetivo principal recopilar y ofrecer la máxima información posible para poder explicar algunos de los usos que aporta esta nueva tecnología, sus ventajas e inconvenientes, y así ser capaces de entender de una manera clara y sencilla cómo puede beneficiar en muchos aspectos el uso de la tecnología Blockchain.

Con lo que sigue, pretendo describir los elementos básicos de esta tecnología, sus principales características, su funcionamiento, además de cómo sirve para eliminar los intermediarios que existen actualmente en la realización de transacciones, gracias a ser un sistema distribuido encargado de recoger las transacciones en bloques de manera ordenada y formando una cadena enlazados entre sí. Además de todo esto voy a describir el trabajo que realizan los mineros y me centraré en el uso que podría aportar esta tecnología en diferentes sectores. Por último, mencionaré algunos de los diferentes protocolos de consenso que se usan actualmente a la hora de confeccionar una blockchain.

La realización de este trabajo se ha centrado en ofrecer al lector una amplia visión acerca de este nuevo mundo tecnológico de la manera más completa posible, haciendo búsquedas exhaustivas de información en diferentes páginas web, así como en blogs o artículos científicos, tratando de dar respuesta a preguntas que solucionarían algunos de los problemas que tenemos actualmente. Está orientado a complementar los estudios realizados y la formación adquirida a lo largo del Grado de Economía, y entender cómo la tecnología Blockchain puede aportar soluciones a clientes, empresas, proveedores y al conjunto de la economía.

En cuanto a la estructura utilizada en la redacción del TFG, podría dividirse en 3 grandes bloques: en primer lugar, entender el funcionamiento de la tecnología

Blockchain, a continuación, sus posibles aplicaciones en diferentes sectores económicos y, por último, diferentes protocolos de consenso, pieza clave para el funcionamiento de la cadena de bloques.

La Blockchain tiene una gran capacidad de desarrollo y expansión gracias a su enorme potencial descubierto y todo el que queda aún por descubrir. Es una nueva tecnología que cambiará nuestra forma de optimización de recursos y ahorros de costes, además de favorecer ampliamente la cooperación entre distintos sectores. Quiere ser una posible solución contra casos de corrupción o fraudes comerciales, los problemas con las propiedades intelectuales, la gestión de documentación por las entidades públicas, etc...

Estamos hablando de una tecnología que va a crear una influencia en nuestras vidas de proporciones similares a las que protagonizó la aparición de internet, y que actualmente está ayudando y facilitando la aparición del nuevo internet del valor, sustentado en los principios de la tecnología Blockchain. El acuñamiento de este nuevo término deriva de la capacidad que ofrece la cadena de bloques para poder compartir diferentes tipos de valor de una manera digital y descentralizada, sin que exista la necesidad de confianza entre las diferentes partes involucradas, esta característica principal en las transacciones de hoy en día la suple una de las características de la cadena de bloques que mencionaré más adelante.

Por otro lado, ya podemos observar el nivel de impacto de esta nueva tecnología tan solo fijándonos en la cantidad de inversión que han realizado diferentes empresas punteras en el ámbito de la informática y tecnología como pueden ser Google, Amazon, Facebook, o diferentes dueños de grandes fortunas como puede ser Elon Musk, dueño de la conocida marca de coches Tesla.

Es un claro indicativo de que el futuro más cercano pasa por esta nueva tecnología, gracias a una de sus principales características como es la ausencia de una entidad central que supervise la realización de diferentes transacciones, dejando al individuo operar por sí solo y poseer de manera segura diferentes informaciones o reservas de valor. Además es una tecnología capaz de aportar diversas soluciones en numerosos sectores de la industria como voy a mencionar a lo largo del trabajo.

Por último, hay que subrayar el papel fundamental de esta nueva tecnología y que le otorga la generación de confianza en ella, a la vez que una gran seguridad en el sistema, estos son

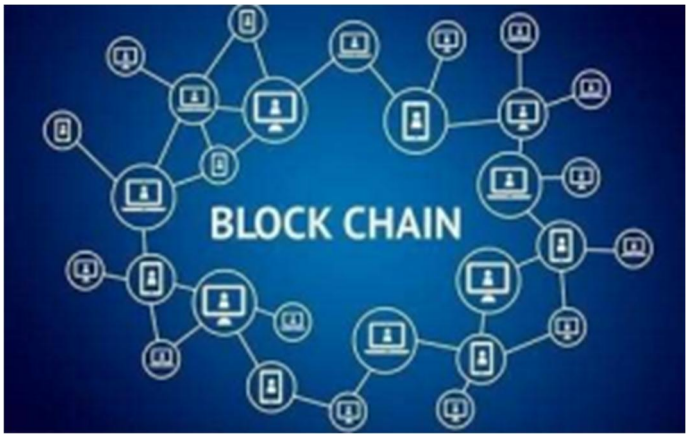
los diferentes protocolos de consenso en los cuales se fundamenta esta tecnología. Acabaré el trabajo hablando del Protocolo de Consenso de Nakamoto, usado en Bitcoin, la primera criptomoneda que empezó a usarse, y además mencionaré alguno de los más conocidos y fáciles de entender para los lectores.

Lo que deben tener en cuenta los lectores de este trabajo, es que esta nueva tecnología Blockchain es ya una realidad y la tenemos que tener muy presente para el desarrollo de cualquier novedad en diferentes sectores y en un panorama a nivel mundial, aunque nos tenemos que preguntar si esta tecnología ha venido para quedarse y modificar nuestro día a día o es algo pasajero en el tiempo.

2. ¿QUÉ ES LA TECNOLOGÍA BLOCKCHAIN?

Una sencilla definición de la tecnología blockchain sería [21]: es una gigantesca base de datos que se encuentra repartida entre numerosos participantes, está protegida mediante criptografía y está estructurada en una cadena de bloques relacionados entre sí encargados de recoger las diferentes transacciones de todos los usuarios de una misma red. Una cadena viene a ser un sistema descentralizado dónde se han eliminado intermediarios de las transacciones, haciendo que el usuario sea también gestor de toda la información formando una red con innumerables nodos.

Imagen 1: Nodos de la blockchain



Fuente: Pastor (2018)

Estamos hablando de un sistema mediante el cual los partícipes de una transacción no tienen por qué tener confianza una parte en la otra, sino que deberán seguir un consenso, aceptado por todos, sobre la evolución y el estado de los factores que se comparten. El consenso es precisamente la clave de la tecnología blockchain ya que este es el fundamento que permite que los participantes puedan confiar en la información de la red en la que se encuentran. Es entonces un sistema que principalmente se basa en la confianza, gracias a un consenso construido a partir de una red global de ordenadores que juntos gestionan una enorme base de datos.

2.1 Elementos básicos de la blockchain.

Como dice Preuskschat [24], para entender bien el alcance de la tecnología blockchain debemos tener en cuenta ciertos elementos básicos que conforman una cadena de bloques:

· Un nodo: es un ordenador personal. Dependiendo según el nivel de potencia, realizan más rápido las operaciones, pero independientemente de la capacidad de los ordenadores todos los nodos deben tener el mismo software o protocolo para poder comunicarse entre ellos, pues en otro caso no podrían conectarse a una red blockchain.

· Un protocolo estándar: lo encontramos en forma de software informático haciendo que una red de ordenadores (nodos) puedan establecer comunicación entre ellos. Consigue que los usuarios de una misma red puedan comunicarse bajo un estándar común.

· Una red entre pares o P2P (Peer-to-Peer): se trata de una red entre iguales, una red de ordenadores (nodos) que funcionan sin servidores fijos, de manera que todos se comporten como iguales.

· Un sistema descentralizado: todos los ordenadores conectados a la red, como son iguales entre ellos, controlan toda la información, es decir, no existe jerarquía, al menos en las blockchain públicas, en algunas privadas puede haberla, más adelante hablaré de ellas.

Podemos entonces resumir una cadena de bloques como un conjunto de ordenadores denominados "nodos" que, conectados en red, hacen uso de un mismo protocolo para comunicarse e interactuar entre ellos con el objetivo de validar y almacenar entre todos la misma información que se encuentra registrada en una red P2P.

2.2 Claves de la tecnología blockchain.

Hay tres claves de la tecnología Blockchain que combinadas entre sí e integradas, logran que se realice un propósito determinado y fundamental:

· La criptografía: se trata de un procedimiento algorítmico con una clave (clave de cifrado), que convierte un mensaje en cualquier lengua o con cualquier tipo de significado

en una cadena de símbolos, haciendo que este sea totalmente incomprensible para toda persona que no tenga la clave (clave de descifrado) del algoritmo que se ha utilizado. En una blockchain, esta criptografía es la responsable de proveer a los usuarios un mecanismo capaz de encriptar de forma segura las reglas del protocolo que rige el sistema, logrando que se evite de esta manera una posible manipulación, hurto o una introducción de información falsa dentro de una cadena de bloques. Además de toda esta protección la criptografía se encarga de generar firmas electrónicas e identidades digitales encriptadas.

· La cadena de bloques o blockchain: es la base de datos encargada de almacenar todos los registros y transacciones efectuados por los usuarios. Todas deben actuar bajo un mismo protocolo para poder dar validez a un bloque y así incorporarlo a la cadena de bloques. Es un proceso que se está realizando continuamente, haciendo que quede inalterada la información anteriormente registrada ya que, mediante la criptografía, los bloques quedan enlazados directamente una tras otro, evitando la necesidad de tener una entidad central que lo controle.

