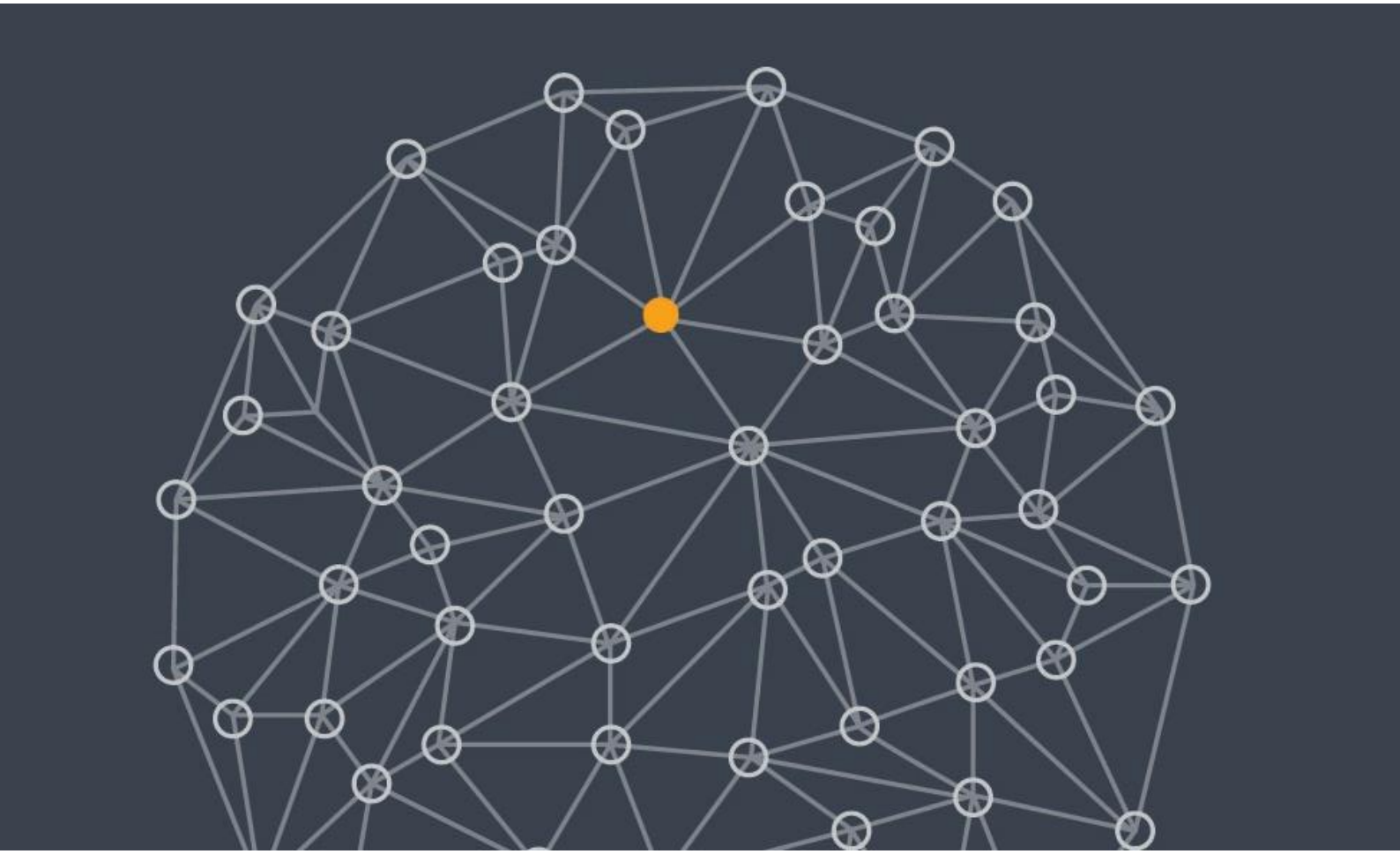
MILLIMAN RESEARCH REPORT

Blockchain en el sector de seguros

Mayo 2019

José Silveiro, IA
Rubén Nova, IA



Milliman

Introducción

Blockchain es una tecnología emergente que se menciona de manera frecuente como un avance con el que distintas industrias deberían familiarizarse, aunque todavía existe la percepción de que se trata más de una teoría que de una realidad. Por otro lado, ya existen numerosas iniciativas en distintos sectores que permiten su exploración o ya están aprovechando las posibilidades que ofrece. El sector de seguros es uno de ellos.

Blockchain es la tecnología sobre la que se sustenta un registro validado y compartido de transacciones y/o eventos y que, junto con tecnologías existentes y ampliamente aceptadas de captura y análisis de datos, se presenta como una plataforma decisiva para la generación de valor en el sector de seguros.

En este informe tratamos de explicar la tecnología *blockchain*, así como algunos de sus usos actuales, presentando un ejemplo de un producto de seguros que se beneficiaría de esta tecnología, con el fin de poner en contexto los aspectos a considerar en el lanzamiento de un prototipo.

A continuación, proporcionamos una breve introducción de *blockchain*, sus usos y sus propiedades.

¿Qué es blockchain?

De una manera formal, *blockchain* puede definirse como una red que gestiona un registro de datos, de forma descentralizada, que requiere protección criptográfica y que ha de estar abierta a un público predefinido. Posibilita que partes que no confían plenamente entre sí puedan mantener una única verdad, mediante consenso y sin necesidad de una entidad central o intermediario.

Cualquier persona autorizada (dentro del público predefinido) puede registrar una transacción en la red. Una vez verificada, se forma un nuevo bloque (*block*), que se une a los bloques anteriores de la cadena (*chain*): de ahí surge su nombre y por eso se conoce como la tecnología de la cadena de bloques. *Blockchain* permite un registro cronológico compartido, que cualquier participante de la red puede consultar, pero nunca modificar o borrar (a lo que suele referirse como propiedad de inmutabilidad). Esto es muy útil para procesos que requieren trazabilidad o auditoría.

