uc3m | Universidad Carlos III de Madrid

Máster Universitario en Ciencias Actuariales y Financieras
2016-2018

Trabajo Fin de Máster

"Blockchain: Aplicación en el sector asegurador"

Rubén Nova Rebanales

Tutores:

José Miguel Rodríguez-Pardo del Castillo

Jesús Ramón Simón del Potro

Madrid, Julio 2018

AGRADECIMIENTOS

Durante este trabajo se ha contado con la participación de diferentes personas e instituciones que ha permitido dotar de una mayor rigurosidad este estudio. Por este motivo se ha de agradecer su apoyo y colaboración al profesor Dr. D. Alejandro Balbás de la Corte, a la compañía Marsh & McLennan Companies por permitirme conocer el estado de esta tecnología en el sector asegurador a nivel global, a los tutores de este trabajo José Miguel Rodríguez Pardo y Jesús Ramón Simón del Potro, por guiarme en todo momento en la elaboración de la presente investigación, al profesor Félix Benito Osma por su ayuda en la parte legal, a mi familia por su confianza y constante apoyo y como no, a mis compañeros y amigos del Máster que sin su apoyo en el día a día no hubiese sido posible llegar hasta aquí. ¡¡A todos vosotros, Gracias!!

RESUMEN

La nueva era digital promete transformar la sociedad, y la manera en la que trabajamos. El sector asegurador, de la mano de Insurtech apuesta por la implementación del Big Data, la Inteligencia Artificial, *Machine Learning* y Blockchain. Este trabajo se centra en el estudio de esta última, entendiendo en qué consiste, cómo funciona, qué se está haciendo en el sector actualmente, qué ventajas y desventajas tiene y hacia dónde se dirige en los próximos años.

Además, se han propuesto nuevos casos de uso, y desarrollado uno de ellos, concretamente un seguro por uso para *runners* que permita ver de una forma más visual el valor que aporta esta tecnología a la industria aseguradora. Este seguro, integrado en la arquitectura de la cadena de bloques, los *Smart Contracts* y el *Internet of Things* permite una interacción con el cliente de una forma totalmente disruptiva, tarificando de forma personalizada a su perfil de riesgo, uso del producto, guiando al cliente hacia nuevos hábitos que conduzcan a una mejor calidad de vida y cambiando el paradigma del sector asegurador, afianzando su carácter preventivo, y ofreciendo servicios en base a la necesidad del consumidor.

Este ecosistema supone un reto para la ciencia actuarial, la gran cantidad de datos biométricos y de consumo que puede llegar a tener una aseguradora, la transparencia, la fidelidad del cliente por la eficiencia, el ajuste de las primas, la reducción del fraude y la automatización de las reclamaciones hace que las compañías transformen su operativa tradicional ante una nueva revolución industrial.

Palabras clave: Blockchain, Insurtech, Contratos Inteligentes

ABSTRACT

The new digital age promises to revolutionize society, and the way we work. The insurance sector, together with Insurtech, is committed to the implementation of Big Data, Artificial Intelligence, Machine Learning and Blockchain. Blockchain is going to be the focus of this study. Understanding what it consists of, how it works, what is currently being done in the sector, what advantages and disadvantages it has and where it is going in the coming years.

Additionally, a number of new use cases have been proposed and one of them has been developed, specifically a use insurance for runners that allows a more visual view of the value that this technology brings to the insurance industry. This insurance, integrated into the architecture of the Blockchain, the Smart Contracts and the Internet of Things, completely disrupts customer's interactions experience. This application allows personalized pricing based on the customer's risk profile and use of the product, guiding the customer towards new habits that lead to a better quality of life and changing the paradigm of the insurance sector, strengthening its preventive nature and offering services based on the consumer's need.

This ecosystem is a challenge for actuarial science, the large amount of biometric and consumer data that an insurance company can have, the transparency, customer loyalty for efficiency, premium adjustment, fraud reduction and claims automation makes companies transform their traditional operations in the face of a new industrial revolution.

Keywords: Blockchain, Insurtech, Smart Contracts

Índice

Índice de Ilustraciones

Índice de Tablas

Firmado: Rubén Nova Rebanales

PARTE I: Introducción

1.1. Antecedentes: La era digital

Muchos son los cambios que se dan en una sociedad a lo largo de la historia. La economía mundial ha ido adaptándose según han ido pasando distintas etapas, como la economía de trueque, la revolución industrial, con la llegada de la máquina de vapor, la producción en cadena de Henry Ford, o la aparición de Internet. Estos cambios económicos-sociales han ido moldeando el mundo tal y como lo conocemos hoy.

En la actualidad estamos viviendo una transformación digital que no deja a nadie indiferente. La llegada de nuevos procesos y tecnologías lleva pasando toda la vida. Sin embargo, esta nueva era para muchos llamada "la cuarta revolución industrial", puede acabar con el fin del mundo tal y como lo conocemos. Sobre esto mismo, la periodista de El independiente Marta García Aller ha escrito el libro titulado, "El fin del mundo tal y como lo conocemos" (Aller, 2017).

Ilustración 1 La cuarta revolución industrial

Fuente: Elaboración propia

La autora señala que vivimos ante el final de ideas, costumbres, tecnologías y profesiones que hoy forman parte de nuestro día a día. Por señalar algunos ejemplos Marta García señala que hace 5 años ningún taxista imaginaba que su profesión iba a verse amenazada por unos algoritmos. Y no solo por conductores de Uber o Cabify, sino ante la llegada de flotas de coches autónomos.

Este es sólo un ejemplo de cómo la llegada de nuevas tecnologías y el big data, la inteligencia artificial, el Machine Learning, y el Blockchain pueden cambiar de forma abrupta nuestra profesión y la sociedad de hoy en día.

Brian Krzanich, consejero delegado de la compañía tecnológica Intel se refería a esto en un congreso de San Francisco[1]:

> *"La inteligencia artificial va a actuar de manera similar a como las máquinas de vapor y las fábricas inauguraron la revolución industrial, cambiando cada aspecto de la vida cotidiana. Y va a liberarnos de una amplia gama de tareas, como conducir, combatir incendios, la minería, y muchas más. La Revolución de la Inteligencia estará impulsada por los datos, las redes neuronales y la potencia de la computación"*

Estos cambios se realizan de forma transversal en todas las industrias, desde sectores más tradicionales como los agrícolas donde la llegada de nuevas tecnologías sustituye y/o complementa el esfuerzo humano y la llegada masiva de datos implementa nuevos recursos y controles de calidad y trazabilidad a sectores como la medicina donde la inteligencia artificial y el Blockchain abren infinitas posibilidades que ayudarán al reconocimiento prematuro de enfermedades y a la prevención de las mismas.

La startup Cyrcadia Health ha desarrollado un sensor capaz de monitorizar con sus algoritmos si hay un cambio de forma o temperatura en el pecho de la mujer que se puede llevar cómodamente en el sujetador. Si detecta un cambio sospechoso, rápidamente la avisa para que concierte una cita con el médico. Su tasa de éxito en detección del cáncer es del 80 por ciento. Mejor que la de cualquier humano hasta ahora.[2]

Este nuevo paradigma abre el debate sobre cuestiones que todavía parecen utópicas. El escritor portugués José Saramago en su novela: Las intermitencias de la muerte (Saramago, 2005) señala: "Y al día siguiente no murió nadie", una novela en la que un 1 de enero, de no se sabe de qué año, los humanos dejaron de morir, planteando un problema de tremenda magnitud para la sociedad y un desafío demográfico difícil de imaginar. Esta novela hoy parece hacerse realidad si se cumple los pronósticos del profesor y asesor de la Singularity University[3] que sostiene que en el año 2045 el ser humano será inmortal. El profesor asegura que "en 2045 vamos a tener computadoras con más transistores que neuronas tiene nuestro cerebro. Y ese será el inicio de la singularidad tecnológica, cuando la inteligencia artificial alcance a la inteligencia humana", por tanto, en esa fecha estaremos ante la primera generación inmortal de humanos.

La inteligencia artificial y todas las tecnologías que hoy están surgiendo hará que muchas de las profesiones que hoy conocemos dejen de existir, y el sector asegurador es

[1] Conferencia AI Day Intel, en San Francisco, 21 de noviembre de 2016.

[2] Un equipo de investigadores del MRC London Institute of Medical Sciences ha logrado acertar en un 80 por ciento de los casos los pacientes que vivirían un año más, frente al 60 por ciento obtenido por los médicos, según una investigación publicada en la revista Radiology (febrero de 2017). El uso masivo de los datos juega un papel clave para ayudar a los médicos a prescribir el tratamiento óptimo.

[3] Singularity University, es una institución académica americana creada en 2009 por la NASA y financiada por Google.

un ejemplo de ello, donde según el informe de Accenture Strategy sobre el futuro del trabajo, los vendedores de seguros serán reemplazados al 99% por procesos automatizados o robots en menos de 5 años[4].

A todo lo anterior hay que sumarle como los nuevos dispositivos, smartphones, wearables, y todo lo relacionado con el internet de las cosas (conocido con sus siglas en inglés IOT: *Internet of things*), hace que las compañías se tengan que adaptar para seguir sobreviviendo, y que las empresas que apuestan por implementar estas tecnologías empiezan a tener una ventaja competitiva a tener en cuenta. En capítulos posteriores abordaremos con mayor profundidad estos temas.

Todos estos dispositivos, conectados a internet han hecho posible el Internet de la información que ha cambiado sin duda nuestras vidas. Un ejemplo de cómo cambia el modelo de negocios está en el conjunto de empresas conocido por "GAFA" (Google, Amazon, Facebook y Apple), que han cambiado los modelos de negocio de industrias asentadas durante años y que hoy se están viendo también amenazados por la tecnología y el modelo descentralizado.

1.2. Objetivos

En este trabajo se intentará poner al lector en un escenario de cambio que le permita ver cómo las nuevas tecnologías, el cambio de mentalidad o los comportamientos de los clientes pueden transformar la sociedad, las industrias y finalmente, el sector asegurador.

Con esta investigación se pretende dar respuesta a cómo la tecnología Blockchain puede afectar al sector asegurador. Para ello, hemos realizado un estudio diferenciando entre objetivos primarios y secundarios.

Objetivos primarios:

1. Revisar la literatura que existe hasta el momento sobre la tecnología Blockchain.
2. Explicar el funcionamiento de la tecnología desde un punto de vista técnico.
3. Ver las posibles influencias y aplicaciones que puede albergar esta tecnología en el sector asegurador y cómo este cambio disruptivo cambiará el sector y tal como se conoce en la actualidad.

En cuanto a los objetivos secundarios:

a) Estudiar la repercusión desde el punto de vista actuarial, y como incide la cadena de bloques en los siniestros, los fraudes o el reaseguro
b) Realizar un prototipo de modelo de negocio con esta tecnología desde el paradigma asegurador.

[4] «Digital Disruption: Embrace the Future of Jobs», Accenture Strategy, 2016.

1.3. Aportaciones que hace el trabajo

Durante la presente investigación se ha revisado la literatura que existe de esta tecnología, se ha estudiado su funcionamiento y sus diferentes casos de uso. Las aportaciones de este estudio se reflejan en los siguientes resultados:

- La investigación sobre el concepto, la revisión de la literatura nacional e internacional establece una aproximación al entendimiento de la tecnología y permite ver cómo está evolucionando en los últimos años.
- Se muestran los trabajos más influyentes, los diferentes estudios en la industria de forma global, mostrando una visión holística de la aplicación de la tecnología.
- Se ha estudiado la aplicación de la cadena de bloques al sector seguros, citando a los diferentes consorcios, permite ver que se está haciendo en el sector y ofrece al lector de una visión real de esta tecnología en el sector.
- Se proponen nuevos casos de uso de la cadena de bloques y nuevos productos que transforman el sector y la profesión actuarial.
- Se hace un prototipo que permita ver el alcance que puede llegar a tener este ecosistema y cómo impacta en el sector asegurador-actuarial.
- Además de todo lo anterior, la revisión de la literatura y el esquema bibliométrico es una aportación por sí misma.

1.4. Estructura

La estructura del presente trabajo se divide en siete partes que se subdivide en varios apartados. El primero es introductorio, en él mismo se presenta el problema de la investigación, los antecedentes, la justificación de este estudio, se plantean los objetivos, su estructura y se muestra la metodología que sigue este trabajo.

En la segunda parte se presenta los fundamentos teóricos de la investigación, que a su vez consta de varios apartados, revisamos la literatura sobre la tecnología Blockchain, se explica su funcionamiento, tipos de cadena de bloques y se hace un estudio de cada una de las partes que integra esta tecnología.

En el siguiente apartado se hace un posicionamiento al lector de la situación actual del sector Fintech e Insurtech, se detallan los diferentes consorcios, aplicaciones de uso de la cadena de bloques en el sector asegurador, ventajas e inconvenientes y previsiones futuras.

En el cuarto bloque se muestran los aspectos legales, se estudia el impacto de la nueva normativa de protección de datos GDPR, y se explica el funcionamiento del marco regulatorio del Sandbox.

En el quinto bloque, se hace una propuesta de producto en el mercado, si es necesario usar tecnología Blockchain, se muestra un prototipo del mismo y se tarifica según las hipótesis establecidas.

En el sexto, se presentan las conclusiones, teóricas y prácticas, las limitaciones que se han presentado y las futuras líneas de investigación.

En el séptimo y penúltimo apartado se mostrará la bibliografía que se ha seguido para llevar a cabo la investigación y se dará paso a los anexos donde se incluirá el código de programación que se ha realizado para la parte empírica del trabajo.

1.5. Metodología

La metodología de esta investigación se divide entre los fundamentos teóricos y el planteamiento actuarial.

Respecto al primero, este trabajo se ha apoyado en los diferentes informes y estudios de investigación que se irán citando a lo largo del trabajo, y asistencia a diferentes congresos, talleres y cursos que permitan adquirir los conocimientos técnicos necesarios para la realización de este trabajo y conocer de una forma más directa qué se está haciendo con respecto a la tecnología objeto de este estudio.

En cuanto a la parte actuarial, para la extracción de los datos, se ha tenido en cuenta diferentes estudios también señalados a lo largo del trabajo y estadísticas oficiales como las del Instituto Nacional de Estadística y la encuesta de Hábitos deportivos.

Respecto al tratamiento de los datos descriptivos, se ha utilizado el programa Microsoft Excel 2016, que ha permitido sacar unas primeras conclusiones prácticas, así como la realización de gráficos para una mejor visualización de estos.

En cuanto al cálculo de la prima se ha realizado utilizando el lenguaje de programación Visual Basic (VBA), teniendo en cuenta el uso por horas del seguro contratado a través de un contrato inteligente.

PARTE II: Fundamentos Teóricos

2.1. ¿Qué es Blockchain?

Para hablar de Blockchain es de obligado cumplimiento hablar de Bitcoin, dado que esta tecnología subyace de esta criptomoneda. Bitcoin es una red abierta y consensuada entre nodos independientes que permite un nuevo sistema de pago de forma completamente digital que permite enviar dinero por todo el mundo, sin la intervención de bancos o intermediarios. Es la primera red entre P2P[5] de pago descentralizado impulsado por sus usuarios de una forma descentralizada, es decir, sin terceros, intermediarios o una entidad central que controle la red. Bitcoin es, por tanto, conocida como la primera moneda digital o "criptomoneda", La primera especificación del protocolo Bitcoin y la prueba del concepto la publicó en su *White paper* Satoshi Nakamoto en el año 2009 en una lista de correo electrónico. Satoshi abandonó el proyecto a finales de 2010 sin revelar mucho sobre su identidad. Hay varias teorías: desde que son un grupo de personas bajo ese seudónimo o que podría tratarse de un estudiante de la *Trinity College* de Dublin. (Nakamoto, 2008)

¿Quiere decir esto que bitcoin y Blockchain es lo mismo? No, la red Bitcoin comparte una contabilidad pública bajo la tecnología "Blockchain". Este libro mayor de cuentas contiene transacciones que son procesadas, permitiendo verificar la validez de cada una de ellas. La autenticidad de cada transacción está protegida por firmas digitales correspondientes a cada dirección de envío, permitiendo a todos los usuarios tener control total al enviar bitcoins desde sus direcciones Bitcoin. Hay que diferenciar Bitcoin con B mayúscula y minúscula, dado que la primera se refiere al nombre del protocolo y la segunda a cada uno de los tokens o moneda digital bitcoin.

[5] Peer to Peer es un término que se utiliza cuando una red de nodos que se encuentran conectados directamente en una misma red. Su traducción al español sería "red de pares" y cuya esencia consiste en la organización entre iguales. Un ejemplo de conocido en la red Bitorrent.

Ilustración 2 Capas de la Red Blockchain

Fuente: Elaboración propia

Blockchain surge por primera vez en 1998 por Wei Dai en la lista de correo electrónico "cypherpunks"[6], donde propuso la idea de una nueva forma de pago que utiliza la criptografía para controlar su creación y las transacciones, en lugar de que lo hiciera una autoridad centralizada, aunque no es hasta 2008 cuando Satoshi Nakamoto ve su potencial y la utiliza para lanzar Bitcoin. (Nakamoto, 2008)

Existen diferentes definiciones y posturas existentes sobre Blockchain, entre las que podemos encontrar:

- Blockchain es una base de datos distribuida por nodos de la cadena, protegidos criptográficamente, relacionados entre sí, entre los participantes de la cadena.
- Es una tecnología que nos permite interactuar entre dos o más intervinientes, transforma intermediarios, y genera confianza entre los intervinientes.
- Una cadena de bloques es el registro maestro de las transacciones que se producen en una red, que es compartida por todos los elementos de la red distribuida. Garantiza que cada participante tiene la misma copia exacta y que, una vez incorporada una transacción, no es posible borrarla de la cadena de bloques.
- Una Blockchain es una red global de ordenadores que gestionan una gigantesca base de datos, de forma descentralizada, abierta al público, que permite que partes que no confían plenamente entre sí, puedan mantener mediante consenso, una única verdad, sin necesidad de una entidad central.

[6] . El término Cypherpunk proviene de la unión las palabras Cypher (clave, cifra, código criptográfico) y punk, y se incorporó al Oxford English Dictionary en el año 2006. Este movimiento, en el cual se encuentran personas como Julian Assange (Responsable de Wikileaks), escribieron el libro La libertad y el futuro de Internet en el año 2012.

¿Qué nos permite hacer una red Blockchain?