· El protocolo de consenso: es la parte imprescindible para todos los usuarios de la blockchain ya que este consenso se sustenta en un protocolo común que se encarga de verificar y confirmar las transacciones realizadas, asegurando una total irreversibilidad de las mismas. Proporciona así una copia inalterable y actualizada de las operaciones realizadas en la red blockchain a todos los usuarios.

2.3 Blockchain públicas VS Blockchain privadas.

Cuando nos referimos al término blockchain, este siempre tiene que ir acompañado de otra palabra, dependiendo de si estamos hablando de una blockchain pública o privada. Existen otro tipo denominado híbridas, pero no es común encontrarlas. De hecho, las primeras blockchain que se diseñaron fueron para ser:

- Públicas: cualquier persona sin ser usuario puede acceder a ellas y ser capaz de consultar las transacciones que recoge.
- Abiertas: cualquier persona, con unos mínimos conocimientos, puede ser usuario participando del protocolo común.
- Descentralizadas: ya que no existe ningún usuario capaz de actuar con más poder que el resto, debido a que todos los nodos son iguales entre sí.

- Pseudoanónimas: los usuarios que realizan las transacciones no son identificados personalmente. Lo que es de dominio público, siendo así rastreable, es la dirección desde la que se está actuando.

Podemos deducir de aquí entonces lo que sería una definición de una “blockchain pública”: es una red descentralizada de ordenadores los cuales hacen uso de un protocolo común que es asumido por todos los usuarios, y que les permite registrar las transacciones en la base de datos (blockchain). Estos registros son totalmente inalterables, pero sí que son visibles para todos los usuarios que se encargan de verificar las transacciones de forma independiente.

De manera alternativa han surgido las blockchain privadas cuyos usuarios argumentaron en su aparición razones como la imposibilidad de compartir de manera pública ciertos registros, por razones regulatorias o de confidencialidad de datos.

Las características fundamentales de estas “blockchain privadas” son las siguientes:

- Privadas: todos los datos que se encuentran en la red no tienen por qué ser de carácter público, siendo solamente partícipes de ellos los usuarios de la blockchain que podrían acceder y consultar las transacciones consultadas.
- Cerradas: la posibilidad de acceso es solo de los usuarios que son invitados a participar en estas blockchain, pudiendo existir en estos casos alguna limitación en el acceso a toda la información de la red.
- Distribuidas: en el sentido en que todos los nodos que participan en estas blockchain se conocen, por eso no suelen ser de excesivos nodos, lo cual puede afectar al nivel de seguridad, ya que cuantos más nodos más segura estará registrada la información.
- Anónimas: pueden tener el grado de anonimato que la blockchain establezca o en algunas ocasiones la que el usuario decida tener.

En las blockchain privadas los usuarios están sujetos a un protocolo que ya se encuentra predeterminado, y que les asigna un nivel de actuación dentro de la red en función de qué características posea el usuario, podríamos encontrarnos con un posible acercamiento hacia cierto nivel de centralización siendo posible la limitación del número de nodos por los promotores.

Podemos concluir esta diferenciación entre los dos grandes tipos de blockchain, privadas y públicas, añadiendo un último apunte acerca de la participación de nodos en ellas. Las blockchain privadas son distribuidas porque hay un número limitado de nodos, mientras

que las blockchain públicas son descentralizadas y no existe controlen el número de participantes.

En definitiva, una blockchain sería pública cuando está al alcance de cualquier usuario participar libremente en ella, mientras que sería privada cuando la participación en ella no está al alcance de cualquier usuario.

3. ¿CÓMO FUNCIONA UNA RED BLOCKCHAIN?

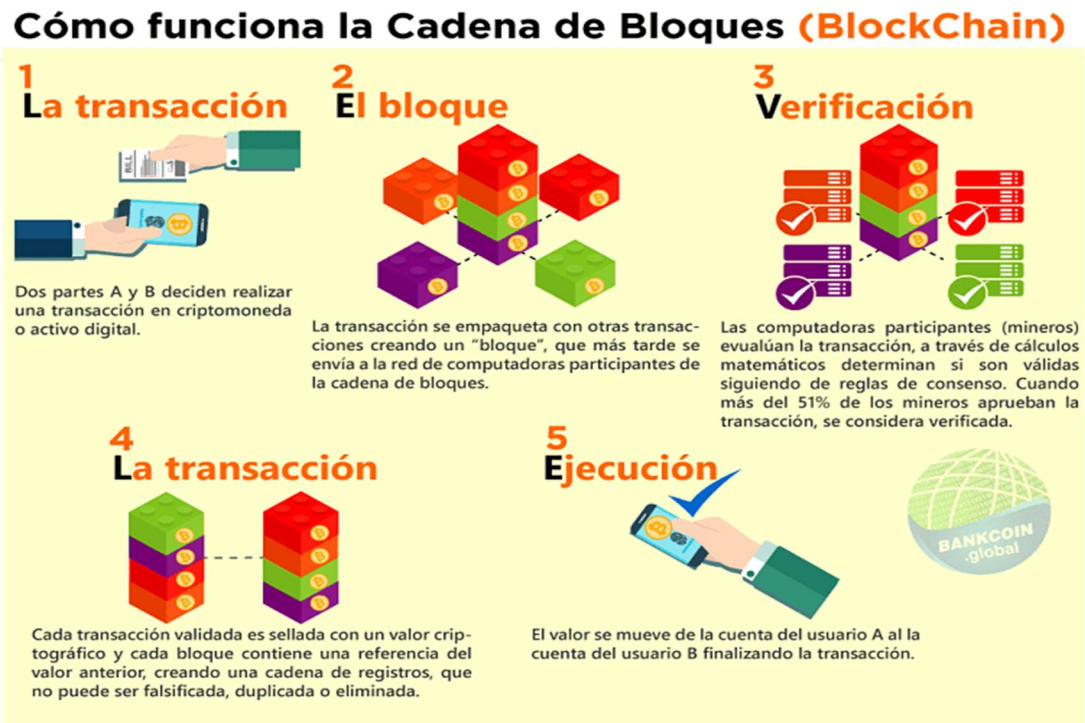
Antes de entrar en profundidad y tecnicismos, voy a explicar de manera rápida y sencilla el proceso y los pasos que seguiría una transacción en una red blockchain:

Supongamos que tenemos unos usuarios A y B, donde A quiere enviar dinero a B. Esta transacción del usuario A se registra junto a otras dentro de un mismo bloque que se transmite por toda la red a todos los usuarios de la misma blockchain.

De todos los usuarios, existen unos con tareas especiales, encargados de verificar las transacciones, haciendo que puedan registrarse dentro de un bloque, y posteriormente unirse a la cadena. Estos usuarios se llaman mineros (más adelante me centraré en las tareas que realizan y sus incentivos).

Tras realizar la tarea de verificación y encriptación de la transacción y el bloque, este se une a la cadena de bloques existente, proporcionando un registro inalterable y transparente acerca de todas las transacciones de los usuarios de una misma red blockchain. Es entonces, después de este proceso, cuando el dinero que deseaba enviar A a B se mueve de cartera.

Imagen 2: Cómo funciona una transacción en blockchain



Fuente: BankCoin (2017)

3.1 Bloques de una red blockchain

Este componente que aparece al realizar una transacción, como ya se había dicho, es redactado por unos usuarios especiales dentro de la red blockchain denominados "mineros", estos nodos especiales se encuentran distribuidos por todo el mundo.

Para entender un poco más cómo sería la estructura de un bloque la podemos dividir en tres apartados diferentes:

- Cabecera: recoge el "hash" del bloque anterior.
- Cuerpo: donde se redactan las transacciones que van a realizar los usuarios.
- Final: es la respuesta a una incógnita.

El término "hash" hace referencia a la firma digital de un contenido, como si fuera una huella dactilar, cuya tarea es conseguir que no se puedan alterar los datos dentro la blockchain, se usa en cada cabecera de cada bloque, respetando así el orden en las transacciones ya que se escribe en el inicio de un nuevo bloque, el "hash" del bloque anterior. Además del orden de los bloques, conseguimos de esta manera proteger la integridad de la cadena porque si quiero cambiar algún bloque existente, tendría que modificar todos los anteriores.

La "incógnita" la han de resolver los mineros para adjudicarse la creación de un bloque y es aquel valor que consigue, que al realizar el "hash" del bloque que se está creando se obtiene un valor de 256 bits que tiene que empezar con "x" cantidad de ceros. La cantidad de ceros depende del grado de dificultad de las transacciones y de la resolución del bloque, y es usado para controlar también la cantidad de bloques a realizar en un período de tiempo. En el caso de Bitcoin el tiempo de creación de cada bloque son 10 minutos, cada criptomoneda puede establecerlo en función de sus características.

En cuanto a la seguridad de los bloques hay que remarcar que de las 3 partes en las que se pueden dividir, no se puede modificar ni la cabecera, ya que contiene el "hash" del bloque anterior, ni las transacciones, ya que son las que los usuarios eligen realizar, por lo que solo nos quedaría el final, la incógnita, que es con lo que los mineros trabajan para adjudicarse así el bloque.