Blockchain empezó a utilizarse en enero de 2009, cuando Satoshi Nakamoto lanzó la criptomoneda bitcoin. Desde entonces, es frecuente confundir bitcoin con *blockchain*. Bitcoin es una red que permite un sistema de pagos digital sin la intervención de ninguna entidad bancaria y que utiliza la tecnología *blockchain* para hacerlo posible. *Blockchain* puede utilizarse sin necesidad de la existencia de criptomonedas.

Como participantes dentro de una red *blockchain*, las personas y las organizaciones pueden controlar una red compartida de transacciones históricas, y beneficiarse de la información agregada que puede ofrecer acerca de ellos o acerca de los productos de interés para las partes involucradas.

USO Y CONSORCIOS

Uno de los casos más conocidos es su uso por los supermercados Walmart para garantizar al consumidor y a las autoridades sanitarias la trazabilidad de sus productos comestibles. El cliente tiene acceso al registro compartido que se construye desde la recogida hasta cada una de las etapas de distribución de los alimentos y, de este modo, puede conocer toda la vida del producto que está comprando, con garantía de procedencia, de que se ha respetado la cadena de frío o del tiempo que ha transcurrido desde su recolección.

La Compañía implementó su piloto en 2019 y su aplicación podría haber disminuido las consecuencias económicas del incidente ocurrido en 2018 relacionado con un brote de la bacteria *E. coli*. La bacteria estaba asociada a un lote de lechuga romana cultivada en la región de Yuma, que causó 210 infecciones, 96 hospitalizaciones y 5 muertes en el estado de Arizona (Estados Unidos). Dado que las autoridades sanitarias no pudieron precisar inicialmente el origen del lote de lechugas contaminadas, se retiraron del mercado millones de bolsas de este producto, sin diferenciar su origen. *Blockchain* habría permitido localizar y retirar el producto afectado en pocas horas, en lugar de días. Tras el éxito de Walmart, se han unido a la denominada red *Food Trust* diez de las compañías de alimentación más grandes del mundo, como Unilever o Nestlé.

En mayo de 2018, el consorcio de la industria del automóvil MOBI (*Mobility Open Blockchain Initiative*), fundado por conocidos fabricantes de automóviles como Ford, BMW, Renault y General Motors, anunció el lanzamiento de varios casos de uso de *blockchain*. Uno de los primeros desarrollos de MOBI ha consistido en dotar de una identidad digital al vehículo para que se pueda localizar en cualquier momento, lo cual previene posibles manipulaciones del odómetro. Esta aplicación aporta beneficios a los distintos participantes de la industria automovilística.

- **Clientes**: potencial reducción del fraude en la compraventa de vehículos usados y mejora del mantenimiento del vehículo;
- **Fabricantes y talleres**: disponen de un historial más preciso del vehículo de cara a sus reparaciones y garantías;
- **Aseguradoras**: cuentan con datos más precisos y fiables para el cálculo de sus primas.

El interés global despertado por *blockchain* ha motivado la formación de consorcios en los que las empresas participantes apuestan de forma conjunta por la investigación, desarrollo e inversión relacionados con la tecnología, para el beneficio conjunto de los miembros del consorcio. A continuación, citamos tres de los más conocidos:

- **B3i (*'The Blockchain Insurance Industry Initiative'*)**: se crea en el año 2016, con la colaboración de compañías aseguradoras globales, con el objetivo de aumentar la eficiencia en el intercambio de datos entre aseguradoras y reaseguradoras mediante el uso de *blockchain*. Los miembros fundadores fueron Aegon, Allianz, Munich Re, Swiss Re y Zurich. En 2017, B3i lanzó un prototipo de sistema inteligente de gestión de contratos de reaseguro catastrófico;
- ***Hyperledger***: se lanzó en 2016 como una colaboración global organizada por ***The Linux Foundation***, e incluye compañías líderes en finanzas, banca, salud, cadenas de suministro, fabricación y tecnología. En la actualidad, *Hyperledger* está compuesto por más de 200 compañías de todo el mundo, incluyendo IBM, R3, la Universidad de Cambridge, el Banco de Inglaterra o el grupo financiero BBVA;
- ***Enterprise Ethereum Alliance***: es una organización sin ánimo de lucro que une empresas para investigar e implementar soluciones basadas en contratos inteligentes a través de la *blockchain* pública de *Ethereum*, fundada en marzo de 2017. Entre sus miembros se encuentran empresas del *Fortune* 500, *startups*, académicos y aseguradoras. Algunos miembros son J.P. Morgan, Banco Santander o Thomson Reuters.

PROPIEDADES

Blockchain tiene algunas propiedades que son clave, y que distinguen esta tecnología emergente de otras tecnologías de red y de gestión de registros:

- **Distribuida:** El registro mantenido por *blockchain* es gestionado por un grupo limitado de usuarios bajo algoritmos de consenso. Cada operación registrada en la red es replicada por todos los participantes de la cadena, garantizando la seguridad y robustez de la red ante ataques maliciosos. Las cadenas de bloques también se pueden combinar entre sí, reforzando de esta forma su carácter distribuido.
- **Permisionada:** Cuando se crea una *blockchain*, se define un protocolo con las reglas que gobiernan la plataforma, incluyendo la definición de un estándar común para delimitar la comunicación entre los participantes de la red.
- **Pública o privada:** Una *blockchain* pública se define por un protocolo abierto a todo usuario que puede acceder, consultar y validar las transacciones. Una *blockchain* privada (o 'permisionada'), requiere un mayor grado de confianza entre las partes, dado que solo los participantes autorizados pueden acceder a los datos inscritos. Según establezca su protocolo, se les permitirá el registro de transacciones en la cadena y/o poder verificar los cambios producidos en la red. Existen también las *blockchain* híbridas, llamadas *blockchain* semi-permisionadas que son una combinación de *blockchain* pública y permisionada.
- **Universal:** la red permite realizar operaciones entre participantes independientemente del lugar donde se encuentren, debido a la eliminación de intermediarios y entidades centrales, y gracias a la descentralización de los procesos. La tecnología facilita operar *business-to-business* (B2B) o *peer-to-peer* (P2P), posibilitando el acceso al sistema a la población no bancarizada (un 38% de la población mundial, según datos del Fondo Monetario Internacional). Además, permite eliminar parte de la fricción relacionada con pagos transfronterizos, reduciendo ineficiencias, costes y riesgos de los intermediarios. Al realizar una operación dentro de una plataforma *blockchain*, se reducen costes marginales y tiempo en la operación**.**
- **Concede autoridad al cliente (Identidad Soberana Personal):** la red dota a cada usuario de una identidad digital protegida mediante sistemas criptográficos que permite prescindir del uso de otras identidades como pueden ser el pasaporte o el permiso de conducción. La información de cada usuario está repartida en los