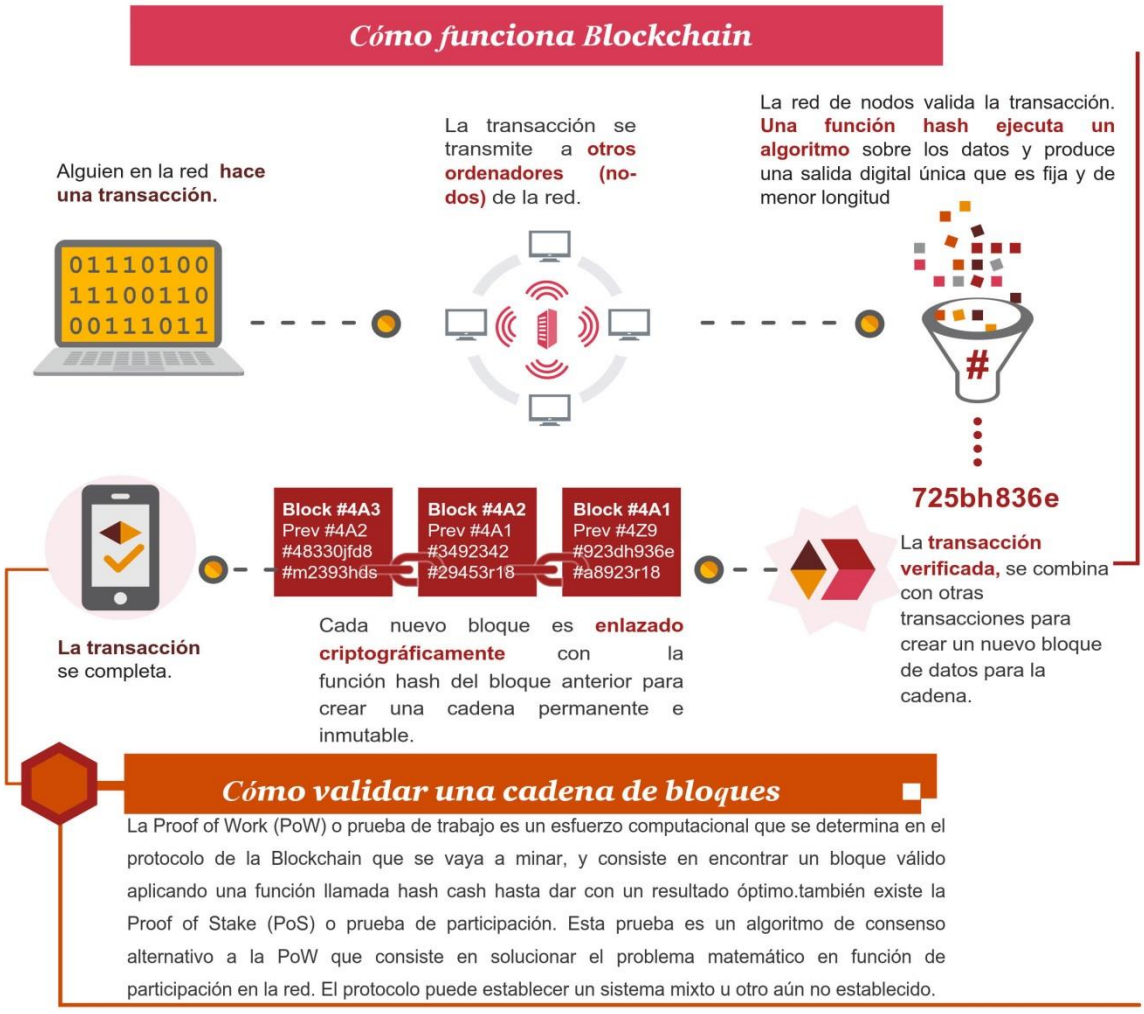
Blockchain es una gran red de ordenadores interconectados en los que se comparte una única base de datos con todos los registros contables en miles de ordenadores a la vez. Esto crea un gran registro compartido, distribuido, en el que no hay una entidad central de control, en el que no hay nadie responsable de mantener ese registro, sino que son los propios usuarios de la red los que se encargan de mantenerlo, y que lo hace seguro dado que la tecnología, por sus propias características, y como más delante se explica, lo asegura mediante la existencia de una base matemática y criptografía. Por tanto, la cadena de bloques nos permite hacer una transacción, de forma segura, de forma inmutable, que nadie pueda cambiar el registro de esa transacción, dado que, si alguien lo hace, el resto de ordenadores va a detectar que ha habido un cambio en ese nodo respecto con los que tienen la mayoría de ordenadores y por tanto, salta la red de alarma y lo van a calificar como fallo del sistema y registro no válido, lo que aporta seguridad dado que la misma verdad está registrada en todos los ordenadores, es trazable lo que significa que podemos encontrarla de nuevo, por ende, saber quién la hizo y es de forma automática. Este hecho es absolutamente revolucionario.

Por poner un ejemplo gráfico en un sistema de pagos, si vamos hacer un pago nacional o internacional entre un comprador y un vendedor, hay una relación de comunicación entre las partes, pero todo lo que supone un elemento transaccional, tiene que suceder offline y para ello necesitamos intermediarios, porque las relaciones transaccionales necesitan confianza, que aportan entidades como personas, empresas, Bancos, Bancos centrales, Visa, PayPal…que son la capa de transacción que dan confianza esta transacción… dado que el vendedor y el comprador no tienen por qué conocerse. Sin embargo, en el internet del valor, se pueden sustituir todos estos intermediarios por la propia tecnología, automatizando ese proceso y haciendo posible que la relación entre las partes en la transacción, se produzca P2P, de persona a persona, haciendo posible que terceros no tengan que intervenir, lo que supone una eficiencia y de automatización de este proceso, de ahorro, … que hacen que muchos denominen a Blockchain como "La máquina de la verdad", dado que supone un gran libro contable, de registros, en el que apuntamos cada una de las transacciones, en el que todos los participantes se ponen de acuerdo en que la verdad está en ese gran libro de cuentas. Nadie pone en duda la existencia de ese registro, y todo lo que contiene esa transacción o nodo de la cadena, se considera verdad por las dos partes, lo que quiere decir que existe confianza. Esto se consigue porque la tecnología hace que todo lo que está ahí registrado no sea manipulable, modificable, y todas las partes se lo creen, y por esto se puede operar persona a persona (P2P), lo que permite operar de forma directa.

La distribución es en sí misma un factor de disponibilidad y escalabilidad. Permite la supervisión directa y enlazar información externa asegurando, la inalterabilidad de dicha información. Estas características habilitan un escenario de absoluta innovación social y económica, transformando lo que se conoce como el Internet de la información (Internet tal y como hemos conocido hasta ahora) al internet del Valor.

En cuanto a la escalabilidad, es un término que se refiere a la capacidad que tiene un sistema de adaptarse a medida que sube el rendimiento del mismo sin que se vea comprometido su funcionamiento. En el caso de una Blockchain podría decirse que la escalabilidad del sistema es la capacidad que tendría el sistema de poder añadir más nodos en función de la demanda de este. Puesto que es una tecnología totalmente descentralizada, esta cualidad debe de estar integrada en el diseño de la Blockchain, y es un requisito muy necesario para su correcto funcionamiento. Por regla general, las Blockchain, como por ejemplo Ethereum (privada) o Hyperledger Burrow, son bastante escalables.

Ilustración 3 Funcionamiento de una transacción en Blockchain



Fuente: Elaboración propia

2.2. Blockchain Publicas y Blockchain Privadas

Un protocolo define un estándar común para definir la comunicación entre los participantes de la red. Estos protocolos pueden darse bajo dos grandes grupos, Blockchain públicas y Blockchain privadas. Existen también las Blockchain híbridas, llamadas Blockchain semi-permisionadas.

Aunque la cadena de bloques nació como una Blockchain pública, esta puede definirse dependiendo de las aplicaciones de uso que se quiera dar.

Una Blockchain pública define el protocolo abierto a todo usuario que puede acceder, consultar y validar las transacciones realizadas. Las transacciones que se registran en la Blockchain públicas muchas veces se denominan *tokens*. Es un sistema *open source*, y cualquier puede ser juez y parte, gestionado bajo normas de consenso.

Algunos ejemplos de cadenas de bloques públicas son: Bitcoin, Ethereum, Litecoin…

El *token* es una cadena de caracteres alfanumérico que representa un activo, cualquier cosa susceptible, puede ser un servicio o un intangible. En otras palabras, un *token* es una unidad de valor digital emitida por una compañía o institución privada. Se representan en una cadena criptográfica que tienen una clave privada y una clave pública. Esta clave pública seria la que correspondería a una cuenta bancaria, y una clave privada puede ser el pin de acceso a esa cuenta. Por ejemplo, una cadena alfanumérica como 5H98DFC-Pmzc34QviMnenRHLYntVRsTy, que representa un registro en la base de datos descentralizada y que debe ser aceptada por consenso dentro de la Blockchain.

La tecnología permite que no todos los participantes puedan acceder y consultar las transacciones, si no que permite una Blockchain privada, cerrada, distribuidas y anónimas.

Esto significa que solo los participantes autorizados pueden acceder a los datos inscritos en la Blockchain, y según establezca su protocolo les permitirá el registro de transacciones en la cadena y/o poder verificar los cambios producidos en la red, aunque el código utilizado sea público. Esta circunstancia hace que una Blockchain privada esté más centralizada, con un número de nodos limitados según el protocolo y que pueden definir los mecanismos de consenso que se aplicará en la red.

Estas iniciativas se conocen con sus siglas en ingles DLT (*Distributed Ledger Technology*), en castellano, Libro Mayor Distribuido, que significa una base de datos gestionada por un grupo limitado de usuarios.

Las Blockchain privadas surgieron entre los años 2014-2015 y son la gran apuesta del sector financiero y otros sectores regulados que por razones de confidencialidad, política o cuestiones legales no pueden compartir sus bases de datos. Estas han recurrido a sistemas de financiación clásicos, como pueden ser inversiones en empresas

de capital riesgo o a través de consorcios (que se hablará más en capítulos siguientes). Las empresas que están invirtiendo en este modelo están surgiendo con el propósito de adelantarse al futuro y tener ventajas competitivas en sus industrias y para reinventar sus modelos de negocio. A raíz de esto, están surgiendo consorcios de empresas (que veremos más detalladamente con posterioridad), y que son claro ejemplo de Blockchain privadas.

A modo resumen, las diferencias entre una Blockchain pública y una privada es que la primera es descentralizada, en el que cualquier persona puede participar de forma libre, y en la Blockchain privada (conocida también como Blockchain permisionada), es distribuida donde el número de usuarios es limitado. En ambos casos, las transacciones que se registran en la red cumplen las características de una Blockchain, por lo que las anotaciones realizadas permanecen de forma inalterable.

También existen las Blockchain híbridas que son una mezcla de las dos anteriores. Las propiedades de esta Blockchain recaen en que para hacer transacciones en esa red debes ser partícipe de la red o ser invitado, aunque las transacciones pueden ser visibles para todos los usuarios, seas o no participante. Ejemplos de este tipo de Blockchain son BigchainDB, un proveedor de tecnología Blockchain, o Evernym, que se le conoce como *Self Sovereign Identity*, una startup que quiere facilitar la gestión de la Identidad Digital Soberana.

Ilustración 4 Bases de datos

Fuente: Blockchain España

2.3. El modelo descentralizado

El cambio de pensamiento de la sociedad es algo que suele ocurrir con bastante frecuencia. Por eso, se habla de que el mundo está en constante movimiento, experimenta cambios estructurales, de pensamiento y manera de hacer las cosas. Esto ocurre por supuesto en las empresas. Cuando se produjo la revolución industrial, se aplicó un modelo de control de la organización y de mando que perdura en la actualidad donde las grandes empresas controlan en gran medida la actividad económica y regulatoria en la sociedad en la que vivimos.

En estos momentos, en muchos foros de discusión se está hablando de una nueva revolución industrial, la revolución 4.0 en el que pasaremos de un modelo jerárquico y centralizado a un modelo descentralizado, donde se dará importancia a la autogestión, el autoconocimiento, la integridad, la autorregulación, ética y comportamientos altruistas, llevado a términos del Blockchain, se puede decir que seremos nodos dentro de nuestra red que es el mundo en el que vivimos.

El modelo de descentralización no es algo nuevo. Muchas empresas han intentado de una manera u otra instaurar modelos de negocio que no dependan de autoridades centrales.

Un ejemplo de este modelo es VISA, su fundador Dee Hock, en 1970 fue nombrado director ejecutivo de National BankAmericard, que más tarde se convirtió en VISA, en la que apostaba por una red descentralizada en la que bancos de todo el mundo y empresas individuales se unen para lograr un movimiento monetario a nivel mundial que beneficia a todos los partícipes.

Visa no es una compañía que se dedica a fabricar no vende tarjetas o terminales TPV por los que se pasan, ni mueve dinero como mucha gente puede llegar a pensar, sino que es una red de telecomunicaciones que envía mensajes de pago por todo el mundo y que garantiza las transacciones que son ejecutadas en la red y en la que existe confianza entre Bancos e individuos que la operación se hará sin fraude. Hock explica en su biografía *One from many* (Hock, 2005) como desde sus inicios profesionales quiso alejarse de empresas rígidas, que ahogan la creatividad del trabajador, y que entorpecen los nuevos retos y oportunidades.

Este paralelismo con la red Blockchain, ha provocado que el creador de VISA apueste fuertemente por esta tecnología y se unió al consejo asesor de la startup Bitcoin Xapo, una de las empresas más importantes del ecosistema Bitcoin.

Esta fuerte inversión en tecnología Blockchain supone un cambio de paradigma, en el que se intenta construir un sistema económico y empresarial abierto, alejado de entes centrales, totalmente transparente y que garantice el anonimato. Este cambio de paradigma no es solo un cambio tecnológico, sino cultural, donde los usuarios están

cansados de instituciones y empresas opacas, la corrupción y bajo el mando de entes centrales o terceros, donde se apuesta por la soberanía monetaria.

Blockchain supone eliminar a esos entes centrales dotando de operabilidad entre pares (P2P), que garantiza transparencia, la eficacia, el doble gasto y el cumplimiento de las condiciones pactadas en los contratos inteligentes. Todo esto debe estar apoyado dentro de una regulación que permita esta transformación, en la que las empresas e instituciones tendrán que adaptarse para poder interactuar en la nueva sociedad que se está creando.

Un aspecto importante es la confianza, al ser una transacción *Peer to Peer*, las partes tienen que tener la confianza de cumplimiento entre ellos. Entonces, ¿Cómo o quién proporciona confianza en la red Blockchain? Así como en los casos de VISA o PayPal son compañías que han tenido éxito debido a la confianza que existe en el mundo, en este caso son empresas centralizadas, creemos que no se puede hackear por lo que nos aporta esa seguridad y está sujeta a las leyes de los reguladores, Blockchain tiene su propia idiosincrasia.

La confianza se establece por consenso dado que los usuarios que no se conocen entre sí, puedan establecer un consenso que permitan que todos los usuarios que existen en la red puedan confiar que la información que se encuentra en ella. Esta confianza se construye, desde el punto de vista técnico, a partir de una red global de ordenadores conectados entre sí, ya sea una Blockchain pública o privada, estos pueden consultar, crear o verificar cualquier transacción que ocurre en la red y en caso de que un usuario intente modificar uno de los nodos de la red, el resto de los usuarios verán que este no está conectado con el nodo anterior y que su hash es diferente, hecho que provocará que los usuarios lo rechacen de forma masiva y que no se una a la cadena. En este proceso computacional se le une la parte criptográfica, o la llamada “minería de datos”, términos que se detallaran en páginas posteriores en este trabajo.

2.4. Criptografía

La criptografía es un elemento básico de la cadena de bloques. La criptografía según la Real Academia Española es “arte de escribir con clave secreta o de un modo enigmático”, y tiene por objetivo cifrar un mensaje o contenido.

Actualmente hay tres tipos principales de criptografías:

- Hashes o función resumen
- Criptografía simétrica
- Criptografía asimétrica

2.4.1. Hashes o firma digital

La función hash también llamada función resumen o *digest*, consiste en aplicar una función matemática a unos datos con el objetivo de obtener una secuencia de datos fijas, normalmente 256 bits, lo que hace que se acorte mucho la longitud del mensaje. Siempre que se aplique la misma función al mismo bloque, obtendremos 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. Una característica importante de las funciones resumen es que son unas funciones criptográficas irreversibles, esto es una vez obtenido un resultado es muy difícil volver a su posición original. Al ser unidireccionales y al tener un tamaño el hash menor que el mensaje de entrada, podrían existir diferentes caminos para llegar al nodo raíz. Por poner un ejemplo práctico, imaginemos la multiplicación de dos números primos en centenas: 577 y 823, la multiplicación de ambos números obtiene un resultado de 474.871, si queremos invertir esa multiplicación y llegar a los dos números primos originarios es un algoritmo difícil de conseguir.

El objetivo del hash es el de comprobar y verificar la integridad del contenido del bloque, no ocultar el mensaje en sí. Estas funciones tienen varias características:

- **Eficiencia de cálculo:** tiene un bajo coste y se generan rápidamente.

- **Resistencia pre-imagen:** computacionalmente es complejo conseguir un mensaje de entrada que produzca una función resumen predeterminada, es decir, que pueda prever el hash que se va a generar con un mensaje de entrada.

- **Resistencia a la segunda pre-imagen y a la colisión:** Es computacionalmente muy complicado crear dos mensajes distintos que den la misma función hash.

La función hash o función resumen convierte un mensaje en un código hexadecimal, actualmente compuesto de los números del 0 al 9 y las seis primeras letras del abecedario (de la letra A a la letra F). Cada pareja de caracteres forma un byte[7] y todas las parejas posibles (16 x 16) que representa 256 posiciones decimales. Un ejemplo práctico puede ser el siguiente:

Mensaje	**Hash (Hexadecimal)**
Madrid	5CDC4F3FEB47CB81
De Madrid al cielo	87DA2D3BCB47CBE1
De Madrid al cielo.	20DFC48EFE51BE84

Como puede verse un minúsculo cambio en un mensaje obtiene un hash completamente diferente. Cada protocolo establece el tipo de tecnología criptográfica que se aplicará. Por ejemplo, Bitcoin utiliza dos tipos de algoritmos hash: SHA-256 como función hash principal o RIPEMD-160 en el proceso de creación de direcciones.

[7] Unidad mínima de memoria computacional que consiste en la secuencia de ocho ceros y unos.

El primero de ellos SHA-256 está diseñado por la Agencia de Seguridad Nacional de los Estados Unidos. SHA viene de sus siglas en inglés *Secure Hash Algorithm*. En cuanto a RIPEMD-160 viene de las siglas inglesas de RACE *Integrity Primitives Evaluation Message Digest*, y se utiliza cuando se requiere una longitud menor de la función resumen (Preukschat, 2017).

2.4.2. Criptografía simétrica

La criptografía simétrica utiliza una única clave tanto para cifrar como para descifrar. El problema de esta criptografía es que cualquiera que conozca su clave puede descifrar el mensaje.

Hay que hacer una distinción entre claves y contraseñas. Las contraseñas están pensadas para que cualquier usuario pueda recordarlas y las claves sin embargo se generan de forma aleatoria. Esto hace que la primera sea más fácil de vulnerar. Muchas veces se utilizan las contraseñas para guardar una clave. En el ecosistema de criptomonedas, existen unos hardware para guardar las claves y evitar la pérdida de estas monedas virtuales llamados *Hardware wallets*.

El algoritmo más usado para para el cifrado de con clave simétrica es AES (*Advanced Encryption Standard*) que utiliza 2^{256} combinaciones de ceros y unos de forma aleatoria. Ejemplo:

1111000100001100110000011101110000000101111110110111010110000010111100
1101001101100111110010001111010100011100011100100101000001000000010101
0000011100100111101011001011101010000110000001111000011110001100000110
1010110111001101111010111000110100100000010

Para hacernos una idea de las combinaciones posibles, la clave anterior equivale a un número decimal de 77 dígitos de largo. Las claves AES 256 son tan seguras que, para poder recorrer la mitad de las claves, se necesitaría la fuerza de 10^{38} superordenadores, que consumirían una energía equiparable a 150 centrales nucleares, funcionando un tiempo equivalente a la actual edad del universo.