Cuando resuelven la incógnita, el bloque queda cerrado de manera criptográfica, tras la resolución del problema por un minero, y es en ese momento cuando la información

recogida por cada bloque es totalmente inalterable y haciendo que toda la cadena al completo tampoco pueda ser alterada.

3.2 Los mineros en una red blockchain

Los usuarios que son denominados “mineros” son aquellos nodos dentro de la blockchain encargados de verificar que las transacciones de los usuarios se pueden realizar, y que posteriormente, tras una serie de operaciones, se encargan de sellar el bloque y añadirlo a la cadena.

Tras verificar las transacciones, y una vez llenado el bloque con “x” número de transacciones, cada criptomoneda establece una cantidad de transacciones dentro de cada bloque, la siguiente tarea que tienen que desempeñar es lograr ser el primero en obtener una solución a un problema criptográfico asociado con cada bloque y recibir los incentivos económicos que estos tienen.

La resolución de la incógnita no tiene ninguna fórmula capaz de simplificarles la tarea a los mineros, sino que solo se puede resolver de la manera tradicional denominada, “ensayo y error”, es decir, realizar pruebas con diferentes valores hasta lograr el resultado.

El objetivo de estos mineros es realizar la mayor cantidad de operaciones posibles por segundo, como estamos hablando de un método de prueba en el que participan miles de nodos, es muy difícil que más de uno lo resuelva a la vez, por lo que es imposible que más de un minero realice un mismo bloque, consiguiendo así que no haya duplicidad de bloques y pudiendo saber qué minero ha sido el que ha conseguido resolver la incógnita. Cuando un minero resuelve la incógnita, el resto de los mineros comprueban que la incógnita resuelve el problema, lo verifican y es entonces cuando el minero sella el bloque, se adjudica su escritura y obtiene una recompensa.

El trabajo de los mineros es costoso económicamente ya que si quieren optar a ser el primero en resolver las incógnitas necesitan ordenadores potentes y realizar un alto consumo eléctrico, además de tener que competir con miles de nodos, con sus respectivos ordenadores, para lograr la resolución de la incógnita.

Debido a este laborioso y costoso trabajo, estos usuarios tienen unos incentivos para competir por ser los primeros, son incentivos puramente económicos ya que al primer minero que resuelve la incógnita se le recompensa con la moneda virtual que esté

trabajando.

En el caso de Bitcoin se le otorgan 6,25 Bitcoins al minero que la resuelve, a 01/12/2020 el cambio se encuentra en 1 Bitcoin más o menos es 15.000 €, por lo que estaríamos hablando de un incentivo económico cercano a los 100.000€ por incógnita resuelta, es decir, por bloque sellado. Esta transacción la redactan en el cuerpo del bloque, anotándola como una transacción del sistema a el minero por dicha cantidad.

4. IMPACTO DE LA TECNOLOGÍA BLOCKCHAIN EN DIFERENTES SECTORES ECONÓMICOS

Hay numerosas industrias que se encuentran en la carrera por explorar el potencial de esta nueva tecnología denominada blockchain, el sector financiero va en cabeza ya que fue el primero en tomar la iniciativa de profundizar en este tema, pero cada vez se está expandiendo a más sectores. Por ejemplo:

4.1 El sector financiero

El sector financiero desde hace casi 15 años está experimentando verdaderas dificultades para conseguir recuperar los niveles de rentabilidad que había adquirido antes de la crisis del 2007, y por eso fué el primero en tomar la iniciativa en intentar reinventarse realizando grandes procesos de inversión en esta nueva tecnología [9]. De los dos grandes tipos de blockchain que existen, públicas y privadas, encuentran más factibles para sus intereses financieros que éstas sean privadas.

En la década de los noventa se empezó a pensar que tal vez podría crearse un sistema financiero abierto, dando uso a todo el potencial que aportaba la aparición del Internet de la información, haciendo desaparecer a los organismos centrales que controlan las transferencias y además garantizando el anonimato de sus participantes y con una total transparencia de las transacciones. El resultado de todo este trabajo y estudio llegó a finales del 2008 cuando se creó la primera moneda virtual que se llamó “Bitcoin”.

Esta aparición provocó que se desarrollara un enorme movimiento hacia el pensamiento de descentralizar ciertas operaciones diarias como podían llegar a ser los pagos, las transferencias internacionales o las remesas. Lo más importante fue comprobar que no había necesidad de contar con un organismo central que aporte confianza y se encargue de la supervisión de las transacciones que tradicionalmente realizaba la “banca”.

Hay numerosos motivos por los que la banca se encuentra en un proceso de transformación y adaptación a la posible aparición de nuevos modelos financieros [16]. Además, estamos hablando de cambios no solo tecnológicos sino también regulatorios y culturales ya que actualmente los hábitos de vida y de consumo de servicios difieren mucho de los que existían cuando apareció este sector, se busca no solo la venta de servicios de la banca sino el acompañamiento diario al consumidor en sus necesidades.

Imagen 3: Banca y blockchain

Fuente: Bitcoin.es

A día de hoy la banca está regulada básicamente por dos iniciativas legales, bastante recientes y que se encargan de orientar de manera diferente la relación entre entidad y cliente: MiFID II (Markets in Financial Instruments Directive II) y PSD2 (Directive on Payments Services 2).

A grandes rasgos la primera iniciativa tiene como objetivo fundamental la protección al consumidor, mientras que la segunda persigue la creación de oferta para dicho consumidor, incrementando así la competencia entre las entidades.

Para la banca, al hacer uso de la tecnología Blockchain le haría aumentar el crecimiento del negocio ya que les permitiría desarrollar un mayor nivel de transparencia y podría ofrecerles posibles aperturas a otros modelos de negocio, creando un nuevo sistema de operabilidad entre diferentes entidades. Esta tecnología permite desarrollar otros objetivos básicos para el sector como son la confianza, la propiedad, la identidad, los activos y los contratos, mediante unos pagos, transacciones, procesos e información en tiempo real, y todo realizado con total transparencia.

La velocidad en la realización de las transacciones con la blockchain es uno de los puntos a favor que ésta posee, por ejemplo, la realización de una transferencia internacional a través del sistema bancario tradicional podría tardar días, mientras que con esta tecnología solo se demoraría unas horas. Por otro lado, la principal limitación observada a día de hoy hacía las blockchain existentes es la necesidad de emplear criptomonedas para transmitir el valor. Si que es verdad que podría ser beneficioso para ciertos países en los que hay una débil estructura financiera, fuertes controles sobre el capital y la inflación, o en países donde la población no pueda disponer de una cuenta bancaria. En estos casos el uso de criptomonedas puede ayudar a los usuarios ya que les aporta seguridad, facilidad de uso y control.

En la actualidad ya existen entidades financieras que están realizando procesos de inversión en la tecnología blockchain para poder adaptarse a este nuevo modelo de interacción entre la banca y el cliente, buscando disminuir la cantidad de participantes involucrados en las transacciones y sobre todo el aumento de la transparencia, con el principal objetivo puesto en la reducción de costes y el aumento de la eficiencia.

4.2 El sector sanitario y farmacéutico

El éxito que está teniendo está aparición para muchas industrias no ha dejado indiferente al sector de la salud que también está iniciando un proceso de acercamiento hacia esta nueva tecnología, aunque sí que se prevé que sea un sector al que le cueste más tiempo adaptarse a este cambio [17].

Cuando hacemos referencia a la atención sanitaria, la información clínica de los pacientes suele encontrarse distribuida en diferentes sistemas, e incluso en ocasiones puedo no llegar a aparecer cuando más se necesita. Esta nueva tecnología podría realizar una transformación en la forma de acceder a los datos de los pacientes, podríamos llegar a ser capaces de compartir, actualizar y sincronizarlos a diferentes niveles, local, autonómico, estatal, europeo o internacional, además con mucha seguridad, de forma inmediata y con privacidad.

No va a ser posible corromper o manipular ningún tipo de información debido a la ausencia de un administrador central que es eliminado gracias a la intervención de la

criptografía. Asimismo, se proporcionará acceso y control a todos los usuarios de la blockchain a cerca de su historial médico, pero siempre de manera segura sabiendo que tratamos con temas confidenciales de un paciente.

Las administraciones sanitarias e industrias farmacéuticas están observando los grandes retos que supone la aparición de la blockchain, pero sobre todo las grandes soluciones que puede llegar a aportar [30]. Hay esperanza de que la seguridad que aporta esta tecnología se pueda extender a la cadena de suministros de medicamentos y sobre todo al intercambio de información centrándose en cuatro aspectos:

- La historia clínica del paciente.
- La información obtenida de la realización de ensayos clínicos.
- Los datos relativos al genoma humano.

· Los servicios de reclamación y pago de servicios sanitarios asegurados.

Para aprovechar todo el potencial de la blockchain, en este sector en particular, va a ser necesaria la colaboración entre las diferentes entidades y actores que participan en él, y que además tendrán intereses y necesidades que se podrán complementar.

Los objetivos principales en los que se centrará la evolución del sector sanitario serán: el aumento de la eficiencia administrativa y con una importante reducción de costes; desarrollar la capacidad de explorar en un mercado mucho más amplio la fabricación de medicamentos, ensayos clínicos... Y añadiendo a estos el desarrollo de soluciones complementarias que potencia la blockchain como la confianza en la realización de las transacciones, la identidad de los usuarios y la integridad de todos los datos.