diferentes nodos de la red y permite autorizar a terceros el uso de datos específicos ante una transacción concreta. Este término es conocido como Identidad Soberana Personal (*Self Sovereign Identity*). Esto significa que el usuario controla y administra su identidad y quién tiene acceso a su información personal. Por ejemplo, si una persona desea acceder a un evento en el que se requiere ser mayor de 18 años, en lugar de mostrar su documento de identidad, con la identidad digital se podría verificar la edad sin necesidad de mostrar ningún otro tipo de dato además de la fecha de nacimiento, como su dirección.

La Identidad Soberana Personal permite concentrar una serie de atributos digitales, como puedan ser la edad, el historial crediticio o de siniestralidad, las licencias o títulos académicos en un único repositorio. Esto permite crear una huella digital que, unida a una clave privada, permite asegurar la transferencia y utilización autorizadas de datos, documentos y otros archivos.

Contratos inteligentes

Uno de los desarrollos clave construidos sobre *blockchain* son los contratos inteligentes (*Smart contracts*), que suponen la ejecución de una o varias de las cláusulas establecidas en un contrato de forma automática, a partir de una transacción o evento validado.

Es relevante especificar que, aunque los contratos de seguro (o cualquier otra información almacenada) permanecen como documentos digitales dentro de una *blockchain*, las condiciones estipuladas en dichos contratos y que dan lugar a los diferentes procesos fuera de la *blockchain* (como la gestión de siniestros, la renovación de pólizas o los descuentos de prima) son códigos programables dentro de la propia red. Por tanto, podemos definir los contratos inteligentes como un código programable que permite establecer condiciones para que ciertos procesos se ejecuten automáticamente con *blockchain*.

Hay que tener en cuenta que en muchos casos la cadena de bloques no dispone ni registra los datos necesarios para que los contratos inteligentes se puedan ejecutar. En estos casos, una fuente de verificación externa (llamada 'oráculo') facilita el desencadenante para ejecutar lo estipulado. Por ejemplo, en un seguro de retraso y cancelación de vuelos sustentado sobre tecnología *blockchain*, la agencia estatal aérea haría la función de oráculo que verifica el retraso o cancelación de vuelos afectados y desencadena el pago de la suma asegurada estipulada en el contrato. De esta forma, ni la aseguradora ni el cliente necesitan realizar un trámite adicional para verificar el siniestro incurrido.

Las ventajas de los contratos inteligentes se amplían cuando se combinan con otras tecnologías como el internet de las cosas. Imaginemos un contrato de *leasing* cuyo contrato inteligente detectara una cuota impagada. En ese caso, se podría enviar un mensaje a la pantalla del coche y/o activar otras acciones, sin necesidad de intervención humana.

Producto de seguros

En esta sección presentamos un ejemplo de uso de *blockchain* en un producto asegurador nuevo hipotético. Supondremos que, dentro de su proceso de transformación digital, una aseguradora se plantea explorar las capacidades de *blockchain* a partir de un proyecto piloto y valorar la contribución de la tecnología para:

- **Optimizar las primas ofrecidas al cliente**, incorporando la mejor información para la valoración del coste esperado de los riesgos asegurados.
- **Fomentar una relación más personalizada con el asegurado**, evaluando las posibilidades de la tecnología para mejorar el conocimiento del cliente y de compartir dicho conocimiento con otros proveedores (servicios de salud y bienestar, proveedores deportivos, proveedores de tecnología).
- **Ahorro de costes**, por la mejora de la eficiencia de ciertos procesos y en la identificación (o prevención) del fraude.

La compañía reconoce que la adopción de *blockchain* no supone una ventaja o solución en sí misma, y actualmente el sector aborda los aspectos anteriores con otros enfoques exitosos. Asimismo, la compañía reconoce que la tecnología *blockchain* tiene costes de infraestructura asociados. El resultado del piloto debería permitir conocer las ventajas de iniciar un proyecto basado en esta tecnología de manera temprana, así como las limitaciones actuales de la misma y otros posibles riesgos.

El producto de seguro que se propone consiste en aprovechar las ventajas de la tecnología *blockchain*, combinada con el internet de las cosas, y ofrecer a los clientes de la compañía un seguro para actividades físicas como correr o andar. La compañía desea ofrecer coberturas novedosas y servicios que permitan disfrutar de una mayor seguridad en la realización de las actividades, y a través de una experiencia más personalizada y eficaz gracias a la automatización que permite *blockchain*.

COBERTURA OFRECIDA

El prototipo ofrece una cobertura novedosa a las pólizas actuales de vida, salud y accidentes de la compañía. Se trata de una cobertura opcional, ofrecida de manera gratuita a aquellos asegurados que actualmente tengan contratados al menos dos de los productos mencionados, debiendo ser uno de ellos el seguro de vida.