2.4.3. Criptografía asimétrica

La criptografía asimétrica, utiliza dos claves: una pública y otra privada. Ambas interaccionan entre sí, dado que la clave pública se crea a partir de la clave privada que se ha generado de forma aleatoria.

La clave pública la podemos compartir con cualquier usuario, pero la clave privada tenemos que mantenerla oculta al resto de personas. Para que se entienda mejor, extrapolamos estas claves a una operación bancaria, la clave pública podría ser los 20 dígitos de una cuenta bancaria, mientras que la clave privada es el pin con el que aprobamos las operaciones.

El algoritmo usado por Bitcoin es el llamado *Elliptic Curve Digital Signature Algorithm* (ECDSA), un número aleatorio de 256 bits (ceros y unos), representado en el sistema hexadecimal comentado anteriormente.

La criptografía de curva elíptica proporciona una mayor seguridad que el resto de los algoritmos y además es más eficiente, rápida y escalable. La ecuación que utiliza este algoritmo es el siguiente:

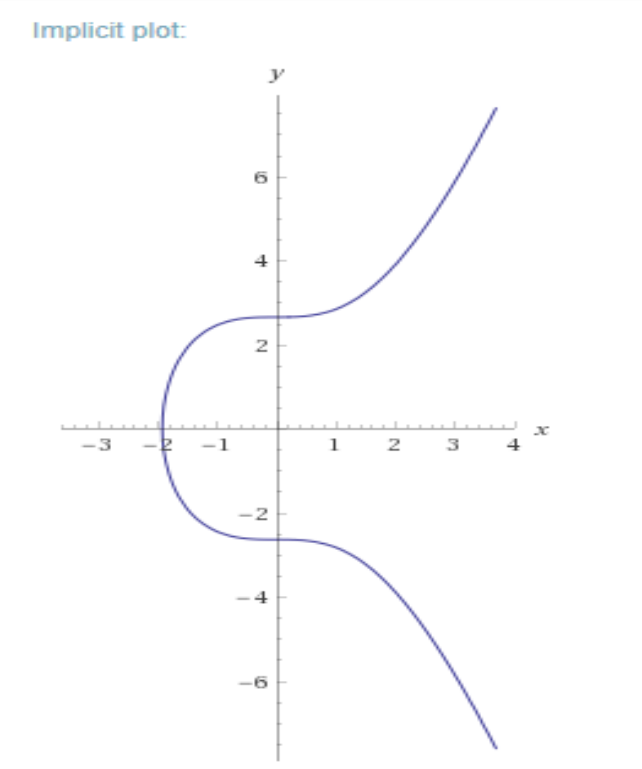
$$y^2 = x^3 + ax + b$$

La curva eliptica usada por Bitcoin sustituye los valores a = 0 y b = 7, quedando su función:

$$y^2 = x^3 + 7$$

Cuya representación gráfica es la siguiente:

Ilustración 5 Representación de curva elíptica



Fuente: Elaboración propia aplicando fórmula $y^2 = x^3 + 7$

Los algoritmos de curva elípticas consumen diez veces menos memoria que otros algoritmos y más rápido, motivo por el que Satoshi Nakamoto lo estableció en el protocolo Bitcoin.

Cuando realizamos una transacción, hay tres elementos claves que actúan en el proceso:

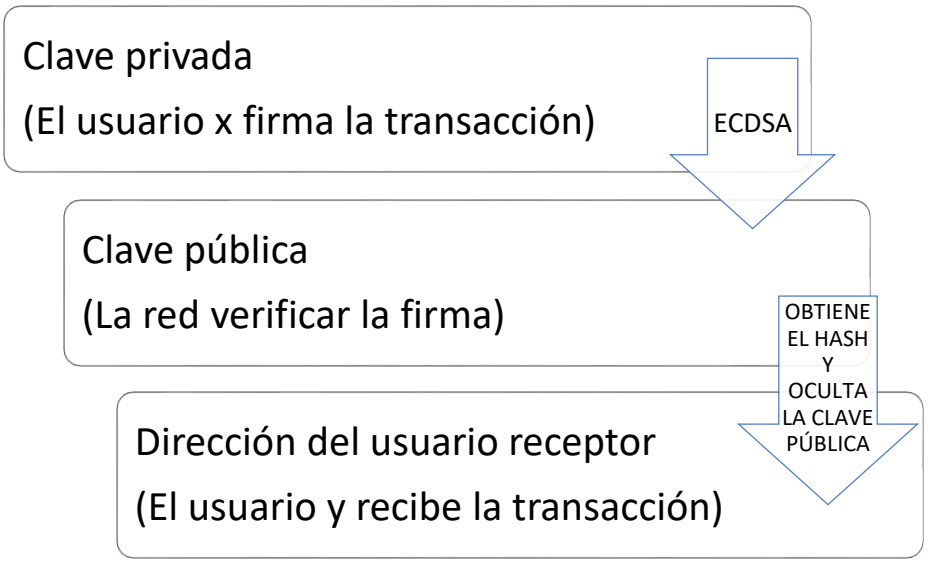
I. **La clave privada:** que siempre debe ser secreta. Esta clave es un código de 256 bits que consta de 64 caracteres. Un ejemplo de clave privada podría ser:

52F21E7B6A307E426A94BE3147045F9F445321AD03SP61F20BD67FC2EB2129C2

II. **La clave pública**: es secreta hasta que se hace una operación. Un ejemplo de clave pública:

21C8Zk4Bla61ogTj2f121MCyQ84AxnB2ae

III. **El hash o función resumen** que siempre es público.



2.5. Minería

Hasta el momento hemos estado hablando de transacciones, nodos, hash… pero ¿qué son realmente? ¿Cómo funciona esta tecnología? Para entenderlo bien hay que volver necesariamente a la primera red pública creada por Nakamato, Bitcoin. Hoy todavía modelo de referencia de muchas Blockchain. El 31 de Octubre de 2008 un usuario, hasta entonces desconocido, publicó un anuncio en una lista de correo de la página web www.metzdowd.com dedicada a criptografía, en el que permitía hacer transacciones y proteger sus activos mediante el empleo de criptografía de clave asimétrica y validar por

consenso de las partes con el mecanismo conocido con su término en inglés *Proof or work* o prueba de trabajo traducido al castellano, donde ya no sería necesario la certificación de un tercero para validar la transacción.

Nos situamos entonces en el 12 de enero de 2009, donde dos usuarios, Satoshi Nakamoto y Hal Finney[8] ejecutan a modo de prueba la primera transacción en Bitcoin para verificar que el software publicado unos días antes, ejecuta correctamente su protocolo. Para ello, en el bloque 170, Satoshi emite 10 bitcoins que irán a parar al wallet[9] de Hall. En esos momentos tan solo es una prueba, dado que la moneda digital no tenía ningún valor. La operación se hace para validar si los nodos de la red, el minero encargado de realizar la prueba de trabajo, y el monedero electrónico funcionan correctamente. (Preukschat, Blockchain: La revolución industrial de internet, 2017)

En ese momento la red está compuesta por catorce nodos conectados a internet en cualquier parte del mundo, que han instalado el software publicado por Satoshi. Cuando arranca la aplicación ese nodo, mediante varios mecanismos (como pueden ser por direcciones IP, peticiones DNS[10] o usando direcciones que tiene codificados ciertos nodos), busca otros pares y el puerto por el que se comunican. Tras descubrir uno o varios pares, y unirse a la red, este nodo pide a sus pares una copia de toda la cadena de bloques, y de esta forma procede a la verificación de la propiedad de las criptomonedas. Así se va formando la red, en este caso como hemos mencionado, con 14 nodos.

A cada unidad que forma la cadena se le conoce como "bloque". Este bloque consta de dos partes: la cabecera del bloque[11] y el Merkle Tree (o árbol de Merkle) de las transacciones o datos de valor, dependiendo de la Blockchain que estemos utilizando. La cabecera del bloque está formada por el hash del bloque anterior, por el "nonce", el cual es un campo de 32 bits (4 bytes) cuyo valor se determina de manera que el hash del bloque contenga una serie de ceros, cualquier cambio en el nonce hará que el hash del bloque sea totalmente diferente, utilizado como veremos más adelante para la prueba de trabajo de los mineros, y el hash raíz del árbol de Merkle de todas las transacciones incluidas.

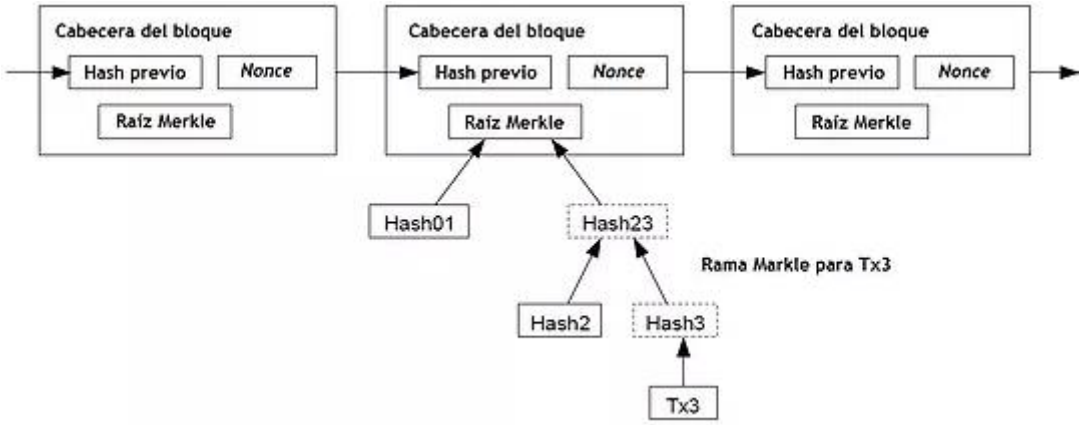
[8] Criptógrafo de PGP Corporation

[9] Los wallets o monederos electrónicos te permiten recibir, almacenar y enviar todo tipo de bitcoins y resto de criptomonedas. Hay muchos tipos de wallets y tienen diferentes características, sería parecido a lo actualmente es una cuenta bancaria.

[10] DNS o Sistema de peticiones de dominio es un sistema descentralizado que asocia información a los dispositivos conectados a redes IP y traduce los nombres de dominios a direcciones numéricas.

[11] Cada cabecera del bloque contiene el hash de la cabecera del bloque anterior, y también es utilizado para conformar la cabecera del bloque sucesor, y así se va formando la cadena, hecho que provoca el origen del nombre de cadena de bloques, conocido con su término inglés Blockchain.

Ilustración 6 Hasheado en un árbol de Merkle



Fuente: Bitcoin: A Peer-to-Peer Electronic Cash System, Satoshi Nakamoto

Satoshi en el bloque cero (conocido como bloque Génesis) incluye el texto "*The Times 03/Jan/2009 Chancellor on brink of second bailout for Banks*" que traducido al español significa "The Times 03/Ene/2009 El Canciller al borde del segundo rescate para los Bancos"[12] haciendo toda una declaración de intenciones.

En ese momento, cada nuevo bloque que se añadía a la cadena era recompensado por 50 nuevos bitcoins que se emitía en ese momento. Esta recompensa cambia cada 4 años dividiéndose a la mitad, por lo que hoy la recompensa por generar un nuevo bloque (lo que se conoce como minería[13]) son 12.5 bitcoin por cada bloque minado. Hay que subrayar que cuando se emitió el libro blanco del protocolo Bitcoin, Satoshi estableció un máximo de 21 millones de bitcoins. A fecha de mayo de 2018 hay en circulación 17.019.512 BTC[14] (BTC son las siglas con las que se denomina bitcoin, al igual que € al euro). Para que estos bitcoins lleguen a tu cuenta, la cadena requiere que conste al menos de 100 bloques de maduración, para evitar situaciones de pagos no aceptados (Preukschat, 2017).

Una vez que todos los nodos sincronizados han validado la transacción, el dinero electrónico llega a la dirección de envío. Este dinero electrónico puede definirse como una cadena de firmas digitales en la que los propietarios transfieren la propiedad firmando digitalmente una función hash junto con la dirección de envío correspondiente. Una vez realizado este proceso, con la clave pública del propietario se da a conocer al resto de participantes los fondos que se quieren transmitir para que lo verifiquen el resto de los participantes y den por válida la transferencia de estos fondos, comprobando que el emisor es el dueño legítimo, en este caso de los bitcoins transferidos.

[12] La frase escrita por Satoshi Nakamoto se refiere a una nota de prensa de la misma fecha que mencionaba al entonces ministro de Hacienda de Reino Unido, Alistair Darling.
[13] Al proceso de minería se le conoce con ese término emulando a la creación del oro en una mina.
[14] https://info.binance.com/currencies/bitcoin

En el caso de los 10 bitcoins transferidos de Satoshi Nakamoto a Hall Finney, Satoshi envía a la dirección 12cbQLTFMXRnSzktFkuoG3eHoMeFtpTu3S de Hal, firma con su clave privada e incluye su clave pública para que el resto de los nodos puedan verificar que es legítimo propietario y por tanto está autorizado para emitir la transferencia de esos fondos. A continuación, se retransmite el conjunto de datos a los pares conectados a su nodo y estos repiten el proceso al resto de pares que desconocen la transacción hasta que toda la red esté cubierta (Preukschat, 2017).

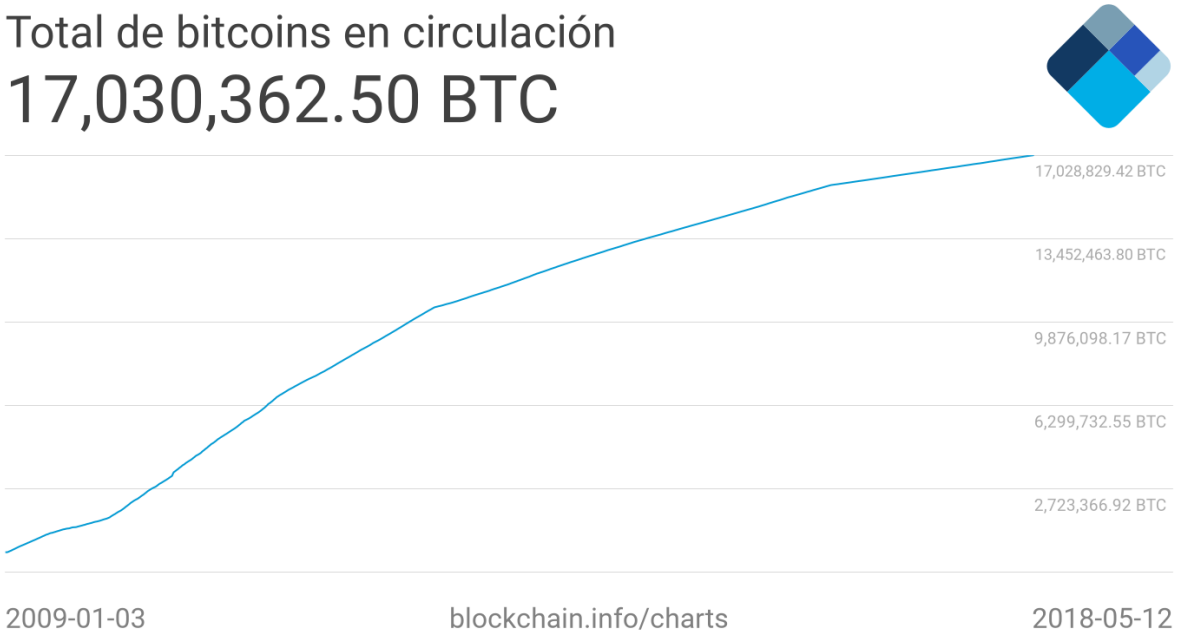
A partir del momento que los nodos reciben la transacción empieza la competencia para generar un nuevo bloque válido para la cadena y tener la recompensa comentada anteriormente además de los *fees* establecidos. El tiempo de procesamiento de estos bloques se estableció en el diseño de la red, de forma que el esfuerzo computacional para minar un nuevo bloque fuera, de media, 10 minutos. Estos bloques al seguir una distribución de probabilidad Poisson, el tiempo medio será siempre de 10 minutos, independientemente de cuando se haga el anuncio del nuevo bloque, dada la propiedad de la Poisson de falta de memoria.

Cuando la potencia de cálculo de la red aumenta, disminuye el tiempo en que se tarda en dar con un hash óptimo, lo que hace que la media baje de 10 minutos, o si pasa lo contrario, el tiempo requerido de minado sobrepasará este tiempo. Para evitar este problema, la red está diseñada para que cada 2016 bloques (aproximadamente 2 semanas a 10 minutos por bloque), la red recalcula la dificultad, de nuevo que se vuelva a ajustar al tiempo estimado de 10 minutos. (Preukschat, Blockchain: La revolución industrial de internet, 2017)

Como es código de programación abierto, estas reglas pueden ser consultadas por todos y su modificación puede ser vista por cualquiera.

El incentivo que tienen los mineros para validar las transacciones en lo que se comentó con anterioridad en la generación de nuevos bloques. Cuando una red da por válido un nuevo bloque, la red recompensa el esfuerzo computacional con 50 bitcoins (siguiendo el ejemplo de la primera transacción entre Satoshi y Hall, pero esto puede ser extrapolable a cualquier otra criptomoneda como Ethereum o LiteCoin, u otras recompensas descritas en cada protocolo). El protocolo Bitcoin describe que cada 210.000 nuevos bloques el premio por minar se reduzca a la mitad como se describe en la siguiente fórmula:

$$N = 210.000 \times \left(50 + \frac{50}{2^1} + \frac{50}{2^2} + \frac{50}{2^3} + \cdots\right) = 21.000.000$$



Fuente: Blockchain.info/charts

El *Proof of Work* (PoW) o prueba de trabajo es un esfuerzo computacional que se determina en el protocolo de la Blockchain que se vaya a minar, y consiste en encontrar un bloque válido aplicando una función llamada hashcash hasta dar con un resultado óptimo. La función hashcash consiste en un proceso iterativo que consiste en aplicar la misma función hash sobre un conjunto de datos estandarizados de 80 bits. Este proceso se hace una vez conocido el valor del nodo raíz de del árbol de Merkle. Lograr un bloque válido se consigue cuando el resultado de la función hashcash[15] expresado en formato hexadecimal, cuyo valor sea inferior al exigido por toda la red en ese momento, cuya información está en el campo target de la cabecera. Las funciones hash muestran un carácter no determinista por lo que necesitaremos aplicar la función un número no definido de veces hasta encontrar un valor menor al requerido. Alex Preukschat en su libro: "Blockchain: la revolución industrial de internet" pone el ejemplo de una tirada de un dado. Imaginemos que nos solicitan tirar un dado de un millón de caras y tenemos que obtener una tirada que sea menor o igual a mil. Necesitaríamos lanzar el dado al menos 1000 veces en términos esperados hasta dar con el valor requerido. Esto es lo que hacen los mineros en la red constantemente.