4.3 Las aseguradoras

La aparición de la blockchain está provocando también un gran cambio en la industria de los seguros ya que permite una nueva dinámica de negocio donde todos los participantes de una cadena valor van a ser capaces de intercambiar información de manera segura y rápida a través de una infraestructura nueva, descentralizada, abierta, verídica y flexible [10]. El gran potencial que han observado las empresas aseguradoras se centra en los contratos inteligentes (Smart Contracts, ver sección 5) que son capaces de conseguir que lo estipulado en ese contrato se pueda autoejecutar en base a unos parámetros prefijados, es decir, el asegurado recibiría la indemnización contratada de manera directa sin la necesidad de iniciar una reclamación.

Gracias a esta tecnología la satisfacción del cliente por la solución recibida incrementará en comparación a la actual, al igual que la confianza hacia las compañías aseguradoras. Además de mejorar la relación con el asegurado, el uso de la blockchain va a ofrecer nuevos modelos de negocio gracias a la reducción de los costes y los procedimientos, incluyendo la capacidad de pagar en cualquier tipo de divisa válida dentro de una plataforma, dando facilidades a los consumidores cuyas monedas estén muy devaluadas o con una gran inflación.

Uno de los primeros pasos que se han dado ha sido la creación de un consorcio entre cinco compañías de seguros [23], Aegon, Allianz, Munich Re, Swiss Re y Zurich, cuyo número de integrantes ha aumentado considerablemente a nivel internacional y actualmente denominado Blockchain Insurance Industry Initiative-B3i, una plataforma

en común con el objetivo de proporcionar facilidades para el uso de la tecnología blockchain haciendo que mejore la eficiencia en toda la cadena de valor del sector asegurador [26].

Estas soluciones beneficiarán a todos los actores que participen en la cadena ya que se va a disponer de una red virtual que permitirá la interoperabilidad entre ellos de manera directa, reduciendo los costes y agilizando la gestión. Otro aspecto importante es la seguridad, aumenta en gran medida con esta tecnología que se encarga de asignar a cada contrato dentro de la red un código privado además de redactarlo totalmente encriptado con algoritmos seguros y almacenarlo en una cadena de bloques inalterable, dificultando la posibilidad de alterar los acuerdos de manera fraudulenta.

En conclusión, la aparición de blockchain puede aportar soluciones a muchos de los problemas que podemos observar a día de hoy en el sector de los seguros, los más factibles y que ya se están implementando se encuentra orientados a tres objetivos principalmente: la gestión del propio contrato a través de los Smart Contracts, reduciendo el tiempo de ejecución de la póliza ante un imprevisto de un cliente; la prevención y detección de fraude orientada a indemnizaciones ilícitas que se realizan falseando información; y por último, el flujo de información entre todos los actores que participan en este sector, y entre las diferentes entidades, siendo capaces de compartir a través de esta tecnología información de clientes evitando así la redundancia en ciertas fases del proceso.

4.4 La Industria 4.0

El concepto de Industria 4.0 se utiliza para hacer referencia a ciertos términos como: Cuarta Revolución Industrial, Ciberindustrias, Industrias Inteligentes… Puede parecer lejano, pero ya se está implementando y se centra en una idea clara que consiste en lograr la interconexión de todas las partes de una empresa, induciendo hacia una automatización efectiva y unas empresas más inteligentes. Es decir, se está buscando conseguir una adaptación lo más perfecta posible de la empresa, a los recursos y medios de producción de los que dispone para aprovecharlos al máximo. Las características que más se pueden destacar de esta revolución son: la automatización, la conectividad, la información digital y el acceso al cliente en menos tiempo.

Éstas cuatro novedades que se presentan en el mundo industrial pueden generar numerosas ventajas, partiendo de una mayor eficiencia, la cual va a lograr a su vez numerosas reacciones en cadena [11]. Si se consigue disponer de una industria

automatizada se puede precisar más en medidas, pesos, condiciones específicas… optimizando de esta manera los niveles de calidad ofertados por las empresas, y además con una reducción muy considerable en sus costes y sus tiempos de producción. Esto desembocaría en un aumento de la competitividad empresarial generando una mejor respuesta a las necesidades del mercado y, por otro lado, si tenemos en cuenta la eficiencia en el uso de recursos, vamos a poder centrarnos en otra tarea muy importante como es un mejor cuidado del medioambiente.

Al igual que se pueden vislumbrar futuras y más que posibles ventajas con la aparición de la Industria 4.0, también se contemplan una serie de desventajas que pueden acabar derivando de ésta. Existen riesgos como por ejemplo que ciertas empresas se queden desactualizadas, ya que la tecnología está en continuo desarrollo, provocando de esta manera la necesidad de personal especializado y del cual puede haber ausencia en el mercado laboral debido a su modernidad [15]. A su vez estamos hablando de la necesidad de un gran volumen de inversión inicial que muchas empresas no pueden permitirse, y esto desencadenaría la mayor desventaja posible, la adaptación de tan solo una parte de las empresas y no de todas o la gran mayoría.

Otro gran inconveniente, que se está empezando a solucionar gracias a la blockchain, es la gran dependencia que esta revolución genera hacia la tecnología, cualquier problema que surge se debe solucionar de manera inmediata para no perjudicar ni ralentizar el proceso, y siempre hay que tenerla actualizada.

Imagen 4: Industria 4.0

Fuente: Mecalux.es

La blockchain puede aportar una buena solución a problemas relacionados con la identidad de los dispositivos y su fiabilidad, la descentralización de las cadenas de bloques es una fortaleza para ayudar con este problema, ya que sería posible verificarla identidad de los

dispositivos que vayan a participar sin depender de una autoridad central. Todas las actividades quedan registradas en una base de datos disponible para los usuarios que necesiten contrastar información, reduciendo la incertidumbre y la posible falta de control, y garantizando una total integridad de la información.

Por otro lado, podemos vislumbrar que en las fábricas inteligentes que se irán desarrollándose van a estar compuestas de numerosos dispositivos diseñados para la fabricación y tendrán que ir conectados entre sí de manera que sean capaces de funcionar por sí solos y entre ellos [29]. Es aquí donde gracias a la blockchain aparecerá una nueva economía en la que los propios dispositivos se conectarán entre ellos (Machine to Machine, M2M) y serán capaces de llegar a acuerdos que quedarán reflejados en los Smart Contracts sin ningún tipo de intermediación, reduciendo así la necesidad de terceros en las transacciones.

La automatización de todos estos procesos sólo se podría realizar gracias a la aparición de blockchain ya que funciona como interconexión entre todos los dispositivos que se encuentren en ella, reduciendo todos los procesos y los costes, que actualmente son los que provocan que el precio de numerosos lotes sea mayor que el propio coste de su producción.

4.5 Los medios de comunicación.

Hoy en día estamos rodeados por un clima de desinformación, las “fake news” y una crisis en el sector del periodismo que ha desencadenado, como en muchos otros sectores, la desaparición de puestos de trabajo y un importante aumento de la desconfianza de gran parte de la población. Una de las posibles soluciones que se están planteando para acabar con esta situación, es el uso de la tecnología Blockchain, pues se está observando que puede ofrecer nuevas oportunidades en materia de calidad en este sector, y cada vez está siendo más utilizada ([4], [5]).

Desde principios del siglo XXI el periodismo está afrontando una serie de dificultad es que le están obligando a cambiar los modelos de negocio tradicionales que llevaban a cabo los medios de comunicación, sobre todo en el sector del papel. Se está intentando conseguir dos objetivos principalmente: conseguir recuperar la confianza de los clientes a través de informaciones verídicas, y como consecuencia, revertir el descenso en las cifras de negocio que ha sufrido durante los últimos años.

La tecnología blockchain puede ser una herramienta para lograr los objetivos mencionados

ya que las principales propiedades de esta tecnología son la seguridad, gracias a la criptografía, y la veracidad de los datos que se hayan escritos en ella, estos se quedan guardados de tal forma que no pueden ser manipulados, potenciando entre otras cosas la adjudicación de la autoría de muchos de los trabajos realizados ya sean entrevistas, informes, fotografías, videos…

Según una serie de estudios realizados algunas de las áreas en las que puede solucionar sus problemas la cadena de bloques en el sector del periodismo son: hacer frente a las "fake news" y disminuir la desinformación, salvaguardar la propiedad intelectual y fomentar la creación de contenidos por parte de los usuarios. Además de todo esto hay que seguir teniendo en cuenta que las entidades centrales no podrán alterar la información, ya que se encuentra distribuida por toda la red de usuarios, y esta podría usarse a su vez para incentivaría la economía de este sector al poder realizar transacciones con videos, noticias, fotos, suscripciones… gracias a esta nueva tecnología.

Encontramos modelos de negocio en los que se conecta directamente periodistas con medios de comunicación y consumidores, se les permiten crear sus propias reglas de uso para cada producto periodístico, así cualquier periodista podrá programar con Smart Contracts las condiciones concretas en las que quiere que se consuma su contenido [27]. Cabe añadir que, gracias a la estructura de cadena, se podrá controlar el ciclo de vida de las publicaciones y remunerar al periodista en función de ello, además de gestionar con facilidad los derechos de autor.