La cobertura novedosa cubre ciertos costes asociados a lesiones causadas durante las actividades físicas de correr y andar. Por tanto, se destina a un amplio universo de pólizas, con edades comprendidas entre 18 y 75 años, ofreciendo:

- Servicio de asistencia para traslado de emergencia a un centro de salud;
- Servicio de alertas climatológicas para el recorrido planeado y geolocalización;
- Servicio de llamada automática a la persona de contacto identificada por el asegurado, indicando el lugar donde se ha producido la lesión y el centro médico al que se ha trasladado al asegurado;
- Descuento del 20% en servicios prescritos de fisioterapia para las 5 primeras sesiones, que se añadirían como un beneficio adicional en el caso de tener contratada la póliza de salud.

La cobertura estaría sujeta a las mismas exclusiones y normas de suscripción que las propias de las pólizas de vida, salud y accidentes. Las coberturas de asistencia y llamada automática estarían 100% reaseguradas. Se establece un límite anual de uso de las coberturas que no podrá ser superior a 2 usos en 2 años consecutivos. La cobertura es anual con posibilidad de renovación por ambas partes al vencimiento.

TARIFICACIÓN

Como se ha mencionado previamente, la cobertura se ofrecería de manera gratuita a aquellos asegurados que tengan contratados al menos 2 de los productos mencionados, debiendo ser uno de ellos el de seguro de vida.

Asimismo, y como contribución al asegurado por la información adicional que la compañía obtiene sobre cómo influyen sus hábitos en el uso de las pólizas contratadas, cada sesión de actividad física permitiría acumular '***Tokens'*** intercambiables por descuentos en la red de proveedores de servicios adscritos al programa.

De esta forma se desarrolla un nuevo sistema abierto entre los clientes de la compañía, la propia aseguradora y otros proveedores de servicios, basado en el sistema de '*tokens*', definidos en los contratos inteligentes y registrados en la *blockchain*.

A medio plazo, cuando la compañía haya podido comprender el impacto de los hábitos saludables, podrían considerarse sistemas de tarificación más sofisticados para los seguros de vida, salud y accidentes. Más allá de una mejora en la segmentación del cliente, también será necesario conocer las implicaciones de trabajar en ecosistemas de colaboración, determinar si se produce un ahorro real de costes y/o mejoras en la prevención de accidentes, así como posibles riesgos relacionados con el producto y no considerados previamente.

ACTIVACIÓN DE LA COBERTURA

La activación inicial de la cobertura sería promovida por los distintos canales de la compañía y, en concreto, se considera una herramienta de fidelización para el mediador. La activación se iniciaría con la descarga de una App en el *smartphone* del cliente, seguida de la configuración de su identidad digital.

En la tabla inferior 'Información del asegurado' se muestra la información que se solicitaría inicialmente al asegurado. Además de la información recogida durante la activación inicial, durante cualquier actividad física monitorizada, se registraría información relacionada con el lugar y el estado físico del asegurado. Finalmente, y en función de las preferencias del asegurado, su información podría compartirse con terceros, como proveedores de servicios, bajo un esquema de descuentos.

GRÁFICO 1: INFORMACIÓN DEL ASEGURADO

INICIAL	DURANTE LA ACTIVIDAD	REGISTRADA POR TERCEROS
EDAD	FRECUENCIA CARDÍACA	EXÁMENES MÉDICOS
ESTATURA	RITMO CARDÍACO	PRUEBAS DE ESFUERZO
PESO	LOCALIZACIÓN	TRATAMIENTOS DE FISIOTERAPIA
SI PRACTICA OTROS DEPORTES	FECHA Y HORA	SEGUIMIENTO DEL PESO Y ALIMENTACIÓN POR NUTRICIONISTAS

DISPOSITIVOS NECESARIOS

La activación contextual de la cobertura se realizaría por parte del asegurado al inicio de la actividad física, para lo que debería acceder a su cuenta, por reconocimiento biométrico o a partir de su código personal, a través de la App instalada en su dispositivo electrónico.

Para registrar la información durante la actividad, el mediador ofrecería al asegurado una "pulsera inteligente", conectada a internet y vinculada con la App de su *Smartphone* (ej. a través de NFC o *Bluetooth*), para el uso del GPS, entre otras aplicaciones.

USO DEL BLOCKCHAIN

La pulsera puede incorporar los siguientes sensores: acelerómetro, pulsómetro, termómetro, giroscopio, geolocalizador, altímetro, etc. y, por tanto, permitiría registrar el pulso cardíaco y duración de la sesión, así como localizar el lugar y el momento de la actividad. Este dispositivo, junto con el *Smartphone* del asegurado y los contratos inteligentes definidos por la *blockchain*, permitiría automatizar los siguientes procesos:

- **Contractual**: junto con la notificación de una lesión sufrida por parte del asegurado, el contrato inteligente comprueba las condiciones pactadas en el contrato de seguro e inicia automáticamente la prestación del servicio. Estas notificaciones pueden darse de manera sencilla a través de la App o pueden ser identificadas de forma automática gracias a los sensores de la pulsera;
- **Gestión del servicio**: en caso de detectarse anomalías en los datos que se están registrando, se activarían varios contratos inteligentes que garantizarían la seguridad del cliente; el primero sería un mensaje automático al asegurado en modo de vibración durante varios segundos para comprobar que se encuentra bien. En caso de que el asegurado no desactivara la alerta, otro contrato inteligente generaría una llamada telefónica al usuario para verificar que no se encuentra en situación de peligro. Por último, se avisaría al número de emergencias, enviando la localización del asegurado para que pudiera recibir asistencia a la mayor brevedad;
- **Antifraude**: en caso de anomalías que pudiesen reflejar un uso fraudulento del servicio, se solicitarían otras medidas de seguridad. Por ejemplo, dado que el historial de actividad es trazable, si la actividad física la realizara una persona distinta al asegurado, podrían detectarse un comportamiento cardíaco o velocidad fuera del rango observado para el individuo, y en ese caso se solicitaría una prueba biométrica adicional, como una fotografía;
- **Oferta personalizada de servicios**: a partir de ciertas reglas de servicio acordadas, los contratos pueden activarse para ofrecer servicios contextuales (nutricionista, entrenador personal, pruebas médicas para deportistas, etc.). Los contratos permanecen en suspensión en la red y, en caso de detectar inactividad prolongada del usuario, podrían activarse incentivos para el retorno a la actividad, o darle la posibilidad de conectar con otros usuarios para unirse a actividades físicas colectivas.