Una vez que uno de los mineros encuentra el valor buscado, la red comprueba que es un resultado óptimo de la función, se verifica (sólo necesita una verificación), y es añadido a la cadena con un sello, una huella del nodo anterior, el nodo que agrega y la firma del minero con la prueba de trabajo. (Preukschat, 2017)

[15] Consiste en un número de 256 bits que se ve en los exploradores de los bloques, y que facilita la búsqueda de información en la Blockchain de forma que pueda ser legible.

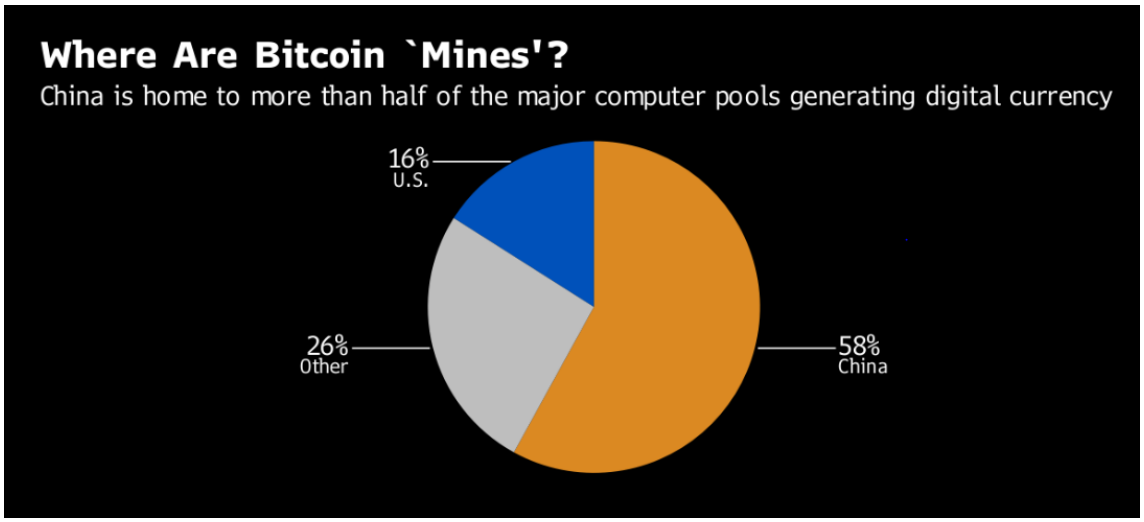
La prueba de trabajo es el tipo de prueba establecida en el protocolo Bitcoin, pero en otros protocolos se define que la prueba de trabajo para validar nuevos bloques sea la conocida como *Proof of Stake* (PoS) o prueba de participación. Esta prueba es un algoritmo de consenso alternativo a la PoW que consiste en solucionar el problema matemático en función de los derechos de propiedad que posee dicho minero, de esta manera si un minero tiene un 1% de Bitcoin solo puede extraer o validar dicho 1% de los bloques. De esta forma se intenta limitar el minado de la criptomoneda que se esté extrayendo, de forma que para atacarla necesitas tener un 51% de la red, y siendo pública, al ver el resto de los mineros que está siendo atacada por el propietario de ese 51% esta criptomoneda deja de tener interés y por tanto deja de tener valor para el resto de las participantes, por lo que se desincentiva el intento de hackeo de la red.

Estas son las dos formas que actualmente se utilizan para poder validar o extraer un bloque en la actualidad. Existen criptomonedas que utilizan un híbrido entre las dos como es el caso de Peercoin. Sin embargo, son muchas las pruebas de validación que surgirán con el desarrollo de la cadena de bloques, y cada protocolo podrá establecer aquella que mejor se ajuste a su idiosincrasia. Desde un punto de vista que permita al lector entender como se hace un minado, hay que subrayar que no hacen falta conocimientos matemáticos elevados, dado que cualquier usuario puede ser minero, haciendo una inversión en un equipo potente, que permita instalar un programa informático que pueda ejecutar los algoritmos y a través de la tarjeta gráfica o la CPU[16] del ordenador pueda empezar a ejecutar dicho minado. Los usuarios que se unen a una Blockchain tienen el ordenador las 24 horas del día ejecutando dicho programa[17], lo que supone un gasto energético importante, de ahí que se recompense al minero con bitcoins u otro activo para compensar el esfuerzo de trabajo y el gasto energético.

En la actualidad están surgiendo “granjas” de minado, que están siendo objeto de crítica por este gasto energético, y el ruido que supone tener un edificio lleno de ordenadores equipado con grandes ventiladores que soporten la actividad a la que están sometidos dichos procesadores. Un estudio de la universidad de Cambridge y Bloomberg[18] el consumo anual de KWh que necesita una empresa como VISA equivale al consumo de 50.000 hogares de Estados Unidos, mientras que solo la red Bitcoin equivale a unos 814.000 hogares estadounidenses. La mayoría de estas granjas de minado se localizan en China, aprovechando el bajo coste de la energía en zonas como Xinjiang y Mongolia.

[16] CPU o Central Processor Unit, esto es el procesador central del equipo. A raíz del minado de bloques los fabricantes de hardware crearon las GPU, que son unas placas especificas creadas con un procesador pensado para la minería de datos.
[17] Existen diferentes programas que permiten el minado de criptomonedas como pueden ser CG Miner o MinerGate, no se entrará en profundidad en este tema dado que excede de los objetivos de este trabajo.
[18] https://www.bloomberg.com/news/articles/2017-12-15/turning-coal-into-bitcoin-dirty-secret-of-2017-s-hottest-market

Ilustración 7 Mapa de minado



Fuente: Bloomberg and Cambridge University study

2.6. Smart Contract

Los contratos son acuerdos legales en el que se establecen derechos y obligaciones entre las partes intervinientes del mismo. El código civil español en su artículo 1088 establece una obligación como:" Toda obligación consiste en dar, hacer o no hacer alguna cosa". Así mismo, establece en el artículo 1091:" Las obligaciones que nacen de los contratos tienen fuerza de ley entre las partes contratantes, y deben cumplirse a tenor de los mismos".

Los elementos esenciales del contrato son:

1. **Consentimiento de los contratantes:** Tiene que existir voluntad de las partes y que esa voluntad se exteriorice.
2. **Objeto cierto**: Todo bien o servicio susceptible de valoración económica.
3. **Causa** de la obligación que ha de existir y ser conforme a la ley.

Si alguno de estos tres elementos no se diera, darían lugar a la inexistencia del contrato (art. 1.261 del Código Civil).

La evolución de la era digital ha dado paso a nuevos activos, y servicios digitales que necesitan de herramientas que eviten procesos lentos, y la necesidad de intermediarios que validen y ejecuten las transacciones.

Los *Smart Contracts* o contratos inteligentes es un término del que se habló por primera vez en 1997 por el informático, jurista y criptógrafo, Nick Szabo, en un *Paper*[19] que

[19] http://szabo.best.vwh.net/smart_contracts_idea.html

escribió, donde propuso contratos inteligentes como un medio para integrar las cláusulas contractuales en los activos digitales, y en los que se necesitaba transparencia y confianza entre las partes. Nick Szabo[20] era conocido por su investigación en contratos digitales y en monedas digitales. (CFO, 2016).

Los Smart contracts, pueden verificar el proceso y autoejecutarse. Un ejemplo que tenemos en nuestro día a día, y que puede ser implementado sin tecnología Blockchain, es el que puso el señor Szabo de las máquinas expendedoras. Esta máquina, cuando introducimos una moneda, esta máquina verifica el valor de la misma y que es de curso legal, y de forma automática, valida la transacción y nos proporciona la opción establecida.

Con la llegada de Bitcoin, se volvió a discutir las propiedades y las posibilidades de implementación de los contratos inteligentes, en los que la tecnología Blockchain aportaba un extra de seguridad y confianza que solucionaba todos los problemas que se habían discutido durante años.

"Intenté imitar lo más posible en el ciberespacio las características de seguridad y confianza del oro, y la principal de ellas es que no depende de una autoridad central confiable"

Nick Szabo

Al igual que el término de Blockchain, para los Smart Contracts existen diferentes definiciones o aproximaciones alrededor de esta figura y en la que se observa la concurrencia de diferentes rasgos comunes.

Una de ellas es la que el profesor Szabo propuso para esta figura, teniendo en cuenta que fue él quien habló por primera vez de este término y que definió de la siguiente manera: *un conjunto de promesas, especificadas en forma digital, incluyendo protocolos dentro de los cuales las partes cumplen con estas promesas.*

Otra propuesta puede ser la establecida por Gideon Greenspan[21] que define a los contratos inteligentes como: *un fragmento de código que se almacena en una cadena de bloques activada por transacciones en la Blockchain y que lee y escribe datos en una base de datos de Blockchain*. Y la definición más común sería: "una herramienta de código computacional programable que se almacenan en una red Blockchain y se ejecuta de forma automática. Una tecnología que permite que se realicen uno o varios términos contractuales entre varios actores que responden a una lógica booleana (si esto, entonces aquello) (Rey, 2018).

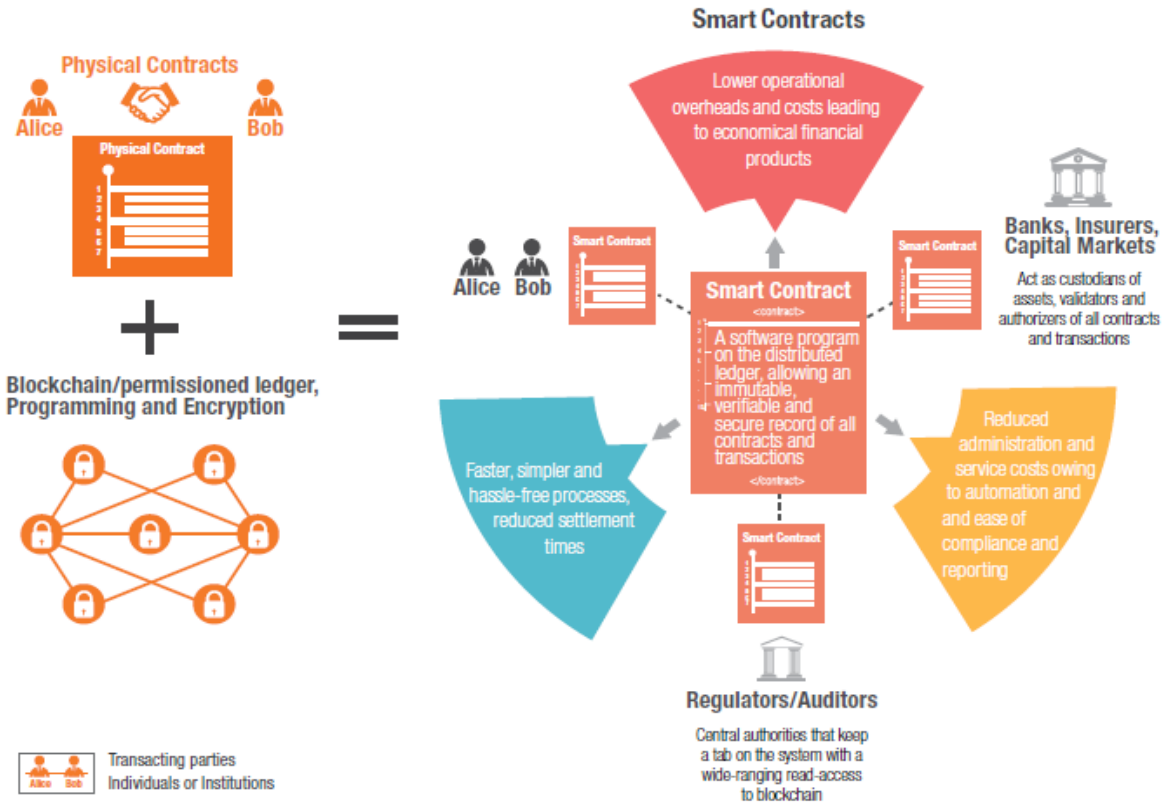
[20] Aunque la figura de Satoshi Nakamoto es anónima, una de las especulaciones es que Nick Szabo está detrás de este seudónimo. Este hecho ha sido varias veces negados por el autor.
[21] https://www.multichain.com/blog/2016/04/beware-impossible-smart-contract

Estos contratos inteligentes son un código programable que con Blockchain permiten establecer condiciones para que las transacciones se ejecuten automáticamente. Aunque el código puede ejecutarse sin Blockchain, esta tecnología aporta propiedades que dotan a los contratos inteligentes propiedades que los hace únicos.

Estas propiedades cuentan con las siguientes características:

- Se ejecuta de forma automática basado en un lenguaje de programación if-then: es decir, el contrato no necesita de intervención humana para proceder.
- Queda registrado en la cadena de bloques de manera que una vez registrado, éste no se puede borrar, lo que entre otras cosas, no puede ser destruido, evita fraudes, y la posibilidad de incumplimiento de una de las partes.
- Elimina la figura de intermediarios: este no necesita de un ente central que tenga que validar la transacción, dado que una vez verificado por la red, el contrato ejecuta la orden previamente programada.
- Su ejecución se produce de una forma más rápida y con menor coste que los contratos habituales.

Ilustración 8 Smart Contracts



Fuente: Capgemini Consulting Analysis

Sin embargo, aún existen limitaciones que hacen que los contratos inteligentes no se estén desarrollando con todo su potencial. Uno de los problemas existentes es pasar de un lenguaje formal a un lenguaje de código programable. No todo lo que puede escribirse puede establecerse en lenguaje virtual o programable. Con la inteligencia artificial se ha avanzado mucho en este sentido, pero hay ciertos sucesos en los que se está trabajando para mejorar los procesos informáticos. En modo de ejemplo cuando un coche autónomo de Google identifica un objeto delante, el mecanismo hace que este coche frene o se detenga, pero imaginemos la situación en la que un balón de futbol se cruza ante el vehículo, este se detendrá porque habrá detectado un objeto, sin embargo, la inteligencia artificial no intuye que detrás del balón, pueda venir un niño.

Otro ejemplo es cuando existe la causa de fuerza mayor en los contratos, dado que una vez que se ha cumplido las condiciones pactadas, el contrato inteligente ejecuta el contrato, pero no entiende de causa o fuerza mayor que ha provocado que el contrato se valide sin entender que ha existido un elemento externo que lo ha provocado. Un ejemplo de esto podría ser un temporal de nieve o viento que imposibilite que un avión salga de destino a la hora establecida y se autoejecute el seguro de retraso o cancelación de vuelos.

Aquí es donde nace la figura del oráculo, que es algo externo en los Smart contracts, pero necesario en multitud de situaciones como pueden ser condiciones excepcionales o la necesidad de verificador de un tercero. Un oráculo, por tanto, puede actuar como un tercero de confianza.

La figura del oráculo conecta la tecnología Blockchain con el mundo real. La cadena de bloques es un proceso determinista, es decir, ante determinado suceso, cuando existe un contrato inteligente, este se autoejecuta, aportando inmutabilidad, aunque reduce la flexibilidad. Los eventos sin embargo son sucesos estocásticos que dependen de múltiples factores que provocan la variación de los términos contractuales. Este gap que se produce entre el mundo Blockchain y el mundo fuera de la cadena lo soluciona la figura del oráculo, que son terceros de confianza y/o estructura de datos confiables que envían datos desde fuera de la red a la cadena de bloques para verificar un suceso determinado.

Estos terceros de confianza deben ser aceptados por los usuarios y/o compañías participes en los contratos inteligentes. En el caso de los retrasos de vuelos, un oráculo válido, podría ser en España: Aeropuertos Españoles y Navegación Aérea (AENA S.A.).

Los contratos inteligentes, dada la tecnología Blockchain, son descentralizados y chocan con la filosofía centralizada de los oráculos por lo que hay diversas startups que están trabajando para aplacar esta discusión. Un ejemplo es el caso de Link que ha creado la primera red de oráculos descentralizados, que permite a los contratos inteligentes conectarse a datos de fuera de la cadena, así como aplicaciones o sistemas de pago utilizados por la gran mayoría. Estos sistemas de pago en mucho de la mayoría de los casos utilizan las criptomonedas, hecho que ha provocado la proliferación de nuevas

monedas digitales. Otro de los oráculos utilizados es el caso de Oraclize, que está constantemente observando la red Blockchain para actuar en caso de ser necesario, en muchos casos se considera la figura de notario o auditor dentro de la red.

La red Ethereum es la Blockchain más prometedora en este tipo de contratos y las grandes compañías y consorcios trabajan en esta red para desarrollar los Smart contracts en sus modelos de negocios. Se tratará con mayor profundidad este tema en el apartado del sector asegurador.

2.7. Criptomonedas

Como se indicó al principio de este estudio, las criptomonedas son sistemas de pago completamente digital que permiten enviar dinero por todo el mundo, sin la intervención de entidades centrales o intermediarios y que permite transacciones Peer to Peer de pago impulsado por sus usuarios de una forma descentralizada. Estas transacciones utilizan técnicas criptográficas y son almacenadas en las cadenas de bloques.

Actualmente existen casi 1600 criptomonedas según la web coinmarketcap, entre las que destacan bitcoin, que, al ser la primera criptomoneda en aparecer, ha alcanzado una capitalización de más de 141 mil millones de dólares americanos, Ethereum cuya capitalización en el mercado alcanza los 70 mil millones o Ripple que alcanza los 26 mil millones de dólares (datos proporcionados por el Exchange Binance a fecha de mayo de 2018).

Las principales características de las criptomonedas son:

- **No son controladas por bancos centrales**: las criptomonedas se crearon para evitar la intervención de entidades centrales o intermediarios, después de la crisis financiera que afectó a todo el mundo, y de esta forma permitiera los pagos por todo el mundo de una forma más rápida, más barata y evitar la legitimidad que subyace del dinero fiduciario.
- **Ofrecen cierto grado de anonimato**: la tecnología permite cierto grado de anonimato dado que puedes identificarte con un seudónimo en vez de tu nombre real. Esto ha permitido que se use este tipo de sistemas para actividades ilícitas dada su esta característica. Por ejemplo, una pieza de *ransomware*[22] llamado *WannaCry* fue lanzado a nivel mundial infectando a multitud de instituciones e individuos a los que eran obligados a pagar una cierta cantidad de bitcoins que permitiera el desbloqueo de sus archivos. Otra de las críticas a las criptomonedas es el uso de estas para el uso de financiación de determinados grupos terroristas.

[22] Un ransomware, del inglés ransom, rescate, y ware, por software, es un tipo de programa informático que limita el acceso a determinadas partes o archivos del sistema infectado, y pide un rescate a cambio de quitar esta restricción.