En conclusión, la aparición de esta nueva tecnología está empezando a mostrar nuevas maneras de rentabilizar el sector del periodismo y los medios de comunicación. Pretende aportar un componente muy importante para el funcionamiento de estos que es generar un aumento más que probable de la confianza de los usuarios en los diferentes medios, gracias a las propiedades de la cadena de bloques y su capacidad para gestionar y verificar la información que en ella se recoge gracias a la distribución de los datos a lo largo de toda la red de participantes. Además de fomentar y ayudar al desarrollo del periodismo a pequeña escala ofreciendo facilidades para el desarrollo del sector de manera individual sin tener la dependencia actual de un medio de comunicación para el que trabajar.

4.6 El sector público.

La aparición de las nuevas tecnologías de la información está provocando grandes cambios en la manera en la que vivimos y trabajamos, pero no solo nosotros, también las administraciones públicas están enfrentándose a grandes retos que provocan estas tecnologías, pero a su vez observan la capacidad que tienen de aportar posibles soluciones a los problemas que pueden presentar en la actualidad.

El sector público se encarga de tareas como la implementación de políticas, la recaudación de impuestos, la protección de los ciudadanos… y todo esto exigido siempre con gran transparencia, agilidad y haciendo partícipes a los ciudadanos [6]. Internet ha ayudado en muchas facetas a aumentar la eficiencia del sector automatizando muchos de los procesos que anteriormente eran muy costosos o tardíos a la hora de realizarse. Pero no se ha acabado de avanzar en materia de confianza y seguridad en el almacenamiento de la información, se sigue estando expuesto a posibles ataques para manipular los datos tanto de agentes externos como internos.

Hoy en día la adaptación de la Administración Pública a estas nuevas tecnologías se ha orientado básicamente en dos vertientes, una interna, con el objetivo de hacer desaparecer el papel y transformar los procesos en electrónicos, y otra externa, a través de la habilitación de plataformas electrónicas para la comunicación con la ciudadanía.

Es ahora cuando se pretende avanzar también en el ámbito de la seguridad y confianza, orientando así la visión de futuro hacia la blockchain o cadena de bloques, una de las tecnologías más disruptivas desde la aparición de Internet. Podemos mencionar los principales motivos por los que esta tecnología es tan atractiva también para las Administraciones Públicas.

En primer lugar, una característica fundamental es la confianza que genera la información que se encuentra en una blockchain independientemente del tamaño y lo heterogénea que sea. En segundo lugar, la cadena de bloques deja un rastro de todas las transacciones que se realizan, permitiendo al usuario conocer cuando y quien ha realizado una operación contribuyendo de esta manera a un gran nivel de transparencia. Y, en tercer lugar, la ausencia de una autoridad central que supervise y gestione los accesos a esta información.

Hoy en día muchas agencias gubernamentales tienen la vista puesta en esta nueva tecnología que posee un gran potencial para ayudarnos a mejorar en muchos aspectos y

conseguir recuperar la confianza en los gobiernos y el Sector Público, aunque no es la solución a todos los problemas, y por ello el desarrollo de la cadena de bloques tiene que ir orientada a aplicaciones pertinentes, a continuación, menciono las más relevantes según Magdalena [6]:

· Registro de títulos o activos: actualmente ya se han iniciado procesos piloto en Suecia y Reino Unido utilizando blockchain, ya que registrar un título o activo es una de las funciones básicas de la cadena de bloques.

· Salud: hoy en día en muchos lugares acceder a los ficheros médicos personales es muy complicado ya que se encuentran distribuidos y almacenados en las bases de datos de los hospitales, y se comparten de manera manual. En países como Estonia o Suecia se está haciendo uso de la blockchain de manera complementaria para garantizar una correcta manipulación de los datos y asegurar que estos son verídicos, aunque se encuentren almacenados fuera de la cadena de bloques.

· El voto electrónico: conseguir este avance sería un gran paso para aumentar la democracia participativa, que la ciudadanía pueda votar desde sus casas a través de las nuevas tecnologías, son objetivos marcados en el corto plazo por los gobiernos, pero para que esto sea eficaz, la principal herramienta tiene que ser la confianza. Blockchain puede aportar soluciones a este principal objetivo contribuyendo con su transparencia, fiabilidad y su confidencialidad, asegurándose además un único recuento de los votos. Actualmente ya se han iniciado iniciativas en Suiza, Estonia o Australia, pero para que funcione de verdad el acceso a este tipo de plataformas debe ser universal.

· Seguimiento y regulación de mercados: el Gobierno de cada país realiza una gran labor para proteger a sus ciudadanos y garantizar la legalidad y viabilidad de los mercados que participan en él, pero esta información se obtiene a través de controles o autodeclaraciones. Los primeros son muy costosos y no se pueden realizar diariamente, y los segundos depende de la sinceridad que muestre cada mercado. Es entonces cuando se observa la posible ventaja que puede aportar blockchain a estos problemas, la capacidad de tener los datos de manera distribuida facilitaría la gestión y control por parte de las administraciones centrales, y a su vez se automatizarían muchas cadenas de producción y suministro quedando registrados todos los datos. Generaría un aumento en la confianza hacia las administraciones centrales siempre y cuando se realice desde la transparencia y con la mayoría de los mercados involucrados en estas nuevas tecnologías.

Se puede vislumbrar el gran potencial que posee esta nueva tecnología, la cadena de bloques, además de los numerosos usos que ésta puede dar en muchos ámbitos, y no menos en el Sector Público. Una tecnología capaz de hacer aumentar la confianza de la ciudadanía puede ser la clave en un futuro de las Administraciones Públicas, así como su aumento en la transparencia y la democracia participativa, todo esto siempre con la gran seguridad que aporta la Blockchain. Aunque no podemos dejar de lado que no todo son elementos positivos en la actualidad, ya que se carece de un marco regulatorio general, por lo menos a nivel europeo, que proteja el uso de esta tecnología, y la situación forzada que pueden llegar a crear los individuos que insisten en que esta tecnología es el futuro, obviando la posible aparición de nuevos modelos tecnológicos que puedan mejorar las propiedades de blockchain.

5. SMART CONTRACTS

La aparición de la blockchain ha generado el resurgir de un término, que había aparecido anteriormente, a finales del siglo XX, pero que carecía de los requisitos necesarios, que aportaría poco tiempo después en 2009 la cadena de bloques, para realizar correctamente sus funciones.

Teniendo previamente en mente la definición de contrato, es decir, un acuerdo entre dos partes que se comprometen recíprocamente a respetar y cumplir una serie de condiciones; podemos definir los "Smart Contracts" o "Contratos Inteligentes" como unos programas informáticos que hacen cumplir de manera automatizada los requisitos que se establecerían en un contrato, es decir, bajo unos parámetros establecidos, dos partes aceptan un acuerdo, y en el momento en que entre en acción una de las partes, el contrato se ejecuta inmediatamente siguiendo las órdenes preestablecidas ([3], [12]).

Imagen 5: Smart Contracts

Fuente:Cysae.com

El uso de este nuevo tipo de mecanismo supone la eliminación de intermediarios con el objetivo de simplificar procesos, y, por lo tanto, ahorrar en costes al consumidor. Generalmente se trata de un programa de ordenador cuya tarea fundamental es controlar directamente la transferencia de monedas o activos digitales entre dos partes, pero los Smart Contracts además de encargarse de definir las reglas relacionadas con un acuerdo, al igual que un contrato tradicional, es capaz de conseguir que se cumplan automáticamente esas obligaciones ejecutando las acciones requeridas por esas cláusulas y almacenándolas en la blockchain para que queden registradas.

Las posibilidades de estos contratos inteligentes van más allá de una transferencia de

activos, pueden realizar transacciones en una gran variedad de campos, procesos legales y financieros, primas de seguros... Las principales ventajas que podemos obtener del uso de esta nueva tecnología se pueden dividir en estos cuatro aspectos:

· Reducción de costes: este nuevo mecanismo de contrato va a eliminar muchos gastos operativos y así ahorrar en recursos para monitorizar el proceso.

· Mayor velocidad de los procesos: estos contratos inteligentes se ejecutan de manera automatizada, aumentando directamente la velocidad en la que se ejecutan las transacciones comerciales que se estipulan en dichos contratos.

· Autonomía: la red realiza automáticamente los Smart Contracts eliminando la necesidad y el posible riesgo que supone involucrar a un tercero en ellos.

· Fiabilidad y precisión: cuando se ingresan los datos en la cadena de bloques, no se pueden cambiar ni eliminar, por lo que, si una de las partes no cumple con sus obligaciones, la contraria estará protegida por las condiciones del contrato que se ejecutará.

En cuanto a las posibles desventajas o dificultades que puede presentar esta novedosa tecnología, podemos destacar ciertos aspectos relacionados fundamentalmente con la falta de regulación existente a nivel internacional actualmente, lo cual produce un prejuicio sobre muchos individuos a la hora de adentrarse en el mundo de estas nuevas tecnologías desarrolladas gracias a la blockchain.

6. PROTOCOLOS DE CONSENSO

Dentro de los sistemas distribuidos que son aquellos en los que la información se encuentra repartida entre los diferentes participantes de una red [1], los consensos que son tolerantes a la existencia de componentes defectuosos se han estudiado en profundidad, ya hay algoritmos de consenso capaces de superar los fallos que pueden aparecen en el sistema, garantizando que todos los componentes estén de acuerdo en unos valores comunes y den la misma respuesta ante determinada solicitud de servicio, aun existiendo en el sistema componentes defectuosos y fuentes de información poco fiables.