GRÁFICO 2: MONITORIZACIÓN DE LA SALUD DEL USUARIO CON BLOCKCHAIN

PLATAFORMA DEL PILOTO

La compañía se ha planteado de manera realista los desarrollos tecnológicos que puede liderar internamente, así como aquellos para los que necesita contar con terceros que faciliten el acceso a soluciones actualizadas y de alto nivel. Además, debe ofrecer garantías respecto al estricto cumplimiento de las leyes de protección de datos.

Por tanto, se decide que la infraestructura de *blockchain* e Internet de las cosas aprovecharía los recursos aportados por un conocido Consorcio, acordando las siguientes condiciones:

- Durante los 2 primeros años, la información se compartiría únicamente entre la compañía, la reaseguradora y los proveedores de servicios autorizados por el cliente. A partir del año 3, el cliente tendría la opción de beneficiarse de cualquier servicio ofertado en la red *blockchain*, incluyendo ofertas de otras aseguradoras, que tendrían de ese modo acceso al historial de actividad física y de servicios del asegurado;
- El capital intelectual desarrollado pertenecería al Consorcio y se compartiría con todas aquellas aseguradoras con interés dentro del Consorcio;
- La aseguradora no estaría obligada a compartir el conocimiento adquirido sobre los clientes, ni sus metodologías de análisis de la información.

CRITERIOS DE MEDIDA DE ÉXITO

Para medir el éxito del proyecto, la compañía ha definido unas métricas combinadas, en un horizonte temporal de entre 12 y 18 meses, que tendrían en consideración:

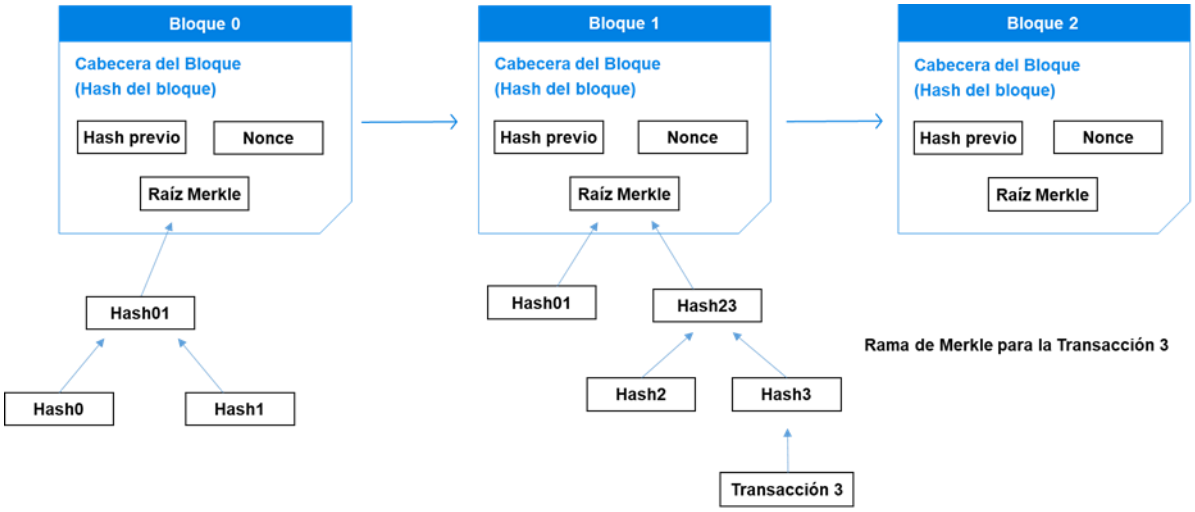
- **Las altas y el uso efectivo de la aplicación**: mediante un análisis estadístico de los clientes que han utilizado la aplicación, recurrencia, su influencia en otros servicios de la compañía, etc.
- **La mejora en la retención de las pólizas que utilizan la cobertura**: si el uso del servicio ha tenido un impacto positivo en el número de clientes que renuevan el contrato con la compañía.
- **Las comisiones percibidas por terceros**: recibidas a cambio de que otros proveedores ofrezcan a los clientes de la compañía los servicios incluidos en los acuerdos de colaboración.
- **La calidad y la capacidad predictiva de la nueva información** (ej. hábitos de vida): tanto en el uso de las coberturas de los seguros de vida, salud y accidentes, como en la prevención y mejora de la experiencia del asegurado.

En definitiva, el producto piloto descrito trata de lograr una mayor cercanía con el cliente y un nivel de interacción superior, tanto en frecuencia, como en distintos tipos de actividad complementarios a la pura actividad aseguradora. La manera de lograrlo no es necesariamente el uso de *blockchain* combinado con otras tecnologías, pero el prototipo serviría para valorar las distintas alternativas.

¿Cómo funciona *Blockchain*?

En el gráfico 3 se refleja de manera esquemática el funcionamiento de la cadena de bloques.

GRÁFICO 3 ELEMENTOS QUE FORMAN LA CADENA DE BLOQUES



El término 'bloque', se refiere a cada unidad de la cadena, formada por la cabecera del bloque y el árbol de *Merkle*[1]. Cada bloque contiene diferentes elementos:

- Cada cabecera del bloque contiene el *hash* de la cabecera del bloque anterior, excepto el bloque cero, conocido como el bloque génesis, donde el *hash* previo es únicamente ceros;
- *Nonce*[2]: funciona en combinación con el *hash* como un elemento de control para evitar la manipulación de la información de los bloques (también incorpora una marca de tiempo);
- *Hash* raíz del árbol de *Merkle* de todas las transacciones incluidas.