- **Volatilidad en sus precios**: desde la creación de bitcoin, en las que simula ser una reserva de valor parecida al oro, limitando su cantidad a 21 millones de monedas, ha incrementado su atracción a los especuladores. A finales del año 2017 bitcoin y Ether (la criptomoneda de la Blockchain pública Ethereum), aumentaron su valor un 1400% y un 9000% respectivamente, mientras que el índice de las principales criptomonedas aumentó aproximadamente un 2800%. Después de estas grandes subidas, se produjeron derrumbes de aproximadamente un 60%. (Mercer, 2018).
  Esto ha sido aprovechado por el uso de la inteligencia artificial y el *Deep Learning* en el que la liquidez de las criptomonedas ha provocado este tipo de trading en busca de un mayor rendimiento.
- **Permiten la financiación de nuevas empresas**: las ICO (*initial Coin Offerring*) también denominado *token crowdsale*, constituyen una novedosa, disruptiva y democrática forma de recaudar fondos para las nuevas empresas basadas en tecnología Blockchain, y que por otro lado no pueden acceder a formas tradicionales de financiación. Entonces cuando una compañía quiere desarrollar un proyecto, crea un *token* y lo emite al mercado para conseguir dinero para su nuevo proyecto de negocio, esta emisión se conoce como *"utillity Token"*, aunque estos no están diseñados como *tokens* de inversión sino como el acceso futuro al producto o servicio de una empresa.

Las ICOs gozan de un importante éxito. Son ya cientos de proyectos financiados por este sistema y el dinero recaudado se eleva a varios miles de millones. En este sentido el Banco de España emitió en enero de este año un comunicado en el que afirmaba que: "En su mayoría, las ICOs están asociadas a proyectos empresariales en etapas muy tempranas de desarrollo, sin que exista un modelo de negocio consolidado o con flujos de caja inciertos. Estas iniciativas pueden tener una alta probabilidad de fracaso".

2.8. La tokenización de activos: ¿Qué es una DAO?

Una organización Autónoma descentralizada (DAO dada sus siglas en inglés: *Decentralized Autonomous Organitation*) sustituyen los procesos que imperan en una organización convencional por un protocolo informático que es programado en un *Smart Contract* y cuya misión es descentralizar las relaciones entre humanos. Esto abarca todos los usuarios internos o externos de una organización incluyendo la junta directiva, empleados, clientes y proveedores. En definitiva, una DAO es uno o varios *Smart Contracts* que se automatizan en una red Blockchain y que se sustenta gracias a una comunidad que lo alimenta. (Preukschat & Molero, 2018).

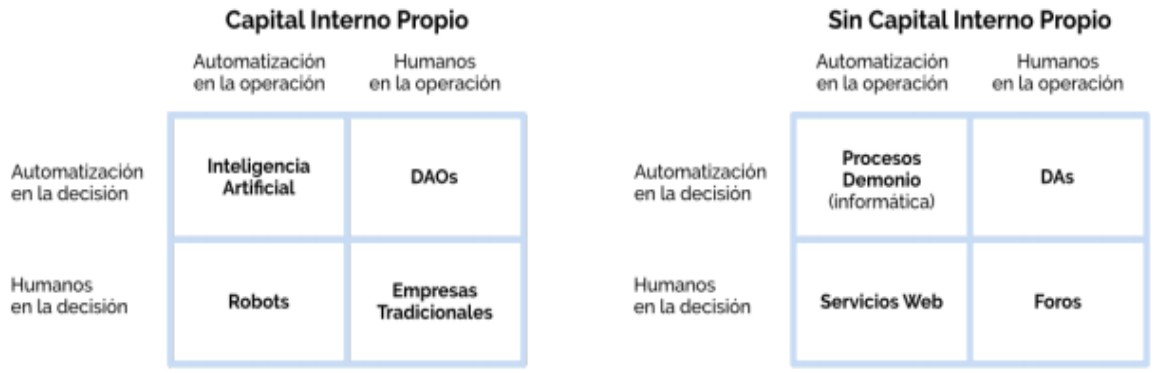
Estas nuevas organizaciones descentralizadas cuentan con todas las ventajas que supone el uso de la tecnología Blockchain: transparencia, abiertas, que permiten una trazabilidad completa de sus registros, operaciones y demás actividades y que otorgan una total confianza de todos los partícipes que la integran.

Un ejemplo claro de lo que puede ser una DAO se muestra en el libro de la Comunidad Blockchain titulado El futuro de la criptoeconomía descentralizada y las ICO´s en el cual expone el caso de Mike Hearn y el coche autónomo. En el cual, el propio vehículo toma sus propias decisiones, desde escoger la mejor ruta para llegar a destino, recoger a sus ocupantes, autoabastecerse o incluso ir al taller cuando sea pertinente. Además, no es necesario que el coche sea propiedad de un solo usuario o de varios, si no que puede ser su propio dueño, estar tokenizado, y sus *tokens* ser comprados o vendidos por inversores interesados.

Bajo este ecosistema surgen las DAC (*Decentralized Autonomous Corporations*). Estas corporaciones Autónomas Descentralizadas se diferencian de las DAO´s en que las primeras distribuyen beneficios entre los dueños de los *tokens*. (Preukschat & Molero,2018).

Así, en una DAO los dueños son los poseedores de los *tokens* y se toman las decisiones por medio del consenso entre los poseedores de los mismos, por tanto, a diferencia de la una organización tradicional, el poder está distribuido. Esto no significa que exista una anarquía en la empresa, dado que una empresa descentralizada también cuenta con un protocolo definido en un contrato inteligente encargado de hacer cumplir con las normas están definidas por consenso, donde el código es propiedad de todos, y que es la comunidad la encargada de su autorregulación y gobernanza.

Ilustración 9 Cuadrantes que ilustran actividades y organizaciones de acuerdo a si cuentan o no con capital



Fuente: LibroBlockchain.com

De acuerdo con este nuevo paradigma de la tokenización, cualquier activo o servicio puede ser tokenizado, como puede ser la entrada de un teatro, un vehículo, una casa o como una nueva moneda (criptomonedas). Sin embargo, en una ICO solo se utilizan tres tipos de *tokens*: *Utility*, *Security* y criptomonedas. Para distinguir cuando un *token* es *Utility* o *Security* se hacen las siguientes apreciaciones:

- ***Token Utility***: representan el acceso futuro al producto o servicio de una compañía. La característica definitoria de los tokens de utilidad es que no están diseñados como inversiones. Un ejemplo es FileCoin[23], una plataforma de almacenaje en la nube que recaudó 257 millones de dólares.
- ***Token Security***: son parte de la compañía, es decir, son considerados valores negociables. En julio de 2017 la SEC[24] (*Securities and Exchange Commission*) publicaron un informe donde fueron admitidos como valores y, por tanto, están sometidos a su regulación.

También podemos distinguir entre los tokens fungibles y los tokens no fungibles. El primero de ellos significa que puede ser intercambiable con uno de igual valor y no importa su individualidad, sin embargo, el *token* no fungible es único, y se utilizan para determinar la propiedad de un *token* o un activo digital específico.

[23] https://filecoin.io/filecoin.pdf

[24] Jay Clayton, director de la SEC, señaló en la publicación del informe: "Puedes llamarlo una moneda, pero si funciona como una *Security*, es una *Security*".

PARTE III: Blockchain en el sector asegurador

3.1. Fintech e Insurtech

Fintech surge de la unión de las palabras inglesas finanzas y tecnología (*Finance and Technology)*, así como Insurtech lo hace con las palabras seguro y tecnología también en lengua anglosajona (*Insurance and Technology*).

La transformación digital que vivimos y se comentó en el primer capítulo, hacen que las instituciones financieras y las compañías aseguradoras, deban adaptarse a estos nuevos cambios tecnológicos, de hábitos, de paradigma, y en el que las personas están completamente integradas en la era digital.

La era digital en palabras del *Massachusetts Institute of Technology* (MIT) es "la adopción progresiva de soluciones, tecnologías y procesos digitales dentro de todas las áreas de una organización para optimizar sus resultados".
La industria financiera siempre ha sido más innovadora que la industria de los seguros, que tiene fama de ser más conservadora. Por tanto, en la actualidad las aplicaciones tecnológicas en el sector financiero están en una etapa más madura que su homólogo asegurador.

Este nuevo ecosistema ha provocado la creación de nuevas empresas, consorcios y asociaciones, como es la Asociación Española de Fintech e Insurtech (AEFI), en la que cuenta con 122 empresas asociadas de las 300 que actualmente existen en España (de las cuales 92 son Insurtech). En Europa hay 1500 empresas con esta consideración. El objetivo de AEFI es el de crear un entorno favorable para el desarrollo de Startups y empresas Fintech e Insurtech en España, realizando labores de interlocución, comunicación y colaboración con los organismos y agentes relevantes del sistema para fortalecer su crecimiento y su ecosistema. Esta asociación define en su *White Paper* el término Insurtech como*: La aplicación de la tecnología a las actividades desarrolladas por las entidades del sector asegurador* (AEFI, 2018).

Ilustración 10 Mapa Fintech

Fuente: http://spanishfintech.net

Las compañías aseguradoras no pueden quedar al margen de este nuevo paradigma, deben investigar, innovar e implantar estas nuevas tecnologías que transformen sus negocios ante este ecosistema de innovación e incorporen con éxito nuevas capacidades digitales.

Esto implica que la industria aseguradora transforme su modelo de negocio, abrazar el nuevo entorno digital y otorgar a los clientes un grado de personificación similar al que se utiliza en otras industrias. Los clientes cada vez son más inquietos, y utilizan nuevas formas de contratación, comparación y cada vez están más integrados en las plataformas digitales.

El cambio en la tendencia de la fidelidad de los clientes obliga a las compañías a adoptar un modelo de negocio en el que ofrezca al cliente nuevos servicios adaptables, dinámicos y que mejore la eficiencia para que las Insurtech puedan obtener una ventaja competitiva respecto a las aseguradoras convencionales.

Mientras el sector asegurador tradicional se enfrenta a los retos y exigencias de los nuevos requerimientos de Solvencia II, que obliga a las compañías a adaptar sus procesos y sistemas, acometiendo para ello cuantiosas inversiones, las Insurtech pueden

dedicar parte de sus recursos en innovación tecnológica con el objetivo de mejorar la experiencia del cliente.

Estas innovaciones dentro del sector provocan la aparición de nuevas formas de comunicación con los clientes, nuevos canales, el uso del *Big Data*, el uso masivo del Internet de las cosas (que trataremos en el próximo apartado), u otro ámbito de aplicación tecnológica que permita al cliente la utilización de nuevos productos, más adaptados a sus necesidades y preferencias individuales que supone a la aseguradora utilizar estrategias de *pricing* individualizadas (Rafael Illescas; Francisco Uría; Álvaro Requeijo, 2017).

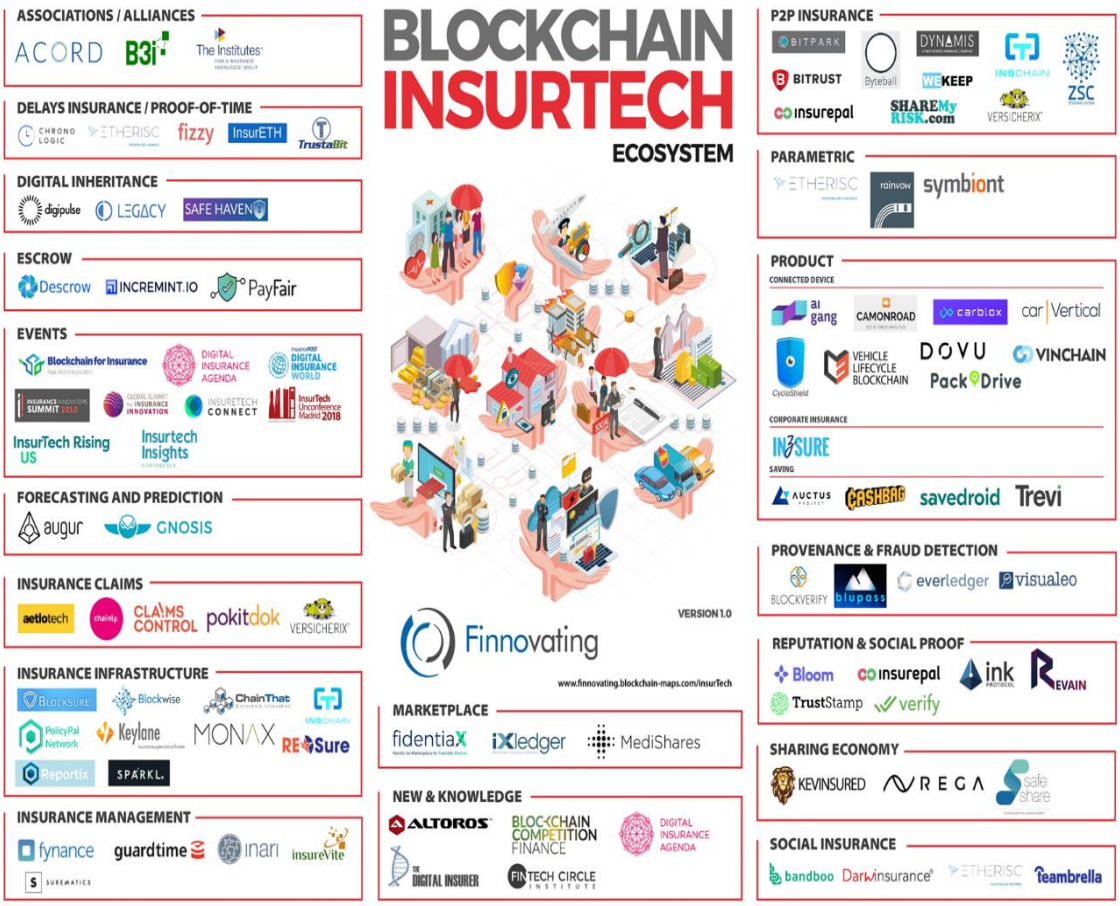
En este sentido, en la semana del seguro organizada por INESE[25] en febrero de 2018, Javier Pimentel, director de Digital de la compañía Caser dijo: "el nuevo entorno digital trae una serie de nuevos riesgos y oportunidades que hasta hace poco eran desconocidos e inexistentes: analítica de datos, drones, IoT, *smart cities*, *wearables*, *e-health*, ciberseguridad, pagos contactless, vehículos conectados… la lista no hace más que crecer año tras año y el reto está en ser capaces de dar una respuesta aseguradora a la disrupción que supone cada una de estas nuevas tecnologías en el mercado y en la sociedad". En esta misma línea, el fundador de la startup Coverwallet, Iñaki Berenguer afirmó que "a las grandes aseguradoras les falta el ADN tecnológico para crear productos innovadores desde cero combinando la experiencia de usuario (UX), diseño, tecnología, datos o marketing digital". Así mismo, comentó que, si las aseguradoras "se unieran a emprendedores, ingenieros, diseñadores y data scientists que se replantean el sector con ingenuidad, podrían tener un cocktail explosivo, y crear empresas referentes en el mercado global de Insurtech".

Finnovating lanzó el pasado mes de mayo de 2018, el primer mapa Blockchain en Insurtech a nivel mundial. Éste congrega casi 100 iniciativas dentro del sector Insurtech que utilizan tecnología Blockchain. Ver Ilustración 11 Mapa Insurtech.

En este estudio se abordará como algunas de estas tecnologías y dispositivos pueden cambiar de una forma disruptiva el sector asegurador y la ciencia actuarial.

[25] Fundada en 1986, INESE se ha desarrollado como una empresa proveedora de servicios para el sector asegurador, con los objetivos de proporcionar conocimiento y crear oportunidades.

Ilustración 11 Mapa Insurtech



Fuente: http://www.finnovating.Blockchain-maps.com

3.2. Blockchain: el aliado natural del Internet of thing (IoT)

El *internet of Thing* (IoT) o internet de las cosas en español, es un término acuñado por Kevin Ashton en 1999, un pionero de la tecnología que trabaja en la identificación por radiofrecuencia (RFID), que concibió un sistema de sensores ubicuos que conectan el mundo físico con Internet.

El *Internet of Thing* se refiere a la combinación de dispositivos físicos, vehículos, edificios y otros elementos incorporados con la electrónica, el software, los sensores, y la conectividad de la red que permiten estos objetos físicos para recoger e intercambiar datos. Otra de las definiciones que podemos encontrar en la literatura esla integración de sensores y dispositivos en objetos cotidianos, que quedan conectados a Internet a través de redes fijas e inalámbricas.

Desde la irrupción del internet de las cosas, su aplicación ha ido evolucionado a partir de la convergencia de las tecnologías inalámbricas, sistemas micro electromecánicos e Internet. Esta convergencia ha ayudado a eliminar las barreras entre la tecnología

operativa y la tecnología de la información, permitiendo que los datos no estructurados generados por máquinas sean analizados en busca de percepciones que permitan mejoras en la conducción.

Una de las aplicaciones más avanzadas del IoT es la telemática, cuyos orígenes se encuentran en la fusión de telecomunicaciones e informática y su aplicación en los vehículos. A medida que la recolección de datos y la transmisión, la telemática conduce a una mejor comprensión de los problemas subyacentes en las actividades y procesos. Por lo tanto, la telemática puede hacer que las ofertas se centren más en el cliente, adaptándolos a los casos individuales, ayudar a orientar el comportamiento de los usuarios y creando nuevos productos para satisfacer necesidades específicas.

Con el aumento de dispositivos conectados, se hace cada vez más necesario mantener unos niveles de autenticación y seguridad que impidan a hackers informáticos sustraer datos personales y/o dañar los sistemas. Con la irrupción del internet de las cosas a las diferentes industrias, el crecimiento de estos dispositivos, con grandes cantidades de datos obliga a las compañías a establecer políticas de seguridad que aseguren la integridad de la privacidad de los usuarios y controle el acceso a los datos. El ejemplo en la industria de la salud, en el que los datos médicos del paciente están en estos dispositivos en tiempo real, hace que el control y la seguridad de sus datos sea una tarea de gran importancia.

Una solución a este problema es la cadena de bloques. Las características que alberga esta tecnología hacen que sea el socio perfecto del internet de las cosas dado que ambos pueden aprovecharse conjuntamente de sus múltiples propiedades.

Hay múltiples formas en las que la tecnología de la cadena de bloques puede ayudar a resolver las limitaciones de los dispositivos conectados, entre ellas se destacan:

- Los sensores del *Internet of things* pueden intercambiar datos a través de la cadena de bloques para asegurar la confianza y evitar recurrir a terceros.
- La tecnología Blockchain protege los datos de los dispositivos conectados y evita su manipulación.
- Blockchain se puede utilizar para rastrear las mediciones de datos del sensor y evitar la duplicación con cualquier otro dato malicioso.
- Los dispositivos IoT son directamente direccionables con la cadena de bloques, facilitando un historial de los dispositivos conectados para la resolución de problemas.

La combinación de estas tecnologías consigue que puedan ser mayor que la suma de sus partes, según un estudio de Gartner[26] estima que la tecnología Blockchain agregará 3.1 billones de dólares en valor comercial en el año 2030 y 457 billones de dólares en el año 2020 en cuanto al *Internet of Things*.