Un consenso significa que estos individuos llegan a un acuerdo sobre ciertos componentes. En realidad, los individuos que componen un sistema distribuido y los canales por los que transmiten su información, tienen facilidad de incurrir en fallos impredecibles y reciben a su vez diferentes estímulos en forma de influencias. Hay tres principales factores en un consenso de un sistema distribuido [35]:

· Sincronía en la red: es un concepto básico en un sistema distribuido y se encarga de definir el grado de coordinación que poseen los componentes de un sistema. Es necesaria la existencia de esta característica antes del desarrollo de cualquier protocolo. Hay tres niveles de sincronía: “Sincrónico” (todos los individuos realizan las operaciones de manera coordinada), “Asincrónico” (las operaciones de los individuos no se encuentran nada coordinadas) o “Parcialmente asincrónico” (las operaciones se coordinan entre todos los individuos, aunque no a la vez).

Generalmente en la mayoría de las aplicaciones se asume que son sistemas sincrónicos o parcialmente. La red Bitcoin en particular se trata de un sistema parcialmente sincrónico.

· Componentes defectuosos: se dice que un componente es defectuoso si sufre un fallo que lo detiene de su funcionamiento normal. Existen dos tipos de fallos, los fallos de los componentes, donde los individuos pueden detectar el fallo y solucionarlo; y, por otro lado, el fallo bizantino, donde el individuo puede actuar arbitrariamente mandando mensajes contradictorios al resto de los componentes para que no exista el consenso, ésta última es considerada el peor fallo existente.

· Protocolo de consenso: define el conjunto de reglas para el paso y procesamiento de los mensajes con el objetivo de que todos los componentes de una red lleguen a un acuerdo

sobre un tema común. Una regla de paso regula la transmisión y retransmisión de mensajes, mientras que una regla de procesamiento se encarga de definir como un componente cambia su comportamiento tras recibir mensajes. El consenso se alcanza si todos los componentes “no defectuosos” coinciden en el mismo resultado. El nivel de seguridad que alcanza un protocolo de consenso se mide generalmente por el número de componentes defectuosos que puede tolerar. Si un protocolo puede aceptar al menos un fallo por componente defectuoso, lo llamamos tolerante a fallos de componentes defectuosos (Crash-fault tolerant CFT), y, por el contrario, si un protocolo de consenso puede tolerar al menos un fallo bizantino, lo llamaremos tolerante a fallos bizantinos (Byzantine-fault tolerant BFT).

Tras una breve explicación introductoria acerca de los consensos en sistemas distribuidos, como es la blockchain, y sus tres principales factores, me centraré en explicar el primer consenso que se puso en práctica, el de Bitcoin, conocido como el consenso de Nakamoto y posteriormente mencionaré algunos de los más usados actualmente.

6.1 El consenso de Nakamoto

Entre los muchos aspectos a destacar de Bitcoin, el consenso de Nakamoto es la creación, sin ninguna duda, clave si queremos referirnos a temas como la seguridad o el rendimiento. Para la red blockchain el objetivo del consenso es recoger una copia completa del historial de transacciones realizadas, y todo esto en orden cronológico. Pero hay que tener en cuenta también una serie de inconvenientes a los que se enfrentan los protocolos de consenso en este tipo de redes distribuidas, como, por ejemplo, la conectividad a la red, el tamaño de esta, y el nivel de influencia que puede existir por parte de los adversarios.

El objetivo del consenso desarrollado por Nakamoto es conseguir que todos los nodos adopten una sola visión unificada de las transacciones realizadas en la red Bitcoin. A continuación, las cuatro características que deben cumplir en el consenso de Nakamoto:

· Finalidad (Probabilística): cada vez que un bloque se va añadiendo a la cadena de bloques, la probabilidad de que ese bloque sea revocado va disminuyendo asintomáticamente a cero.

· Acuerdo: cada bloque tiene que ser aceptado o descartado por todos los nodos honestos. Una vez es aceptado debe quedar registrado con el mismo número de

bloque en todas las réplicas que existan de la cadena, es decir, todos los nodos honestos están de acuerdo en seguir una misma cadena.

· Validez: cuando todos los nodos de la red reciben un bloque validado, este es aceptado y se une a la blockchain.

· Integridad de la cadena-hash: la blockchain recoge todos los bloques hasta el actual. Supongamos un bloque B con número 't' y otro bloque B* con número de bloque 't+1', el hash del bloque B* debería contener el hash del bloque anterior B, y así con todos los bloques, es decir, cada bloque posee una parte del bloque anterior, de manera que se consigue una integridad total de la cadena de bloques.

Por otro lado, el modelo de red en el que se fundamenta Bitcoin se basa en Internet y cada nodo se encarga de ejecutar parte del consenso de Nakamoto y guardar una copia de toda la cadena de bloques. Se trata de una red parcialmente sincrónica en la que el paso de mensajes en la red ocurre con un pequeño retardo de transmisión limitado entre dos nodos honestos. A parte de la sincronía de la red, Bitcoin tiene un acceso sin permisos y su información y existencia se propaga en función de la moda que exista en la actualidad.

Bitcoin es la primera red de blockchain a la cual se puede acceder sin permisos y no requiere de una autentificación para que un nuevo individuo se cree como nodo y participe en la red. Para configurar un nodo y unirse a la red tan solo hace falta seguir tres pasos:

1. Obtener una lista de nodos que sirvan de servidores conocidos.

2. Buscar una serie de nodos compañeros preguntando entre los que ya tienes y mediante los anuncios de estos, hasta conseguir un número de nodos mínimo (actualmente en Bitcoin son 8).

3. Rescatar una copia de la cadena de bloques de tus compañeros e iniciar a el funcionamiento normal.

Para salir de la red blockchain es tan sencillo como desconectarse de ella y se te irá eliminando de forma gradual de la lista de tus compañeros.

Protocolo de consenso

El protocolo de consenso de Nakamoto se ejecuta sobre una red que se encuentra distribuida, lo que significa que cada nodo ejecuta el protocolo y se encarga de

guardar una copia de la red blockchain. El nivel de seguridad de las cadenas de bloques depende fundamentalmente de la cantidad de nodos que sean honestos, es decir, que ejecuten correctamente el protocolo de Nakamoto. Este protocolo tiene cuatro reglas fundamentales:

1. Regla del paso de mensajes: cada bloque que reciba un nodo, o bloque que genere el mismo, debe compartirlo en ese momento con todos sus compañeros.

2. Regla de validación: los bloques y transacciones necesitan ser validados antes de compartirlos con tus compañeros y de añadirlos a cadena de bloques. Los bloques que no sean validados se tienen que descartar.

3. Regla de la cadena más larga: la cadena que sea más larga es siempre la cadena deseada. Los mineros deben tener como objetivo principal alargar la cadena más larga agregando a ella los nuevos bloques creados. Por ejemplo, si el nodo minero recibe un bloque B* validado de la misma longitud que un bloque B en el que todavía se está trabajando, tiene que descartar el bloque B y continuar la cadena con el bloque B*.

4. Prueba de trabajo (Proof-of-Work, PoW): La generación de un bloque incluye la inserción de una huella (hash) en el encabezado del bloque. El hash debe tener menos valores de uno determinado, así es como se controla la dificultad del PoW, cuanto más largo sea, requerirá más operaciones para conseguir el resultado por lo que la dificultad será mayor. Por razones de seguridad para las cadenas de bloques, este nivel de dificultad del PoW se ajusta automáticamente haciendo que el tiempo de generación de bloques se mantenga en una cifra estable a medida que se generan los hashes.

Como resultado de estas cuatro reglas del protocolo de Nakamoto, se consigue que las decisiones que se toman de manera honesta en la red estén representadas siempre en la cadena más larga, la que ha conllevado un mayor esfuerzo de cálculo y de PoW, creando así una mayor confianza.

El nombre de esta última característica del protocolo de consenso deriva del trabajo que tienen que realizar los mineros para conseguir adjudicarse la publicación de un bloque, el objetivo es que estos demuestren que de verdad se han esforzado en lograrla solución en un tiempo determinado, al resto de bloques que van a verificar el resultado.

El PoW hace que cada vez que se quiere publicar un bloque en la blockchain, los mineros tengan que resolver un acertijo matemático de manera que solo lo pueden

conseguir usando el método de prueba y error, de manera que tienen que realizar numerosos intentos para lograr resolverlo. Este problema matemático consiste en descubrir un parámetro que logre dar un determinado resultado, que será el futuro hash del bloque, de aquí que sólo pueda resolverse mediante este método tan laborioso.

El funcionamiento de esta prueba de trabajo es bastante sencillo y se puede dividir en cuatro etapas:

Etapa 1: el nodo tiene que establecer una conexión con la red, la que le asigna una tarea bastante difícil por resolver con un incentivo económico.

Etapa 2: el nodo tiene que comenzar a solucionar el acertijo, esta etapa es la más costosa ya que ha de usar mucha potencia, se denomina minería.

Etapa 3: el nodo tiene que compartir la solución en la red y esta es la encargada de verificar si el resultado es el correcto. Si es así se le adjudica el resultado.