Cada uno de los bloques anteriores puede almacenar diferentes operaciones. En el contexto de un seguro de automóvil, el Bloque 0 o génesis podría ser el alta del contrato de seguro, el Bloque 1 la declaración de un siniestro y el Bloque 2 una renovación. La transacción 3 dentro del Bloque 1 podría ser, por ejemplo, el envío de una foto de un vehículo siniestrado, a la que podrían añadirse informes policiales sobre el accidente o un informe médico. Cada informe constituye una transacción diferente dentro de la raíz de *Merkle*, que contiene un resumen de todas las transacciones realizadas que dependen del árbol.

Cada protocolo de *blockchain* define el tamaño de cada bloque, que depende de diversos factores, como la velocidad de la transacción, robustez o pruebas de verificación y en los que se va regulando mediante consenso entre sus participantes. Por ejemplo, el protocolo de *Bitcoin* establece que los bloques deben tener un tamaño de 1MB. La capacidad de los bloques entra en conflicto con la supuesta escalabilidad de *blockchain*, que implica que un sistema debe poder crecer y adaptarse sin comprometer su rendimiento. Continuando con el ejemplo, una transacción en *Bitcoin* suele ocupar de media 0.5kb, y como los bloques son de 1024kb (1MB), en un bloque pueden realizarse hasta 2048 transacciones.

La función *Hash* se conoce también como función resumen o función *digest*. Se define como un procedimiento criptográfico irreversible donde se aplica un algoritmo matemático para transformar información en una secuencia alfanumérica. Siempre que se aplique la misma función al mismo contenido, se obtendrá el mismo *hash*. De esta forma, si alguien intentara modificar cualquier contenido, el *hash* cambiaría completamente, por lo que son muy útiles en aplicaciones criptográficas.

[1] Árbol de *Merkle*: Estructura de valores en forma de árbol donde cada *hash* es el resultado de aplicar una función *hash* sobre el *hash* anterior, hasta llegar a un *hash* raíz. De esta forma proporciona un método de verificación segura y eficiente de los contenidos de grandes estructuras de datos.

[2] *Nonce* (*Number used only once*): Número que cambia secuencialmente para variar el mensaje original y provocar que el *hash* obtenido sea distinto en cada intento. El *nonce* es usado para comprobar que un bloque ha sido verificado y para evitar manipulaciones.

Si utilizamos la función SHA-256[3] para aplicar la función *hash* sobre el *input* que contiene el mensaje: “Milliman”, el *output* resultante sería:

f65e5463f55186c7c8a515f4e429a02192460ce62d229bf3a46ce581a8c2aeb4

Si, por el contrario, el mensaje fuese: “Milliman ha escrito este documento”, la función *hash* se representaría de la siguiente forma:

3f1828b144913a7cd6bc5d22b662484b851ab1b77f981afe7450fd206a874cd1

A continuación, se enumeran las características de la función *hash*:

- No se puede deducir un patrón que permita llegar desde el *input* al *output*. Es decir, leyendo el mensaje “Milliman”, del ejemplo anterior, no es posible (en la actualidad) deducir la salida de la función *hash*;
- Imposible de revertir. Al igual que en el punto anterior, teniendo la salida de la función *hash*, es difícil saber el mensaje original sin tener las claves que permitan descifrarlo;
- Siempre que se aplique la función sobre el mismo *input*, se obtendrá el mismo *hash*. De esta forma, siempre que el mensaje sea “Milliman”, se obtendrá el mismo *hash*, por lo que se puede comprobar fácilmente si una transacción ha sido modificada;
- Siempre tiene la misma longitud independientemente de la longitud del *input*. Es decir, no importa el tamaño del mensaje, documento o archivo al que se le haya aplicado la función *hash*, que siempre tendrá la misma longitud (equivalente a 32 *bytes*).

Para ver el potencial de la función *hash*, imaginemos que se quisiera proteger la información sobre el listado de todos los libros que existen en la biblioteca de una universidad en un solo *hash*, éstos ocuparían solo esos 32 *bytes*. Esto es posible dado que en el bloque solo se guarda la salida que produce la función resumen y ésta es de longitud fija, indistintamente del tamaño de los archivos a los que se aplica la función. Por tanto, si accedemos al *hash* de un bloque, podremos acceder a la dirección URL asociada al *hash*, que puede estar localizada en la nube, accediendo así a la dirección donde se encuentran los libros. Además, si alguien intentara modificar el documento o borrar uno de los libros, la función *hash* cambiaría completamente, y el resto de los participantes podrían rechazar la operación, por lo que sirve también como prueba de verificación.

Otros conceptos relevantes para el funcionamiento de la cadena de bloques son los conceptos de *tokens*, claves públicas y privadas y validación de las transacciones.

Un *token* es un activo digital en el que pueden incluirse uno o varios derechos. Cualquier activo físico, digital o servicio puede ser subido a la cadena bajo el concepto de *token*. Hoy por hoy, las criptomonedas de la red *Bitcoin* o la red *Ethereum* representan gran parte de los *tokens* existentes. Sin embargo, gracias a la huella digital que permite la tecnología, cualquier elemento puede ser susceptible de ser ‘tokenizado’ y, por lo tanto, intercambiado en el mercado con una liquidez inmediata.

Existen los *tokens* fungibles y los *tokens* no fungibles. Los primeros son los *tokens* que son intercambiables por uno de igual valor y no importa su individualidad, por ejemplo, las criptomonedas. Los *tokens* no fungibles son aquellos que presentan características únicas que hacen posible su distinción de otros *tokens* del mismo tipo. Un ejemplo puede ser una casa, un contrato de seguro o los datos de una persona en particular.