[26] https://www.ibm.com/blogs/Blockchain/2018/01/why-Blockchain-and-iot-are-best-friends/

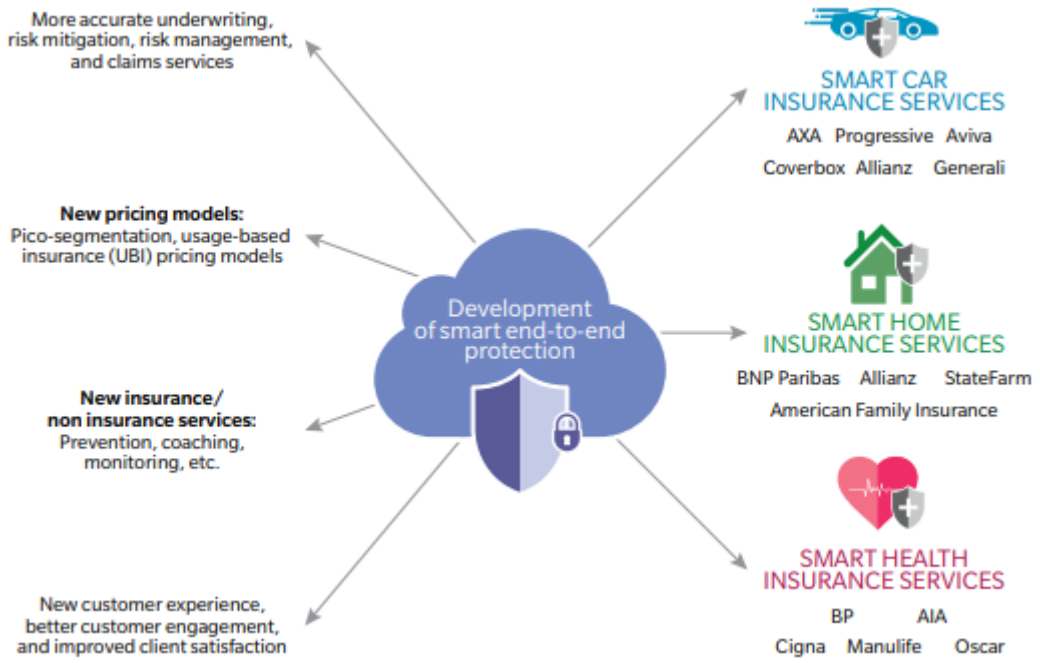
La industria aseguradora puede ser un gran actor en esta fusión, incorporando el valor de los datos, que permita hacer un procesamiento de los datos más preciso y eficientes, que permitan realizar cálculos actuariales con el objetivo de aproximar cada vez más una prima individual y aumente la optimización de las operaciones.

Con el procesamiento de estos datos las compañías pueden entender el comportamiento de los clientes, mejorar la oferta de productos, ayudar a prevenir siniestros y reducir el coste de los mismos.

Comprender y analizar el riesgo es, sin duda, una de las piedras angulares del negocio asegurador. La evaluación del riesgo requiere que la información sea recopilada y observada a lo largo del tiempo. Hasta ahora, el modelo básico de comprensión del riesgo ha consistido en observar las correlaciones entre los costes de los siniestros, entendiéndolo desde la frecuencia y la severidad, y las características de los activos asegurados.

Este análisis es la base para gestionar las carteras y seleccionar los riesgos. Esta información es conocida como “datos fríos”, y principalmente implicaba una descripción estática del objeto expuesto a un riesgo asegurable y el entorno esperado que pueda influir en ese riesgo. El internet de las cosas hace un nuevo modelo dinámico de información para los activos de riesgo, conocido como “datos calientes”. Los datos se relacionan con el objeto, su uso y el comportamiento del usuario, con magnitudes de medición directas. Cuando el riesgo está directamente relacionado con el objeto y el comportamiento de los asegurados, el internet de las cosas tiene el potencial de transformar a fondo la selección de riesgos, primas de seguros y modelos de monitorización (Oliver Wyman, 2017).

Ilustración 12El impacto del IoT en los seguros



Fuente: ABI Research, Oliver Wyman analysis

3.3. Consorcios

El interés que despierta Blockchain en usuarios y empresas hace que estén surgiendo diferentes consorcios que apuestan de forma conjunta en la investigación e inversión de la aplicabilidad de la tecnología en sus líneas de negocio. Algunos de estos consorcios son: B3i, Hyperledger, Enterprise Ethereum Alliance, Acord, The Institutes RiskBlock Alliance o la española Alastria, que reúnen a empresas nacionales e internacionales que son referentes en su sector.

3.3.1. B3i (Blockchain Insurance Industry Initiative)

Este consorcio se crea en el año 2016, en colaboración de empresas aseguradoras y reaseguradoras para explorar y potenciar la tecnología Blockchain en la industria aseguradora con el objetivo de aumentar la eficiencia en el intercambio de datos entre compañías de reaseguros y aseguradoras, transformar positivamente la industria y beneficiar al cliente.[27]

Sus miembros actuales son: Achmea, Aegon, Ageas, Allianz, Generali, Hannover Re, Liberty Mutual, Munich Re, RGA, SCOR, Sompo Japan Nipponkoa Insurance, Swiss Re, Tokio Marine Holdings, XL Catlin y Zurich Insurance Group (los miembros fundadores fueron Aegon, Allianz, Munich Re, Swiss Re y Zurich).

Su misión es:

[27] https://b3i.tech/home.html

- Mejorar la forma en que los datos, las reclamaciones, el capital, los pagos se divulgan, utilizan, automatizan y administran.
- Centrarse en el servicio al cliente que agrega valor, la prevención de riesgos y la gestión de riesgos.
- Haga que los riesgos de seguro sean más negociables.
- Haga que el seguro sea más asequible con una mejor experiencia del cliente.

Su presidente Gerhard Lohmann dijo: "*La transición de B3i de consorcio a compañía independiente es un paso adelante concreto para realizar el enorme potencial de Blockchain para la industria de seguros"* (B3i, 2016).
B3i completó con éxito su primer producto, un prototipo de cadena de bloques para contratos de reaseguros *Excess of Loss* (XL) a mediados de 2017, cuando un grupo formado por sus miembros, siendo aseguradores, corredores y reaseguradores, probaron su funcionalidad y solidez. El prototipo demostró que las transacciones eran más rápidas, más eficientes y más seguras comparadas con las transacciones realizadas con los métodos actuales. Los primeros intercambios en vivo en la plataforma se esperan para finales de este año 2018 (B3i, 2016).

3.3.2. Alastria

Alastria es una Asociación sin ánimo de lucro que pretende proveer a España de la Infraestructura Blockchain[28]. Este Consorcio construye, de manera colaborativa y consensuada, la plataforma Blockchain Alastria y sus librerías, que quedan a disposición de los socios (Alastria, 2017). Entre sus principales actividades se encuentran:

- Establecer los estándares técnicos de la infraestructura, y promover el acuerdo entre los asociados para su desarrollo, explotación y uso.
- Fomentar el conocimiento y el uso de las tecnologías DLT o Blockchain, promoviendo su uso entre las Administraciones, empresas y demás agentes sociales.
- Poner en manos de los desarrolladores herramientas, librerías, repositorios...que faciliten el acceso a la tecnología, uso y adopción de esta.

Alastria está construida sobre Quorum[29], la plataforma basada en Ethereum de JP Morgan.

[28] https://alastria.io

[29] JPMorgan Chase, Goldman Sachs, el Banco Nacional de Canadá y otras compañías del sector financiero pertenecen a Quorum, en 2018 cuenta con más de 120 compañías. La organización Quorum promueve el desarrollo colaborativo basado en una Blockchain mixto y emite contratos inteligentes. Se caracteriza principalmente por su procesamiento de alta velocidad y alto rendimiento. Además, cuenta con ajustes que brindan balance entre la privacidad que requieren los bancos y la exigencia de regulación que imponen los Estados.

3.3.3. Hyperledger

Hyperledger se lanzó en 2016 con una estructura de gobierno técnico y organizativo y 30 miembros corporativos fundadores. Hyperledger es un esfuerzo colaborativo de código abierto creado para avanzar las tecnologías Blockchain de la industria cruzada[30]. Es una colaboración global, organizada por The Linux Foundation, que incluye líderes en finanzas, banca, Internet de las cosas, cadenas de suministro, fabricación y tecnología.

Solo un enfoque de desarrollo colaborativo de software de código abierto puede garantizar la transparencia, la longevidad, la interoperabilidad y el soporte necesarios para llevar las tecnologías de Blockchain a la adopción comercial convencional. De eso se trata Hyperledger: comunidades de desarrolladores de software que crean marcos y plataformas de Blockchain.

Entre sus objetivos se encuentran:

- Crear procesos distribuidos, *open source*, y códigos para impulsar y proteger transacciones comerciales.
- Crear una infraestructura abierta y neutral estimulada por la comunidad empresarial.
- Compartir y difundir conocimientos sobre la tecnología Blockchain y detectar oportunidades de mercado.

Ahora Hyperledger cuenta con más de 200 compañías de todo el mundo entre las que destacamos IBM, R3, las grandes consultoras, la Universidad de Cambridge, el Banco de Inglaterra, o BBVA entre otras.

El pasado 26 de abril de 2018, BBVA e Indra firmaron el primer préstamo corporativo en el mundo emitido con tecnología Blockchain[31].

Esta operación supuso cerrar un préstamo de 75 millones de euros utilizando tecnología de registro distribuido (DLT). Para ello, una vez acordado el contrato, se utilizó la Blockchain pública de Ethereum (Tesnet), para registrar el Hash que identifica la operación. De esta forma, se aprovecha de las propiedades con la que cuenta Blockchain, en el que se garantiza la inmutabilidad, la auditabilidad y la trazabilidad de esta. Esto supuso además de lo anterior, el ahorro en tiempo de días a horas, aumentado la eficiencia y el ahorro de costes.

BBVA e Indra forman parte de los consorcios R3, Hyperledger, Enterprise Ethereum Alliance y Alastria.

[30] https://www.hyperledger.org

[31] https://www.bbva.com/es/bbva-indra-realizan-primer-prestamo-corporativo-tecnologia-Blockchain-mundo/

3.3.4. Enterprise Ethereum Alliance

Enterprise Ethereum Alliance[32] es una organización sin ánimo de lucro, que une a las empresas para investigar e implementar soluciones basadas en Smart contracts a través de la Blockchain pública de Ethereum.

Entre sus objetivos se hallan:

- Modelo de gobierno basado en la robustez que ofrece Ethereum, claridad en torno a los modelos de licenciamiento e IP para tecnología de código abierto.
- Recursos para que las empresas aprendan sobre Ethereum y aprovechen esta tecnología innovadora para abordar casos de uso específicos de la industria.
- Sea un estándar de código abierto, no un producto.

Entre sus miembros se encuentran empresas de Fortune 500, startups, académicos y aseguradoras. Algunos miembros son American Family Insurance, J.P. Morgan, Banco Santander, Thomson Reuters o Consensys[33] entre otras muchas.

3.3.5. ACORD

ACORD (*Association for Cooperative Operations Research and Development*)[34] es el organismo mundial de establecimiento de normas para las industrias de seguros y servicios financieros. ACORD se crea en 1970 para ayudar a sus miembros a realizar mejoras en toda la cadena de valor del seguro. Esta asociación reúne a más de 4000 empresas de seguros, reaseguros, corredores y agentes en todo el mundo.

ACORD está investigando e impulsando iniciativas basadas en tecnología Blockchain para aprovechar el flujo de datos e información entre todas las partes interesadas de seguros de manera global.

Como se ha mencionado anteriormente cuenta con cientos de compañías en el sector asegurador que operan por todo el mundo. Algunos de sus miembros son: Mapfre, MetLife, Swiss Re, Marsh o Zurich.

[32] https://entethalliance.org/

[33] Consensys es una empresa creada en 2014, especializada en la Blockchain pública de Ethereum y que agrupa a un equipo global de tecnólogos y empresarios que desarrolla la infraestructura y las aplicaciones que permiten un trabajo distribuido bajo la tecnología Ethereum. https://new.consensys.net

[34] https://www.acord.org/home

3.3.6. The Institutes RiskBlock

The Institutes RiskBlock[35] es un consorcio liderado por la industria que investiga el potencial de Blockchain en toda la industria de seguros. RiskBlock impulsa el tiempo de comercialización y adopción a través de aplicaciones del mundo real y casos de uso de la cadena de bloques.

Para ello se compromete a satisfacer las necesidades de desarrollo profesional en evolución de la comunidad de seguros y gestión de riesgos. Educan a las personas para que cumplan con sus responsabilidades profesionales y éticas al ofrecer soluciones educativas, de investigación, de redes y de recursos profesionales.

A su vez, The Institutes RiskBlock, colabora con los diferentes consorcios mencionados anteriormente, dado que las empresas miembros también pertenecen a estos consorcios.

Como se puede apreciar, son muchas las empresas y consorcios que están apostando por investigar e implementar en sus estrategias de negocio soluciones en Blockchain y conseguir las ventajas de contar con registros distribuidos (DLT).

3.4. Blockchain: Casos de uso y su impacto en la ciencia actuarial

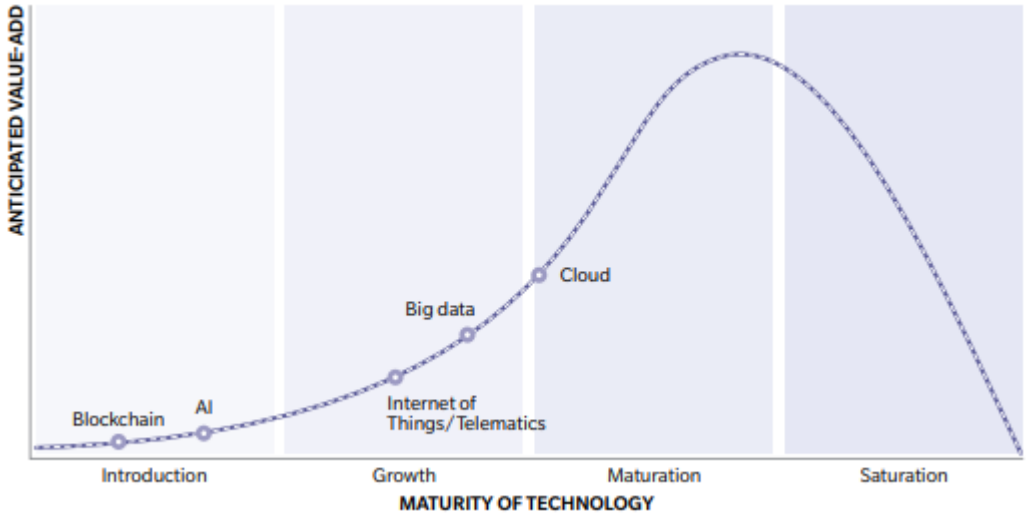
La cadena de bloques en la industria aseguradora se encuentra en una fase introductoria y de investigación. Como hemos mencionado en el apartado anterior, el interés de las compañías en esta tecnología está aumentando, y están probando su aplicación para sus procesos internos a través de proyectos piloto y pruebas de concepto.

Si comparamos la implementación de la arquitectura Blockchain con el resto de las tecnologías podemos ver que aún le queda un largo recorrido, lo que hace vislumbrar un proceso disruptivo del sector. En la siguiente ilustración se puede ver en qué fase nos encontramos de desarrollo de la cadena de bloques en el Hype Cycle de tecnologías emergentes de Gatner[36] elaborado por Oliver Wyman.

[35] https://www.theinstitutes.org

[36] El concepto de Gatner proviene del 1995 de una empresa consultora llamada con el mismo nombre, que ideó una herramienta gráfica desarrollada y utilizada para la representación de la madurez, adopción y aplicación comercial/social de una tecnología en particular, según su ciclo de vida, según su resolución de problemas reales de negocio y para explotar nuevas oportunidades.

Ilustración 13 Nivel de Madurez de la tecnología Blockchain



Fuente: Oliver Wyman

Sin embargo, aún en fase inicial, muchos son los beneficios que aporta esta tecnología en la industria aseguradora debido a su transparencia, su inmutabilidad y la capacidad de trasmitir confianza entre las partes. La cadena de bloques en el sector asegurador permite la transformación en los siguientes campos:

- **Riesgo de fraude**: uno de los grandes problemas a los que se enfrenta el sector, es el alto coste que supone el fraude en las compañías aseguradoras. Se estima que entre el 5% y 10% de todos los siniestros son fraudulentos. Según un estudio del FBI[37] esta cantidad para asegurados en ramos de No Vida supone a las aseguradoras en Estados Unidos alrededor de 40 billones de dólares americanos lo que supone un coste medio de 550$ por familia estadounidense al año. (McKinsey&Company, 2017).

  Con la cadena de bloques se puede, por ejemplo, exponer informes de daños o robos falsificados al validar la autenticidad, propiedad y procedencia de los bienes, autenticar documentos como informes médicos, revisar informes de robos de la policía e historiales de reclamaciones, verificar identidades y obtener el dato en tiempo real de dónde y quién tuvo un siniestro.

  Es evidente que esto requiere la cooperación de todos los actores participantes para poder desarrollar todo el potencial que la tecnología permite. Existen ya varias iniciativas que están trabajando para erradicar este problema. Blockverify, una empresa del Reino Unido que está construyendo un sistema que permitirá a los usuarios verificar transacciones fraudulentas, falsificaciones o robos relacionados con productos electrónicos personales, productos farmacéuticos y artículos de lujo. Funciona etiquetando los productos y luego almacenando su historial y la actividad de la cadena de suministro en una cadena de bloques. Everledger, también con sede en el Reino Unido, ha ideado una aplicación

[37] https://www.fbi.gov/stats-services/publications/insurance-fraud

similar, utilizada para verificar los diamantes y las transacciones relacionadas con ellos, y destinada a ayudar a las aseguradoras, las fuerzas del orden y los comerciantes de diamantes a detectar el fraude[38].

Además, una plataforma compartida por toda la industria permitiría detectar reclamaciones a varias aseguradoras y patrones de comportamiento relacionados con el fraude.

- **Siniestros**: la cadena de bloques con la ayuda de los contratos inteligentes va a cambiar la forma en la que se tramitan e informan los siniestros hoy en día, donde existe el riesgo de los errores humanos, la duplicación de datos, la participación de terceros y procesos ineficientes entre otros. Los siniestros con la utilización de los Smart Contracts servirá para declarar los siniestros en tiempo real, verificar el hecho, se procederá al pago y se grabará la información de manera que sea trazable y todo ello, de manera automática.

  De esta forma, se reducirán los costes de administración, se agilizará el pago, se generará una mayor satisfacción del cliente y se crearán nuevos modelos de negocio. Esta situación concede al actuario un papel fundamental, en el que tendrá que reinventarse para ir modelizando las primas hacia un enfoque más individual alejado de los clásicos sistemas de clusterización.

- **Reaseguro**: el proceso de reclamación cuando se produce un siniestro, por parte de la cedente a la reaseguradora puede ser bastante tedioso, dado que esta tiene que demostrar las pérdidas de la cartera en relación con el riesgo declarado. La tecnología Blockchain el asegurador y el reasegurador pueden rastrear y conciliar la información, que dota de confianza entre ambas compañías provocando la agilidad de los procesos.

  Además, la forma en que realiza el seguimiento de sus propios riesgos permite una mejor gestión de los mismos.

  Otro de los beneficios de la cadena de bloques aparte de la eficiencia en las transacciones y las gestiones de los siniestros, es con los swaps y bonos catastróficos (*Cat Swaps* y *Cat Bonds*). Gracias a los Smart Contracts se puede acelerar y facilitar el proceso de gestión. Así, cuando se cumplen las condiciones pactadas, el contrato inteligente activa y auto ejecuta los pagos o transacciones a las partes correspondientes. De esta forma, se aumentará la fiabilidad y auditabilidad de estos swaps y bonos catastróficos, al necesitar menos tratamiento manual, autenticación y verificación por medio de intermediarios para confirmar la legitimidad de los pagos y las transacciones (ADN del seguro, 2016).