Etapa 4: tras ser confirmada la validez del resultado del nodo, éste recibe su compensación económica.

Estas 4 etapas mencionadas son las encargadas de regular y modelar el funcionamiento de la Prueba de Trabajo (PoW). El uso de estos protocolos se centra en las redes blockchain, las cuales se benefician de sus principales características. Entre ellas podemos destacar el gran nivel de seguridad que aportan, y que además va aumentando cuantos más mineros se unan a la red. De manera adicional a esta característica podemos mencionar que la aplicación de estos protocolos es sustentada en unos algoritmos sencillos y fáciles de implementar y mantener lo que favorece el uso de ellos. Como principal característica negativa podríamos mencionar el gran consumo energético que conlleva este tipo de consensos.

Además de la prueba de trabajo, el Consenso de Nakamoto nos mencionaba que otra característica fundamental era que la decisión mayoritaria de toda la red estará representada por la cadena de bloques más larga ya que ha sido ésta la que ha conllevado un mayor esfuerzo de creación.

De acuerdo con la regla de la cadena más larga, los bloques que terminen en una rama de la cadena que no tenga el sufijo de la cadena más larga se desecharán o quedarán huérfanos. Esto significa que cualquier bloque de la cadena puede ser revocado,

principalmente para afrontar los ataques que se encuentran intentando hacer falsas cadenas iniciando una réplica de la original para que la red se confunda. Además de esta opción para controlar a los nodos deshonestos, si el atacante tiene menos de un 50% del poder de los hashes de la red, éste producirá bloques de manera más lenta que el resto de la red honesta.

Si denotamos 'p' al porcentaje del poder que puede ser controlado por el atacante, y si además denotamos "m" como la cantidad de bloques, entonces la probabilidad de que el atacante eventualmente alcance el ritmo de la cadena seguiría la siguiente ecuación:

$$P(\text{actualizarse}): (P/P-1)^{m}$$

Si p<50%, esta probabilidad cae de manera exponencial según 'm' va aumentando, es decir, la posibilidad de revocar el siguiente bloque de la cadena es cada vez más imposible si más de la mitad de la red pertenece a los nodos honestos y si de manera adicional tiene un tamaño grande. Actualmente en Bitcoin, m=6, se usa para conseguir un tiempo de confirmación de una transacción específico y controlado.

6.2 Otros protocolos de consenso en blockchain

Aunque ya se conoce la estrecha relación que existe entre seguridad y escalabilidad en la prueba de trabajo (PoW), los investigadores y desarrolladores han explorado cómo conseguir nuevos modelos de blockchain que consigan realizar un mayor número de transacciones y que pueda tener un mayor tamaño de red a la vez que un reducido consumo de energía ([2], [14], [25]). Entre los más comunes y utilizados podemos encontrar diferentes algoritmos de consenso como pueden ser: Prueba de Participación (Proof-of-Stake, PoS), protocolos de consenso basado en Tolerancia a Fallos de Práctica Bizantina (Practical Byzantine Fault Tolerance, PBFT), protocolo de consenso de Ripple o prueba de tiempo transcurrido (PoET). Estos algoritmos han sido propuestos como alternativas para pruebas de trabajo para blockchain públicas(PoS y PoET) o para aplicaciones específicas (PDFT-based, Ripple).

6.2.1 Prueba de participación (Proof-of-Stake, PoS)

Este nuevo modelo de consenso fue creado como una alternativa al Proof-of-Work y en vez de competir unos mineros contra otros por lograr el siguiente bloque haciendo uso de fuerza de cálculo bruta, en PoS se desarrolla de una manera más civilizada, con el objetivo principal puesto en el ahorro de energía y lo más importante la seguridad de la cadena de

bloques. La idea central era conseguir sustituir los recursos computacionales usados para dar seguridad en la red, por la mera característica de tener monedas, reduciendo de esta manera los costes y eliminando el fallo físico que pueden aportar estos sistemas.

La principal diferencia es el método para seleccionar el próximo bloque de transacciones que va a ser añadido a la cadena, el cual va ligado a la cantidad de monedas que posee el nodo participante. Los validadores que participan en este modelo de consenso entran en una especie de "concurso" depositando una cantidad de moneda, denominada participación, con la que entran en la competición de manera que la parte más interesada en conseguir la validación de un bloque tenga una mayor probabilidad de lograrlo si aumenta su participación y así sus opciones de ganar.

Usando un modo de vista económico, los individuos que quieran atacar a una red distribuida serán más reacios a realizar un ataque a un sistema PoS que en un sistema de consenso PoW, ya que en la mayoría de los sistemas PoS si se observa un comportamiento fraudulento de un individuo de la blockchain, éste pierde automáticamente su participación, mientras que si lo realiza en un sistema PoW lo único que pierde es electricidad. Por lo tanto, es económicamente más devastador realizar un ataque en una red blockchain con un sistema de consenso PoS.

6.2.2 Prueba de tiempo transcurrido (Proof-of-Elapsed-Time PoET)

La prueba de tiempo transcurrido o PoET fue desarrollada por Intel en 2016 como una alternativa a la Prueba de trabajo (PoW) [19]. Actualmente lo están desarrollando en el proyecto Sawtooth de Hiperledger. A diferencia de los consensos mencionados anteriormente, este no compite con fuerza como el caso de PoW, ni tiene la obligación de realizar un coste económico mediante participaciones como en PoS, sino que se basa en un sistema de lotería justo en el que se ha implementado un mecanismo basado en el retroceso aleatorio, ya usado en muchos otros campos con otros objetivos. Para producir un ciclo de generación de un bloque, es tan sencillo como seguir estos pasos:

- Paso 1: cada validador tiene que esperar un período de tiempo de tiempo aleatorio(el retroceso).
- Paso 2: el validador de bloques que primero acaba su retroceso es el encargado de generarlo.

Para garantizar que el tiempo de espera de cada validador sea de verdad aleatorio y lo

transcurra por completo, el mecanismo de espera de cada validador debe ser comprobado por el resto de validadores. En la práctica eso es tan sencillo como adquirir un microprocesador especialmente diseñado para ejecutar este tipo de sistemas de retroceso.

Si queremos mencionar alguna característica negativa podemos encontrar dos cuestiones principalmente y son, que este modelo de consenso puede aceptar cualquier número de validadores deshonestos, pero lo que se tiene que controlar es que éstos no sean más de un 50%. Y otro problema fundamental de este modelo es la actual dependencia hacia los proveedores de los microprocesadores encargados de ejecutar el proceso de retroceso necesario para la generación de un bloque.

Lo que se puede concluir de todo esto es que el consenso entre los participantes de una blockchain es una función central en un sistema distribuido, y hay que tener en cuenta diferentes modelos y características a la hora de diseñar un protocolo de consenso de blockchain. Si nos queremos centrar en una red que esté altamente conectada, sea accesible y que los participantes puedan realizar transacciones y bloques de manera autónoma, hace que sea más conveniente orientarse hacia unos protocolos de consenso con sistemas diseñados para la alta seguridad.

Por otro lado, si el objetivo es conseguir y lograr un modelo centrado en la confianza, hace necesario la utilización de unos sistemas mucho más eficientes que se encaminen más hacia el rendimiento de la red que hacia la seguridad de esta. El protocolo de consenso de Nakamoto al igual que los algoritmos de consenso PoW normalmente tienen una capacidad limitada de emisión de transacciones porque se diseñan para soportar condiciones de red inciertas y en unos escenarios en los que la confianza entre participantes es casi nula. Sin embargo, los protocolos basados en BFT son muy eficientes y soportan una gran cantidad de transacciones ya que se encuentran diseñados para aplicaciones específicas en las que se tiene que garantizar una alta conectividad a la red y además hay un control de acceso.

7. SUMARIO

Tras recopilar la máxima información posible acerca de esta nueva tecnología denominada Blockchain, procedo a establecer una serie de conclusiones que he podido obtener de la cadena de bloques.

Lo primero a destacar es que estamos hablando del nacimiento de una nueva tecnología y que queda mucho por descubrir aún de ella, pero lo que nos está enseñando hasta el día de hoy, es que posee numerosas características con las cuales vamos a poder ofrecer solución a muchos de los problemas que podemos tener actualmente en distintos sectores de la industria e incluso en el sector público.

La cadena de bloques es un sistema descentralizado que se encarga de eliminar los intermediarios de las transacciones, y es capaz de eliminar una de las características más importantes de ellas que es la necesidad de confianza entre las partes, todo ello gracias a su seguridad criptográfica y al registro continuo de todos los datos en una misma red.

Actualmente hay numerosos casos donde se hace uso de esta nueva tecnología, y el gasto en inversión ha aumentado considerablemente en estos últimos años. Esto quiere decir que no es una moda pasajera, sino que ha venido para quedarse y gracias al gran potencial que posee y los beneficios que puede aportar a la sociedad.

En el sector bancario se está adaptando continuamente desde la aparición de internet, y con el descubrimiento de la tecnología blockchain va a volver a experimentar un gran cambio. En la actualidad ya existen entidades financieras que están realizando procesos de inversión en la tecnología Blockchain para poder adaptarse a este nuevo modelo de interacción entre la banca y el cliente, con el objetivo de disminuir la cantidad de participantes involucrados en las transacciones y sobre todo el aumento de la transparencia con el cliente.