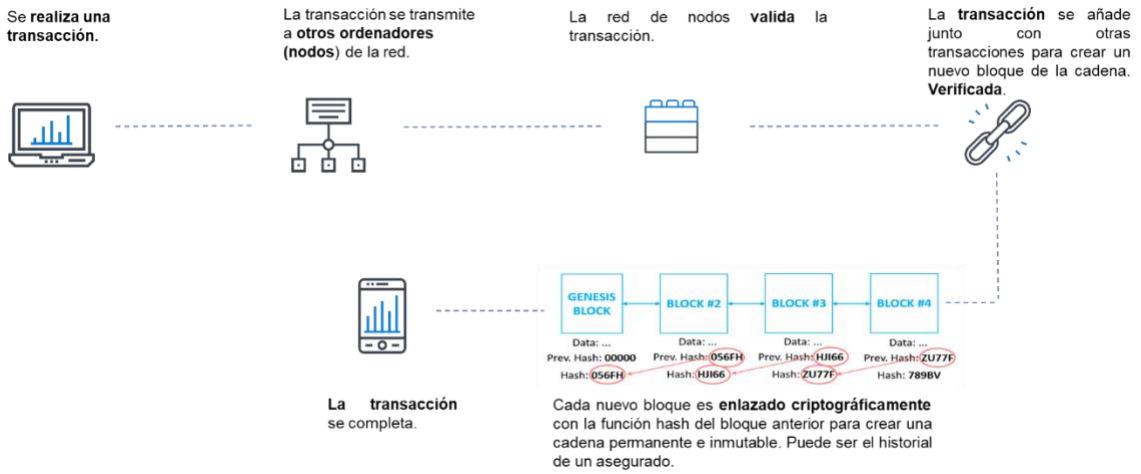
Claves públicas y privadas: son dos claves de criptografía asimétrica vinculadas entre sí mediante una función matemática. La clave pública se calcula a partir de la clave privada. Si conocemos la clave privada podremos conocer la clave pública, pero no al revés. Si alguien quiere enviar un mensaje cifrado solo necesitará conocer la clave pública, con ella cifrará el mensaje y solo se podrá descifrar con la clave privada. Un ejemplo de clave pública sería el número de cuenta de una entidad bancaria. El número de cuenta puede ser facilitado a un tercero para que realice una transferencia o domiciliar un recibo, pero nunca tendrá acceso a los datos, ni consultar saldo ni retirar efectivo de la cuenta. Solo la persona que posea la clave privada podrá realizar esas operaciones.

Validación de las transacciones: Cuando se dice que la red de nodos valida la transacción, se refiere al hecho de que una de las partes autorizadas que conforma la *blockchain*, verifica que la transacción es correcta (por ejemplo, un perito certifica el siniestro) y, una vez verificada, se comparte con el resto de la red de forma

[3] SHA-256 (*Secure Hash Algorithm*): Es un algoritmo criptográfico de *hash* desarrollado por la Agencia de Seguridad Nacional de Estados Unidos (NSA) y el *National Institute of Standards and Technology* (NIST) con el objetivo de generar *hashes* únicos en base a un estándar con el que se pudieran cifrar las comunicaciones. Es uno de los más usados por su equilibrio entre seguridad y coste computacional.

automática. No es necesario que todas las partes involucradas y autorizadas verifiquen la transacción. De esta forma, si el perito ha validado el siniestro, la aseguradora o reaseguradora no tiene que volver a hacerlo, dado que puede acceder a la información de forma automática. Si un perito certificara un siniestro falso, y éste se detectara por el resto de la red, se podrían crear nuevas transacciones para corregir la anterior, pero nunca borrar el posible error o intento de fraude.

GRÁFICO 4 EJEMPLO DE UNA TRANSACCIÓN DENTRO DE UNA RED *BLOCKCHAIN*



LIMITACIONES Y CONCESIONES

Para poner en contexto las posibles limitaciones actuales, hay que diferenciar entre las limitaciones que ofrece el uso de *bitcoin* o cualquier otra criptomoneda y las limitaciones propias de la tecnología *blockchain*.

En el caso de la primera, existen limitaciones que se producen por el propio protocolo, como el tiempo de ejecución de las transacciones (alrededor de 10 minutos). Este tiempo refleja el tiempo medio que los nodos de la red (los 'mineros', en la jerga *bitcoin*) necesitan para validar un bloque, que en este caso se hace a través de la prueba de trabajo ('*PoW*'). Como promedio, se realizan aproximadamente 3 transacciones por segundo en la red *bitcoin*, muy lejos de las 56.000 transacciones por segundo que soporta VISA en su red. Por lo tanto, a pesar de que cada protocolo de *blockchain* establece la velocidad a la que se gestionan las transacciones de cada red concreta, todavía se está lejos de implementar soluciones eficientes a escala mundial.

Otra de sus limitaciones está relacionada con el coste computacional. Con las criptomonedas, en la medida que *PoW* sea más utilizado, la complejidad de minería requerida aumenta, y del mismo modo aumenta el consumo eléctrico para mantener la red segura.