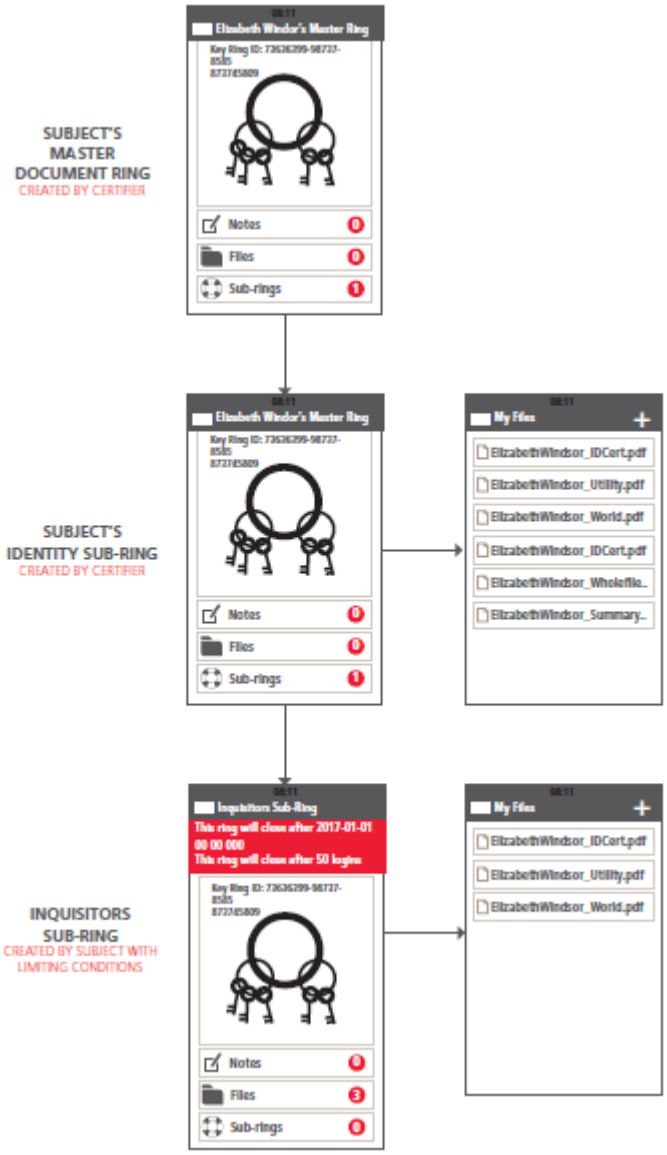
[38] Publicación: *Everledger is using Blockchain to combat fraud*, Reuters. En la cual se estima que el coste de la industria del diamante es de 2 billones de dólares solo en la ciudad de Londres.

Hay varias reaseguradoras que estan apostando por esto último, como Mapfre Re, que se ha unido a otras 22 compañias, para simular la creación y gestión de contratos de reaseguro para catastrofes, o el caso de Allianz y Nephila Capital demostraron que el procesamiento y la liquidación de pagos entre aseguradores e inversores podría acelerarse y simplificarse significativamente mediante contratos basados en cadenas de bloques (Reuters, 2016).

- **KYC o Identidad digital**: *Know your customer* (KYC) es un término que significa conoce a tu cliente. Se refiere al hecho de la verificación del cliente de su identidad cuando tramita el alta o algún servicio de una entidad, y cuando se produce de forma repetida en varias entidades, se produce en el cliente una sensación de frustración. Imaginemos que un cliente tiene su póliza de vehículos en una aseguradora, la de hogar en otra, y su seguro de vida en otra compañía; cuando quiere realizar algún cambio, lleva a una proceso repetitivo y lento en cada de las entidades a las que el cliente quiere llevar sus seguros.

  Con Blockchain se puede solucionar este problema, permitiendo al usuario obtener una identidad digital, con la cual, una vez se produce el alta en cualquier compañía, y verificada por ésta, el usuario cuando quiera cambiar solamente tendrá que compartir la parte de su identidad que sea requerida con un solo clic sin necesidad de tener que pasar procesos arduos.
  Todos los documentos en la cadena de bloques son encriptados y sólo el cliente tiene la clave, compartiendo solo lo que el cliente permite, resolviendo así un conjunto de problemas regulatorios en torno a la privacidad de los datos. Esto provoca una reducción de costes y de tiempo dedicado por el cliente, significando una mayor satisfacción del usuario (Mainelli & Manson, 2016).

Ilustración 14 Ejemplo de cómo un usuario de KYC puede controlar el acceso de sus datos con Blockchain



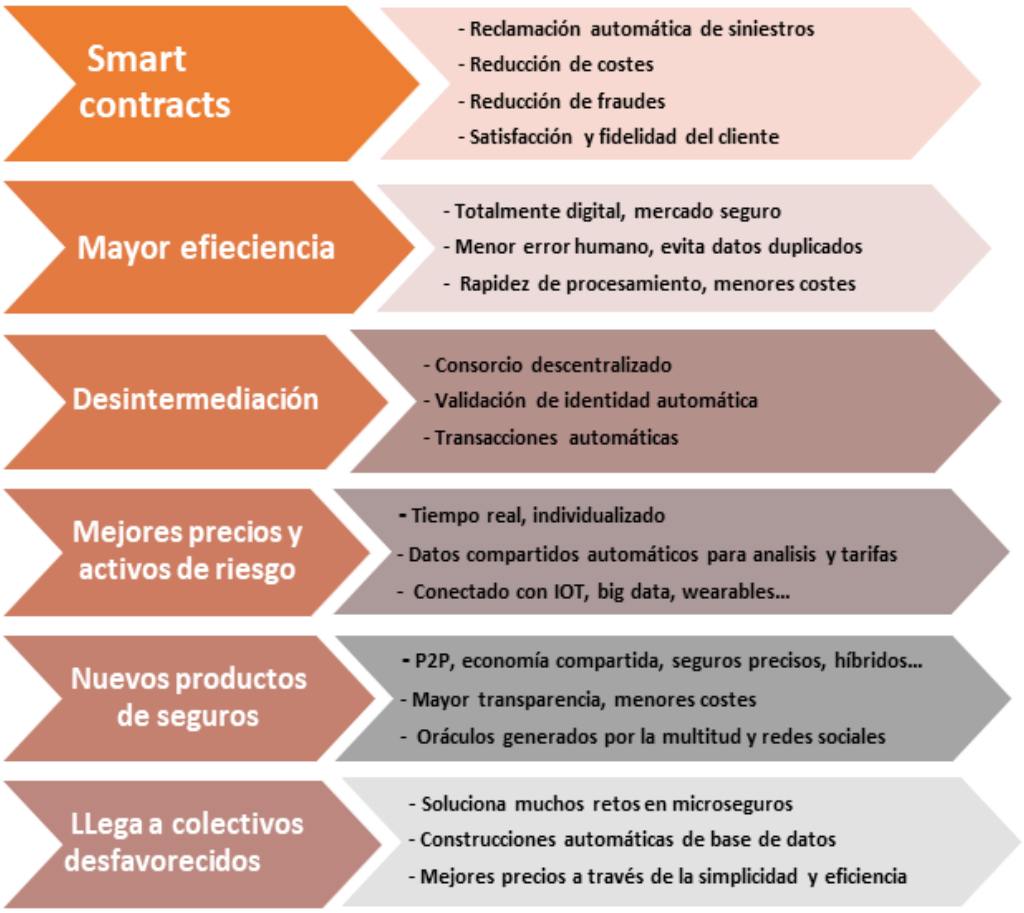
Fuente: PWC: How Blockchain Technology Might Transform Wholesale Insurance

Otro ejemplo, es la empresa británica Tradle que está trabajando en una solución en Blockchain que permitirá a las instituciones financieras llevar a cabo los controles de "conozca a su cliente" (KYC) exigidos por los reguladores para evitar el blanqueo de dinero, un proceso que, por lo demás, es costoso y lleva mucho tiempo para las instituciones y molesto para los clientes que tienen que ofrecer la misma información sobre su identidad y fuente de riqueza a diferentes instituciones. Una vez verificados los datos de KYC, el cliente podrá utilizar una clave privada para conceder a las empresas de la red acceso a los datos cifrados siempre que lo necesiten con diferentes contratos en otras compañías con la misma herramienta, incrementando la eficiencia y satisfacción del cliente.

- **Smart Contracts**: los contratos inteligentes, tal y como se ha tratado a lo largo de este estudio, supone un cambio disruptivo del sector y un reto para la ciencia actuarial que dispondrá de nuevas herramientas que le permitan ajustar los riesgos de una manera más precisa gracias a la cantidad de datos en tiempo real de los que dispondrá, y de esta forma, elaborar nuevas técnicas de *pricing*.

  Son muchas las ventajas que proporciona los Smart Contracts en el sector asegurador. En la siguiente tabla se podrá ver de una forma agregada algunas de estas.

Ilustración 15 Diferentes formas de cómo Blockchain puede transformar el seguro



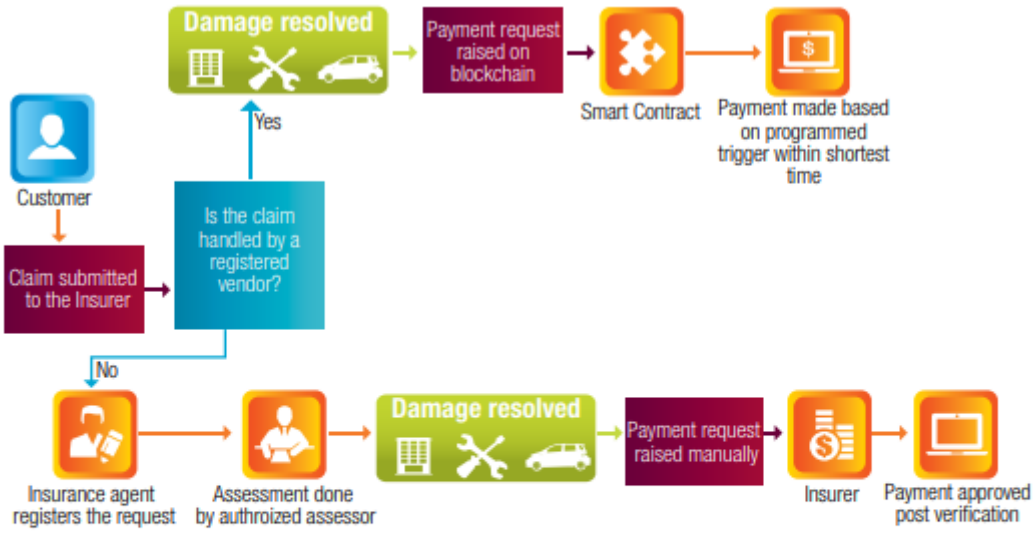
Fuente: Elaboración propia a través de información en www.WillisTowerWatson.com

En la actualidad podemos encontrar algunos ejemplos que se están aplicando con esta metodología. AXA cuenta con un seguro de retraso y cancelación de vuelos llamado Fizzy en fase de pruebas, en el cual de momento opera entre los aeropuertos de Paris y Nueva York, que, en caso de producirse un retraso de 2 horas, de forma automática se activa el contrato inteligente (mediante la figura del oráculo que nutre de información a tiempo real), y antes de que el asegurado tome el avión ya dispone de la suma asegurada en su cuenta corriente. Este

hecho tiene varias implicaciones actuariales que hay que tenerse muy en cuenta a la hora de la modelización del riesgo y la tarificación.

En primer lugar, el ahorro de costes administrativos y de gestión son importantes. Según un estudio de la consultora Capgemini[39] solo en los seguros de motor en Reino Unido, supone un 12.5% de ahorro al utilizar Blockchain con contratos inteligentes, lo que podría suponer 21 billones de dólares en la industria global del motor (Capgemini Consulting, 2017).

Ilustración 16 Ahorro potencial de costes en la industria aseguradora del motor gracias al uso de los Smart Contracts



Calculation of the cost savings potential from the use of smart contracts in the UK motor insurance industry

Year-2015	Number of Motor Insurance Claims in the UK (A)	Claims cost and Expenses in $ million (B)	Total Expected Savings in Claims Costs and Expenses $ million (C)	% Savings (C/B)
Total	3,733,000	13, 320	1,665	12.5%

Fuente: Capgemini Consulting Analysis

Otro punto a tener en cuenta es el *pricing* de este seguro considerando el ahorro anterior, algo que puede repercutir en la prima del seguro y de esta forma el asegurado pague menos, en un mayor beneficio para la compañía o en un mix de ambos. Sin duda la modelización de los precios de los seguros mediante la utilización de los contratos inteligentes es un reto para la profesión actuarial.

Además, el pago de los siniestros se producirá de forma inmediata, muy lejos de los días o incluso meses que se tardaba en un seguro de retraso y cancelación de vuelos, tal y como se hace en la actualidad. Esto provoca una enorme

[39] https://www.capgemini.com/consulting/wp-content/uploads/sites/30/2017/07/smart-contracts.pdf

satisfacción al asegurado, y, por tanto, la fidelidad de este en la compañía será mucho mayor. Si le sumamos otro tipo de tecnologías como *Machine Learning*, utilizado en la ciencia actuarial para medir el riesgo de *Lapses* (Caída de la cartera), entre otros, será sin duda un cambio disruptivo en el sector asegurador y la función actuarial.

- **Seguros P2P**: Aunque la cadena de bloques no es necesaria para crear un modelo de negocio peer-to-peer, podría impulsar a que los consumidores participen en los seguros entre iguales. Las características de esta tecnología hacen que una solución basada en Blockchain genere transparencia y sea fiable para los consumidores, y de esta forma, las compañías de seguros puedan automatizar la administración de los servicios peer-to-peer con contratos inteligentes.

- **Seguros por uso:** con la irrupción de nuevas tecnologías como el big data, internet de las cosas y la arquitectura del Blockchain la transformación de los convencionales servicios que ofrecen las compañías aseguradoras será un hecho. Gracias a ello, se podrá ofrecer nuevos productos y servicios como son los seguros por uso, en los que el usuario no solo pagará la prima que mejor se ajuste a su riesgo individual, si no que permitirá pagar solo por el uso que haga del servicio. Imaginemos el caso de que un usuario alquila una bicicleta a un tercero durante un fin de semana, pero quiere asegurarse que ante un posible accidente o robo de la misma, tenga un seguro que responda ante alguna de estas contingencias. Una compañía aseguradora podrá asegurar por días o incluso por horas ajustado a la necesidad de cada cliente particular.

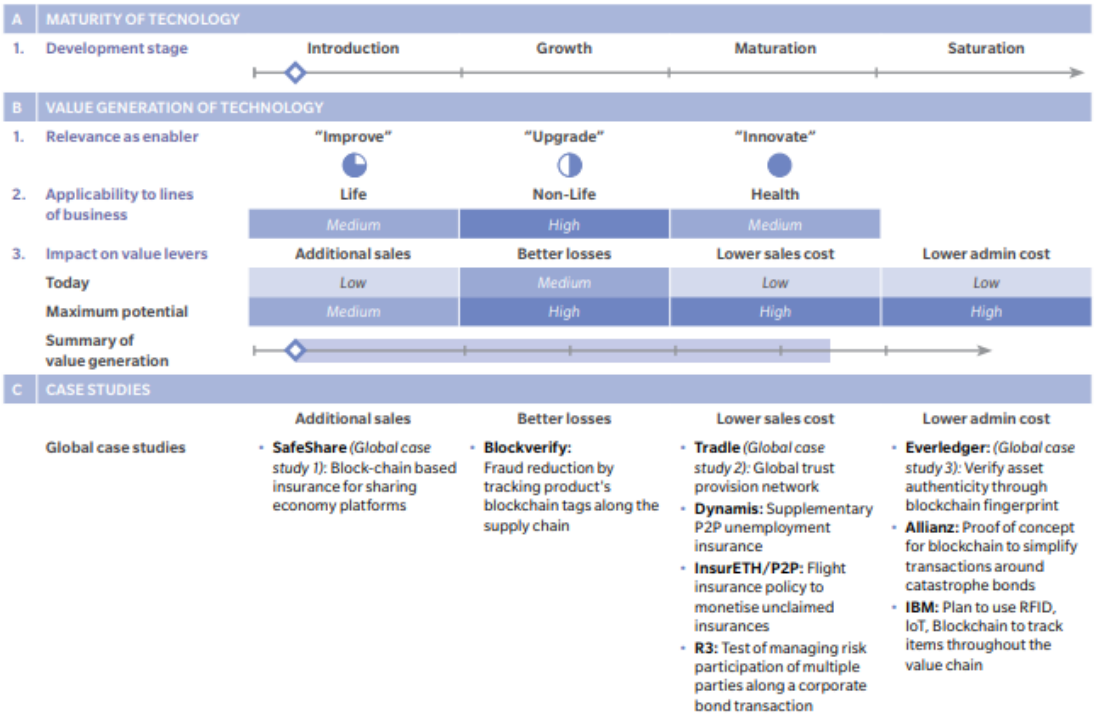
- **Auditabilidad de los procesos:** gracias a las propiedades de inmutabilidad, transparencia y trazabilidad de la tecnología Blockchain, los supervisores y reguladores podrán disponer de herramientas más eficaces y ágiles. Esto puede suponer un control de los riesgos a tiempo real y con ello, nuevas normativas que exijan un menor requerimiento de capital al tener herramientas eficaces de gestión de riesgos.

Son muchas las iniciativas que existen en la actualidad alrededor del ecosistema Blockchain, como Blem, una compañía tecnológica que desarrolla sistemas informáticos para el sector, y que ha empezado a ofrecer contratos basados en Blockchain para reaseguros. Y Safeshare, una startup con sede en el Reino Unido, está utilizando la tecnología Blockchain para dar cobertura de seguros a personas que alquilan las habitaciones libres de sus casas como oficinas.

Estas ventajas y casos de uso son solo un ejemplo de lo que se está investigando en el sector asegurador y otros muchos que se irán viendo a medida que la tecnología Blockchain vaya ganando madurez en el mercado.

La cadena de bloques está posicionada para permitir modelos de negocio innovadores adyacentes a los tradicionales que aportan múltiples beneficios a todas las partes implicadas en un contrato de seguro. Se esperan grandes oportunidades para la generación de valor, además del potencial de generar modelos de negocio con nuevos productos.

Ilustración 17 Evaluación de la tecnología Blockchain



Fuente: Oliver Wyman analysis

El pasado 6 de junio de este año 2018, la consultora Grant Thornton y TIREA[40] (Tecnologías de la Información y Redes para las Entidades Aseguradoras S.A), firmaron un acuerdo para crear la primera plataforma Blockchain adaptada al sector asegurador.