Hay otros sectores como el periodismo o el de la salud, que están necesitando de una gran cooperación entre los diferentes agentes implicados para conseguir rentabilizar el beneficio que puede aportar esta nueva tecnología. En el sector sanitario, por ejemplo, podría facilitar la capacidad de gestión de la historia clínica del paciente, cosa que hoy en día cuesta bastante, el ser capaces de gestionarlo cada uno por sí mismo ya que se encuentra registrado en las bases privadas a diferentes niveles: hospitales, comunidades autónomas, países…

Al igual que los sectores industriales, las administraciones públicas están observando el gran potencial que puede ofrecer la tecnología blockchain y conseguir reducir los costes de transacción de muchos de los departamentos del Sector Público. Siempre es exigido un trabajo rápido y claro por los ciudadanos y esta tecnología puede proporcionar ambas peticiones de la población.

Sabemos que puede ayudar en temas de transparencia al existir un único registro en las transacciones realizadas en una misma red, por lo que daría mayor confianza a la gente además de permitirles ser partícipes de la información.

Uno de los mayores problemas existentes en la actualidad es la falta de regulación normativa por parte de los Estados, necesaria para conseguir una confianza plena en la blockchain por parte de inversores y ciudadanos. La existencia de incertidumbre, orientada sobre todo hacia la falta de protección legal, hace que se frene el desarrollo de esta nueva tecnología.

Los defensores de esta nueva tecnología podían usar como defensa ante la desventaja comentada anteriormente la existencia de los protocolos de consenso, elemento fundamental y necesario en la creación de una blockchain. En él se establecen los requisitos a seguir para poder trabajar con una cadena de bloques determinada, y con ellos se asegura que la información registrada en una blockchain no va a ser alterada aun existiendo cierto número de participantes cuyo objetivo sea desestabilizar la armonía de la red.

Como conclusión final al trabajo cabe destacar que esta nueva tecnología junto a todas las aplicaciones que puede aportar en diferentes ámbitos va a ser fundamental en el desarrollo económico y social de muchos países en los próximos años. A pesar de las diferentes barreras que tiene esta tecnología y de que su adaptación está siendo lenta, hoy en día muchos proyectos con la cadena de bloques van avanzando, aunque se encuentren en fase de prueba, se prevé que su adopción a nivel mundial pueda llegar a ser superior a la que tuvo la aparición de Internet.

8. BIBLIOGRAFÍA

[1] Ast, F. (2019). *Entendiendo los Protocolos de Consenso de Blockchain.* https://medium.com/astec/entendiendo-los-protocolos-de-consenso-de-blockchain-4858c71722d2

[2] BitDegree. Prueba de Trabajo vs Prueba de Participación: ¿Cuál es mejor? https://es.bitdegree.org/crypto/tutoriales/prueba-de-trabajo-vs-prueba-de-participacion

[3] Blockchain: Contratos inteligentes - Smart Contracts. [Entrada en un blog]. Obtenido de https://www.lisdatasolutions.com/blog/blockchain_contratos_inteligentes/

[4] Blockchain, nueva herramienta para el periodismo. https://somacomunicacion.com/blockchain-y periodismo/

[5] Colle, R. (2017). Blockchain para periodistas y medios de comunicación. INCOM-Chile.

[6] Cordero, M. (2019). Blockchain en el sector público, una perspectiva internacional. *Revista Vasca de Gestión de Personas y Organizaciones Públicas*. Núm. 16/2019. Págs. 16-34.

[7] Crypto Español. (2018). *Cómo funciona blockchain. Explicación sencilla visual en español.* YouTube. https://www.youtube.com/watch?v=hEoYL5j0wYU&t=21s

[8] ¿Cuál ha sido el impacto del Blockchain en el sector consumo? (2020, 15 de junio). https://www.ey.com/es_do/consumer-products-retail/cual-ha-sido-el-impacto-del-blockchain-en-el-sector-consumo

[9] El Blockchain y los bancos. [Entrada en un blog]. Obtenido de https://www.theblockchain.es/blog/blockchain-los-bancos/

[10] El Mar, C.P. (2019). Blockchain y el sector asegurador. *Pyme Seguros*. nº 87/2019. pp44- 46

[11] El papel del Blockchain en la industria 4.0. [Entrada en un blog]. Obtenido de https://www.masterindustria40.com/blockchain-industria-40/

[12] Fernández, L. (2019). *Qué son los 'smart contracts' o contratos inteligentes.* https://www.bbva.com/es/smart-contracts-los-contratos-basados-blockchain-no-necesitan abogados/

[13] Füture, R. (27 de marzo 2018). *B3i crea una sociedad independiente de servicios para impulsar el blockchain en seguros* [Entrada en un blog]. Obtenido de https://future.inese.es/b3i-crea-una-sociedad-independiente-de-servicios-para-impulsar-el

blockchain-en-seguros/

[14] Gómez, I. (2020). *Algoritmos de Consenso: Prueba de Trabajo vs Prueba de Participación.* https://www.criptonoticias.com/tecnologia/algoritmos-consenso-prueba-trabajo-vs-prueba participacion/

[15] Industria 4.0, ¿Qué debemos saber? (2018, 12 de julio). https://www.isotools.org/2018/07/12/industria-4-0-que-debemos-saber/

[16] La banca se suma al "blockchain", la tecnología que revolucionará el sector (2018, 25 de febrero). https://www.finanzas.com/mercados/la-banca-se-suma-al-blockchain-la-tecnologia-que revolucionara-el-sector_13790106_102.html

[17] La tecnología blockchain concita interés en el sector sanitario (2020, 16 de abril). https://diarioti.com/la-tecnologia-blockchain-concita-interes-en-el-sector-sanitario/111 561

[18] Laurence, T. (2017). Blockchain for Dummies. John Wiley & Sons, Inc. Mitra, R. (2019). *Prueba de trabajo vs Prueba de participación: Guía básica de minado.* https://blockgeeks.com/guides/es/prueba-de-trabajo-vs-prueba-de-participacion/

[19] Montaner, D. (2021). *¿Qué es la Prueba de tiempo trascurrido (PoET)? (Criptomoneda).* https://criptomundo.com/que-es-la-prueba-de-tiempo-transcurrido-poet-criptomoneda/

[20] Muñoz, J.M. (2019). *El blockchain y el impacto en los distintos sectores y negocios.* https://valenciaplaza.com/el-blockchain-y-su-impacto-en-los-distintos-sectores-y-neg ocios

[21] Pastor, J. (2018). *Qué es blockchain: La explicación definitiva para la tecnología más de moda.* https://www.xataka.com/especiales/que-es-blockchain-la-explicacion-definitiva-para-l a tecnologia-mas-de-moda

[22] Peña, C. (2019). *Blockchain y el sector asegurador.* https://www.pymeseguros.com/blockchain-y-el-sector-asegurador

[23] Pérez, I. (2017). *Consorcio Blockchain de aseguradoras B3i crece con 10 miembros globales.* https://www.criptonoticias.com/negocios/consorcio-blockchain-seguros-b3i-10-miembros-globales/

[24] Preukschat, A. (2018). Blockchain: La revolución industrial de internet. (7ª ed). Gestión 2000

[25] ¿Qué es Prueba de Trabajo / Proof of Work?
https://academy.bit2me.com/que-es-proof-of-work-pow/

[26] Rodríguez, N. (2018). *Transformación Digital de Blockchain -30+ Ejemplos de la Transformación de Blockchain.*
https://101blockchains.com/es/transformacion-digital-de-blockchain/

[27] Romero, F. (2018). *¿Qué puede aportar el Blockchain a la comunicación?*
https://innova.dircom.org/noticias/innovar-en-comunicacion-noticias/aporta-blockchai n comunicacion/

[28] Rubio, A (2020). *Blockchain en el sector asegurador.*
https://www.digitalbizmagazine.com/blockchain-en-el-sector-asegurador/

[29] Samaniego, J.F. (2018). *Blockchain, la tecnología imprescindible en el avance de la Industria 4.0*
https://hablemosdeempresas.com/grandes-empresas/blockchain-en-la-industria/

[30] Sanidad - Trazabilidad basada en Blockchain en este sector.
https://www.blockimpulse.com/2019/10/07/sanidad-trazabilidad-identidad-digital-basada en-blockchain/

[31] Sintes-Olivella, Marçal; Xicoy-Comas, Enric; Yeste-Piquer, Elena (2020). "Blockchain al servicio del periodismo de calidad. El caso Civil". *Profesional de la información*, v. 29, n. 5, e290522.
https://doi.org/10.3145/epi.2020.sep.22

[32] Smart Contracts: ¿Qué son, cómo funcionan y qué aportan?
https://academy.bit2me.com/que-son-los-smart-contracts/

[33] Smart Contracts: Qué son, para qué sirven y ventajas. [Entrada en un blog]. Obtenido de https://www.iebschool.com/blog/smart-contract-blockchain-tecnologia/

[34] Tic portal (2018). *Blockchain (cadena de bloques)*.
https://www.ticportal.es/glosario-tic/blockchain

[35] Xiao, Y; Zhang, N; Li, J; Lou, W; Thomas, Y. (2019). Distributed Consensus Protocols and Algorithms. En Wiley & Sons (Ed) *Blockcahin for Distributed Systems Security.*