Como limitaciones propias de la tecnología *blockchain* se suelen destacar las siguientes:

- **Escalabilidad**: Cuando se utiliza *blockchain*, cada nuevo registro debe ser validado, lo que significa que la operativa es más lenta que en las bases de datos tradicionales. Cada protocolo debe considerar un equilibrio entre la velocidad de procesamiento de las operaciones, y otros factores como la seguridad de la red, la resistencia ante los ciberataques y el coste computacional. En general, las cadenas de bloques que no utilizan criptomonedas en su operativa suelen ser escalables.
- **Protección de datos**: Bajo la normativa de la UE, los usuarios tienen el derecho a autorizar o a retirar permisos para acceder a sus datos personales a cualquier entidad interesada. Así, cuando una compañía necesita utilizar datos personales para realizar sus estudios, debe solicitar el acceso a la red donde se encuentran dichos datos. Esta autorización deberá solicitarse cuando la compañía necesite datos distintos a los previamente autorizados por el cliente.
- **Vulnerabilidad de la nube**: Los servicios tradicionales en la nube requieren que los usuarios se registren con el proveedor del servicio y, por lo tanto, permiten que esa empresa administre sus identidades y credenciales digitales, hecho que choca con la descentralización que propone la tecnología de la cadena de bloques. Otra limitación sería el caso en que el servidor que gestiona la nube sufriera una caída y no se pudiera acceder a los nodos de la *blockchain*. Es cierto que la limitación no viene dada por el funcionamiento de la tecnología *blockchain*, sino por la propia idiosincrasia de la nube. Por estos motivos, están surgiendo diferentes iniciativas empresariales que proponen un espacio descentralizado y localizado en la nube, permitiendo

alquilar espacios no utilizados de diferentes usuarios y entidades, y en la que un archivo estaría dividido en diferentes localizaciones de forma protegida. De este modo, solo quien disponga de la clave privada puede acceder a la información completa y puede borrarla cuando lo solicite.

- **Confianza en el dato**: Dado que un registro en la *blockchain* es inmutable, una vez integrado en la cadena, no se puede modificar o borrar. Sin embargo, no garantiza que un dato incorrecto haya sido validado inicialmente, por lo que solo puede garantizarse la auditoría a partir de ese momento. Por ejemplo, el kilometraje de un vehículo de segunda mano puede introducirse por primera vez en la cadena cuando el mismo ya ha sido manipulado. La cadena garantiza la consistencia de la información a partir de ese momento, pero la información puede ser errónea en su origen. El protocolo permite establecer que el participante sea responsable y/o el proceso de validación del dato de origen registrado sea correcto.

En definitiva, es relevante considerar todas las limitaciones propias de una tecnología incipiente, para las que se están investigando soluciones gracias al trabajo de diferentes *startups*, compañías tecnológicas y consorcios.

Conclusiones

En la actualidad, las compañías de seguros poseen una visión 'silo' de sus clientes; y el mismo cliente puede ser percibido como un riesgo distinto por las diferentes compañías, sirva como ejemplo la dispersión en las primas ofrecidas para un mismo riesgo de un seguro del automóvil, que es común en muchos mercados.

La cadena de bloques, con sus propiedades de trazabilidad y auditoría, permitiría una mayor transparencia, tanto por la mejora del conocimiento del cliente y de sus necesidades como por el uso que las empresas hacen de los datos de los clientes y cómo influyen los mismos en la personalización de los productos y servicios.

La generación de valor en un futuro cercano dependerá en gran medida de la capacidad de las compañías para incorporarse a ecosistemas digitales, en los que el cliente lidera la relación y elige si se quiere presentar él mismo o a través de otros *partners*. *Blockchain* facilita que el cliente pueda tener control de sus datos, elegir con quién compartirlos y beneficiarse del tratamiento personalizado que permite el acceso a una información nunca antes tan completa. Por supuesto, el uso de la información deberá seguir las directrices de los organismos de protección del consumidor y de privacidad de sus datos.

Aunque en este informe hemos mencionado solo unos pocos casos de éxito conocidos, el uso de la tecnología *blockchain* está madurando y, una vez superadas las etapas de investigación y pruebas piloto, la tecnología se encuentra en la transición a soluciones reales en las distintas industrias.

La industria aseguradora se beneficiaría de la madurez de la tecnología *blockchain*, si bien las ventajas competitivas no vendrían por la mera adopción de la tecnología. En nuestra opinión, la prioridad para las compañías de seguros debería ser mejorar y actualizar sus técnicas de modelización y programación para apoyar la innovación en multitud de áreas diferentes.

En conclusión, creemos que la tecnología *blockchain* tiene el potencial de respaldar una mayor eficiencia y dimensiones comerciales para las compañías de seguros. Por lo tanto, les interesa estar preparadas para su futura adopción una vez que la tecnología haya madurado completamente. Además, la tecnología aumentará el nivel de competencia y son las capacidades tradicionales de la industria las que convertirán los nuevos riesgos y oportunidades en beneficios tangibles para cada negocio.

Referencias

How blockchain could address five areas associated with GDPR compliance. IBM. (2018).

IBM and Walmart: Blockchain for Food Safety. Walmart & IBM. (2017).

Blockchain: Aplicación en el sector asegurador. Ruben Nova. (2018).

Why blockchain and IoT are best friends. IBM. (2018)

https://www.ibm.com/blogs/blockchain/2018/01/why-blockchain-and-iot-are-best-friends/

https://academy.bit2me.com/

Introducing MOBI: The Mobility Open Blockchain Initiative. IBM. (2018)

https://www.ibm.com/blogs/blockchain/2018/06/introducing-mobi-the-mobility-open-blockchain-initiative/

Bitcoin: un sistema de dinero en efectivo electrónico peer-to-peer. Satoshi Nakamoto. (2009)

https://bitcoin.org/files/bitcoin-paper/bitcoin_es.pdf

Insurance Interrupted: How Blockchain Innovation is Transforming the Insurance Industry. Forbes. (2019).

https://www.forbes.com/sites/andreatinianow/2019/01/09/insurance-interrupted-how-blockchain-innovation-is-transforming-the-insurance-industry/#20faf0683ec6

Monetary Statistics. Blockchain Luxembourg. (2017)

https://www.blockchain.com/es/stats

Milliman

Milliman is among the world's largest providers of actuarial and related products and services. The firm has consulting practices in life insurance and financial services, property & casualty insurance, healthcare, and employee benefits. Founded in 1947, Milliman is an independent firm with offices in major cities around the globe.

milliman.com

CONTACTO

José Silveiro
jose.silveiro@milliman.com

Rubén Nova
ruben.nova@milliman.com