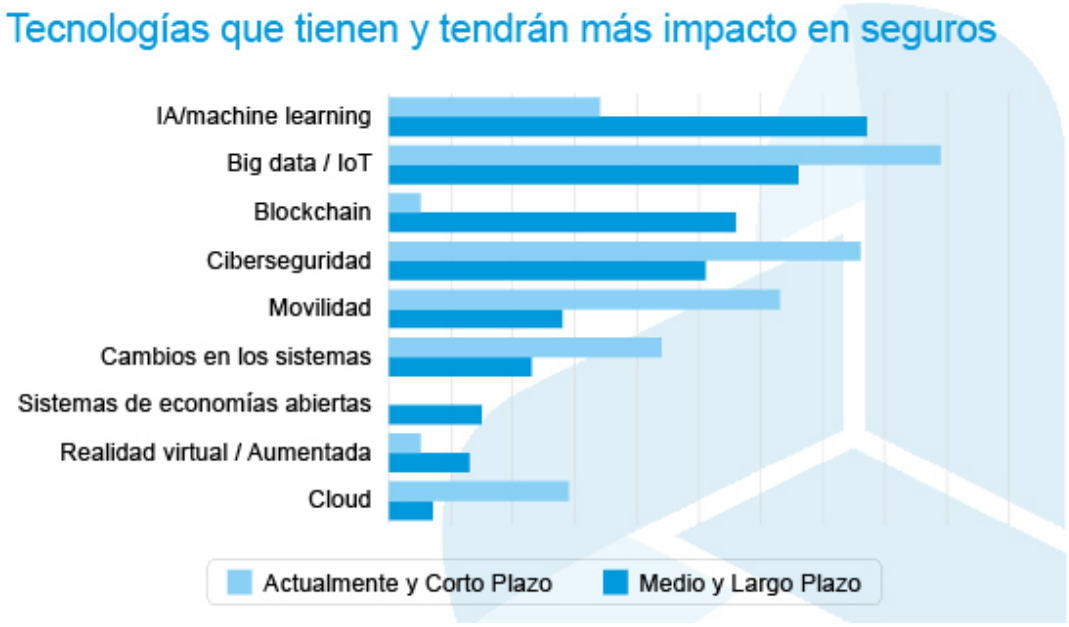
Con este acuerdo, se intentará resolver el problema de la falta de un estándar y de procedimientos automatizados que dificultan la coordinación y el intercambio de información homogénea entre compañías, lo que da lugar a ineficiencias y a costes añadidos. La solución cubrirá el ciclo completo de vida del coaseguro recogiendo toda su compleja casuística y facilitando su automatización, a la vez que permitirá la operatividad entre los datos de las distintas entidades aseguradoras. Según Luis Pastor, Socio de Tecnología e Innovación de Grant Thornton, además de miembro fundador de los consorcios Alastria y de la CECA, manifestó: *La tecnología Blockchain resulta idónea para resolver los principales problemas que hacen que los procesos de*

[40] Respaldada con más de 130 aseguradas, TIREA nace en 1997 para establecer un medio eficaz, seguro y económico, que facilite la comunicación y colaboración necesaria para ayudar en la mejora del negocio de las Entidades Aseguradoras, así como mejorar su eficiencia e impulsar la adaptación a futuras evoluciones tecnológicas del ámbito asegurador.

coaseguros resulten tan difícilmente automatizables. Además. Blockchain actúa como fuente de confianza entre las partes, y su aplicación permite eliminar duplicidades y agilizar procesos, e incluso generar nuevos modelos de negocio. Junto con TIREA vamos a hacer posible una plataforma pionera que permita a las entidades aseguradoras aprovechar, ya hoy, los beneficios de Blockchain en un aspecto de su negocio muy complejo (Grant Thornton, 2018).

Icea, el 13 de junio de 2018, publicó un estudio[41] de las tecnologías que tienen más impacto en el sector seguro, y lo que se espera de ellas en el futuro, en el cual, la cadena de bloques, como se ha visto en otros estudios, se encuentra en una fase introductoria aunque se espera que transforme la industria aseguradora, junto con el *Big Data*, la Inteligencia Artificial o el *Machine Learning*.

Ilustración 18 Tecnologías con mayor impacto en seguros



Fuente: Icea

[41] https://www.icea.es/es-ES/noticias/Noticias/Noticias0618/Dia-13/inteligencia-artificial.aspx

3.5. Casos de uso de la cadena de bloques en otras industrias

La tecnología Blockchain tiene una propiedad fundamental, y es que es refundacional, esto quiere decir que puedes reconstruir muchos sectores, por ejemplo, imaginemos un préstamo bancario a un año establecido en un *Smart Contract* dividida sus partes en términos digitales que son programables, llamado Business as usual[42], en sus términos analógicos y en los oráculos (en este caso podría ser Reuters que me de los tipos de interés a un año). El termino analógico puede ser que yo le pida al banco que me permita hace una mora, de uno o dos meses, y los digitales que, llegado el vencimiento mensual, me cobre los intereses pactados con anterioridad.

Un ejemplo de lo anterior es el caso que han protagonizado las compañías BBVA e Indra el pasado mes de abril de 2018 en el que realizando un préstamo de 75 millones de euros utilizando la tecnología Blockchain. La innovación en este piloto supuso una reducción de tiempo de días a horas y una simplificación de los procesos. La operación se hizo en la Blockchain pública de Ethereum y tanto BBVA como Indra pudieron consultar en todo momento el estado y las condiciones de contratación gracias a la trazabilidad que aporta la cadena de bloques. Desde BBVA se manifestó la seguridad que aporta esta tecnología: *De esta forma se garantiza la inmutabilidad del contrato acordado, ya que cualquier cambio sobre el contrato firmado daría un hash completamente diferente.*

El acuerdo anterior, ha servido de antesala para nuevos negocios por parte del BBVA, y aprovechando las ventajas que supuso su acuerdo con Indra, el banco ha cerrado un nuevo acuerdo en junio de este año 2018, con la compañía Repsol. El acuerdo de un crédito de 325 millones de euros a largo plazo ha permitido reducir el proceso a horas, cuando antes se tardaban días. Este acuerdo se ha desarrollado en el Blockchain privada Hyperledger, registrado en la red Ethereum. Esto supone dotar de transparencia a la operación, además de inmutabilidad, y mejora de procesos en áreas como pagos, emisión de valores o comercio internacional. La directora de experimentación digital de Repsol, Nuria Ávalos, indicó: *Repsol quiere contribuir de forma activa en entornos de colaboración. Blockchain es una tecnología disruptiva que ha venido para quedarse y el acuerdo con BBVA suma en nuestra estrategia para impulsar la digitalización en todas nuestras áreas de actividad.*

Otro caso de uso lo protagoniza la Start up Monuma[43] , que permite a los amantes del arte proteger su patrimonio a través de su aplicación, pionera en el mundo y dedicada a la valoración y certificación de objetos valiosos.

Monuma ofrece a las personas tomar fotos autenticadas, integrarlas de forma inmediata en la cadena de bloques, probar su propiedad y lanzar una estimación en tiempo real del

[42] Business as usual se traduce como los métodos utilizados por una organización conforme a métodos pasados o presentes. Esto implica que las empresas, evitan adoptar cualquier cambio novedoso, debido a su perfil conservador y generalmente adverso al riesgo, les hace asociar cambio con incertidumbre.
[43] https://www.monuma.fr

valor por expertos jurados. Cualquier objeto puede ser evaluado: vinos, pintura, escultura, plato precioso, dispositivo tecnológico, mobiliario...

Otra de las industrias en las que la cadena de bloques está penetrando es en el mundo de la información. Debido a la tendencia de las noticias falsas (*Fake News*) dado que cualquier persona puede publicar en la red, están surgiendo iniciativas de empresas como Userfeeds o Publiq que utilizan "Prueba de evaluación" para medir la importancia de diferentes mensajes en el protocolo. Además, utiliza monedas de reputación para crear un sistema de reputación para que los usuarios eviten la publicación de este tipo de noticias.

Con relación a esta última, el deportista Fernando Alonso ha protegido sus derechos de imagen y videos con Blockchain. Según una noticia en el diario expansión[44] de Julio de 2018, el deportista ha llegado a un acuerdo con Kodakone, plataforma que asegura con esta tecnología rastrear Internet para controlar las licencias de todo contenido audiovisual y evitar posibles robos.

Otra industria que está atenta a la tecnología Blockchain, aunque con cierto grado de escepticismo es el Registro de la Propiedad y la Notaría, dado que las propiedades de esta tecnología podrían sustituir alguna de las funciones que hoy realizan, como pueden ser la trazabilidad de una casa, hoy si necesitamos saber si el historial de una propiedad y si esta tiene cargas, se solicita en el registro de la propiedad una nota simple donde viene la información de forma pública. Con la tecnología Blockchain, cualquier persona podría quién es el propietario de cierta vivienda, si ha tenido dueños anteriores y demás información que necesitamos saber, o en la notaría se podría sustituir la figura del notario como el tercero de confianza al enajenar o comprar una vivienda, haciéndose esta operación en la cadena de bloques sin necesidad de un tercero.

Por último, entre otras muchas industrias y empresas que están apostando por esta tecnología, es Maersk, un gigante dedicado al transporte marítimo, que ha realizado con éxito proyectos pilotos en los que ha aplicado el modelo de la cadena de bloques en el transporte internacional de mercancías, gracias a la trazabilidad de los contenedores marítimos mediante la digitalización de los mismos, aportando transparencia y consiguiendo un intercambio seguro y confiable de información entre los socios comerciales.

[44] http://www.expansion.com/directivos/deporte-negocio/2018/07/03/5b3a8605e5fdea8f2f8b45ba.html

PARTE IV: Aspectos legales

De forma habitual, las instituciones privadas suelen abrazar las nuevas tecnologías e innovaciones tecnológicas antes que los organismos públicos puedan adaptar estas innovaciones en su regulación. Esto puede suponer que una compañía pueda operar bajo un "vacío" legal y le permita obtener ventajas competitivas, o que pudiendo obtener estas ventajas, no pueda implantarlas dado que la ley actual no permita estas innovaciones y deba esperar a modificaciones en la misma para que puedan implantar estas nuevas tecnologías conforme a la ley o puedan operar nuevas Startups. Respecto a esto último, los países que son más ágiles a la hora de adaptar su regulación suelen acoger a las nuevas compañías ávidas de empezar a operar, y que en su país habitual no puede hacerlo aún.

En este sentido hay dos aspectos legales en los que se está trabajando actualmente y que hay que tener en cuenta a la hora de implantar la tecnología Blockchain en los modelos de negocio.

- La nueva normativa de protección de datos GDPR
- El Sandbox

4.1. Normativa de protección de datos GDPR

El Reglamento General Europeo de Protección de Datos (RGPD) fue adoptado por la Comisión Europea el 4 de abril de 2016 y entró en vigor el 25 de mayo de 2018. Eso incluye a las empresas que se encargan de procesar los datos, es decir, para almacenar, analizar u otros medios de procesamiento.

El reglamento establece que las instituciones que tratan datos deben aplicar un conjunto de medidas que deben cumplir en consonancia con las nuevas normas y principios que recoge la normativa.

Según el Art. 1 parte 1 del reglamento, este se aplica sólo al tratamiento de "datos personales" que es legalmente definido como, "cualquier información relativa a una persona física identificada o identificable (persona a la que se refieren los datos); un dato identificable de persona física es aquella que puede ser identificada, directa o indirectamente, en referencia a un identificador como un nombre, un número de identificación, datos de localización, o a uno o más factores específicos de los factores físicos, fisiológicos, genéticos, mentales, económicos, culturales o identidad social de esa persona física;" (Art. 4 par. 1 GDPR)

Para determinar si una persona física es identificable, deben tenerse en cuenta todos los medios que están a su alcance y que sea razonablemente probable que el responsable de

estos datos o cualquier otra persona lo utilicen. Eso significa que no importa si la empresa tiene o no la intención de identificar al interesado. Sólo los aspectos técnicos y legales son relevantes.

Por lo tanto, los principios de la protección de datos no deben aplicarse a los datos de la empresa ni a los datos anónimos. Hay varias tecnologías que pueden anonimizar los datos hasta cierto punto. Agregación, encriptación y tokenización son las técnicas más comunes. Estas propiedades están definidas dentro de una red Blockchain.

Entender el impacto del GDPR en la Blockchain, ya sea procesando los datos en redes privadas, como Hyperledger o Corda, o cadenas de bloques públicas, como Ethereum se debe tener en cuenta:

1. ¿Se aplica el GDPR a una empresa que opera una cadena de bloques pública, privada o de consorcio?

2. ¿Existen datos en las cadenas de bloques que se consideran Información de Identificación Personal?

En caso de que ambas preguntas sean afirmativas, deben surgir requisitos regulatorios más explícitos en este sentido.

En el caso de las Blockchain que son completamente públicas, ejemplo de Bitcoin, la red, al ser distribuida, no "pertenece" a ninguna compañía o persona de forma específica. A diferencia de Google, no existe un controlador específico que pueda ser obligado a garantizar que los datos sean borrados y por tanto dejen de ser accesibles.

Cuando utilizamos una red privada como Ethereum podemos hacer transacciones de valor como ethers (ETH) o bien un contrato inteligente. Cuando se hace una transacción en esta red, especificamos una dirección de destino, una cantidad de ethers, y con ellos unos datos como pueden ser saldos de cuenta o la reputación de un usuario (Moser, 2017).

Otro de los factores que debemos tener en cuenta es el derecho al olvido (Articulo 17 GDPR).

El "derecho al olvido" fue el tema de una famosa sentencia del Tribunal de Justicia Europeo en 2014. Según la Agencia Española de Protección de Datos (AEPD), el *derecho al olvido hace referencia al derecho que tiene un ciudadano a impedir la difusión de información personal a través de Internet cuando su publicación no cumple los requisitos de adecuación y pertinencia previstos en la normativa*.

El articulo 17 apart. 2 expresa: *Cuando haya hecho públicos los datos personales y esté obligado, en virtud de lo dispuesto en el apartado 1, a suprimir dichos datos, el responsable del tratamiento, teniendo en cuenta la tecnología disponible y el coste de su aplicación, adoptará medidas razonables, incluidas medidas técnicas, con miras a informar a los responsables que estén tratando los datos personales de la solicitud del*

interesado de supresión de cualquier enlace a esos datos personales, o cualquier copia o réplica de los mismos.

El derecho al olvido bajo el GDPR choca fuertemente con el hecho de que las cadenas de bloques están destinadas a mantener la inmutabilidad de los datos. Una manera de solventar esto es trabajar en las cadenas de bloques con seudónimos que vayan ligado datos encriptados, cuyos datos se encuentre fueran de la red, y que solo el dueño de los datos o persona autorizada puede consultar dichos datos. Este asunto sin duda debe seguir trabajándose dado que podría debilitar la seguridad de esta tecnología, al estar almacenados fuera de la red.

Cuando los datos son almacenados en cadenas de bloques privadas o en consorcios, estos pueden establecer en sus protocolos normativas que se ajusten a esta norma de protección de datos y de esta manera poder cumplir con esta normativa en sus operativa.

Sin embargo, cuando hablamos de Blockchain públicas, se podrían acoger a lo comentado anteriormente, con la tesitura de que estos datos no pertenecen a ninguna empresa o persona en particular por lo que nadie tiene la responsabilidad de borrar los datos de una red.

Sin duda, en el futuro cuando la tecnología Blockchain alcance una mayor madurez en el mercado, surgirán nuevas disposiciones o normativas que se ajusten mejor a la operativa de la cadena de bloques.

4.2. Sandbox

El sector financiero y asegurador, está atravesando un cambio estructural debido entre otras cosas, a las nuevas tecnologías, y en el que el usuario busca flexibilidad, agilidad, eficiencia y servicios a la carta en cualquier soporte tecnológico, preferentemente en dispositivos móviles. Estos avances están produciendo cambios sustanciales en los procesos de producción, en modelos de negocio, la relación con el cliente, canales y en la propia estructura del negocio.

El *Sandbox*, o caja de arena en su significado en español, es una normativa que permite un entorno de pruebas que está controlado y delimitado por los organismos públicos mientras se esté bajo esta denominación legal.

Cuando una entidad no puede operar bajo la normativa vigente, la aprobación del *Sandbox* dicha entidad permitiría entrar en fase experimental, donde bajo la supervisión de los reguladores puedan ofrecer sus servicios operando dentro del marco legal del *Sandbox* e informando a sus clientes que se está bajo esta aprobación y los riesgos que esto conlleva.

¿Por qué es importante la aprobación de un *Sandbox*? La asociación española de Fintech e Insurtech junto a la compañía Hogan Lovells, lanzó en marzo de 2018 una propuesta de implantación de un Sandbox en España y en dicho informe se señala lo siguiente: (AEFI, 2018).

- **Desarrollo de la innovación:** Permite actuar a nuevos modelos de negocio que trabajan con el uso de datos y nuevas tecnologías para obtener recursos innovadores y eficientes para sus clientes.
- **Fomento de la competencia:** Al ser más flexible en el cumplimiento de la regulación y reducir las barreras de entrada, favorece el aumento de nuevos competidores, provocando una mejora en los servicios y productos del mercado.
- **Revisión constante de la legislación:** Permite obtener un entorno donde los marcos regulatorios deban adaptarse a los cambios que los sectores Fintech e Insurtech necesitan para operar con normalidad y no retrasar la innovación.
- **Minimización de riesgos:** Es un ecosistema perfecto para generar un *win to win* donde puedan producirse un aprendizaje mutuo sobre los riesgos y oportunidades en la aplicación de las nuevas tecnologías en nuevos modelos de negocio.

En este sentido, los reguladores competentes en cada área, como pueden ser la Comisión Nacional del Mercado de Valores (CNMV) o la Dirección General de Seguros y Fondos de Pensiones (DGSFP), deben aprobar los requisitos establecidos que permita operar bajo este nuevo marco legal. Algunos de los requisitos técnicos, son los siguientes:

- Establecer un periodo limitado en el que se opere bajo el marco *Sandbox*.
- No tener más de un número determinado de clientes o consumidores.
- No superar un volumen global de facturación.
- Limitar el riesgo en productos y/o servicios.
- Tener implantando un servicio de reclamaciones para posibles quejas o demandas provenientes de clientes.

El pasado mes de mayo de 2018, el ministerio de economía, industria y competitividad publicó un Proyecto de Ley de medidas para la transformación digital del sistema financiero. Según la propuesta, la regulación financiera tiene que adaptarse para garantizar el cumplimiento de los objetivos de política pública, garantizar la protección al consumidor, evitar la financiación del terrorismo y el blanqueo de capitales.

Además, este proyecto de ley tiene como objetivos:

- Aumentar el marco de protección de los consumidores.
- Facilitar la innovación digital aplicada a los servicios financieros.
- Aumentar las herramientas de las que disponen los reguladores y supervisores.
- Impulsar la innovación tecnológica de la economía del país.
- Promover la eficiencia de las entidades y el aprovechamiento de las economías de escala.

- Reforzar la seguridad jurídica.
- Mejorar la integración del sector financiero en la sociedad.
- Mantener la eficacia de la política financiera mediante una transformación tecnológica organizada.

Con la aprobación de este *Regulatory Sandbox*, España está apostando por la transformación digital, impulsando la actividad empresarial y la creación de empleo. Se pretende, apoyar esta transformación digital de la economía controlando los riesgos que supone, incorporando nuevas herramientas para reguladores y supervisores. La aplicación de este marco regulatorio puede implicar la es atracción de talento y nuevas inversiones en nuestro país desde el exterior y fomentar la competencia.

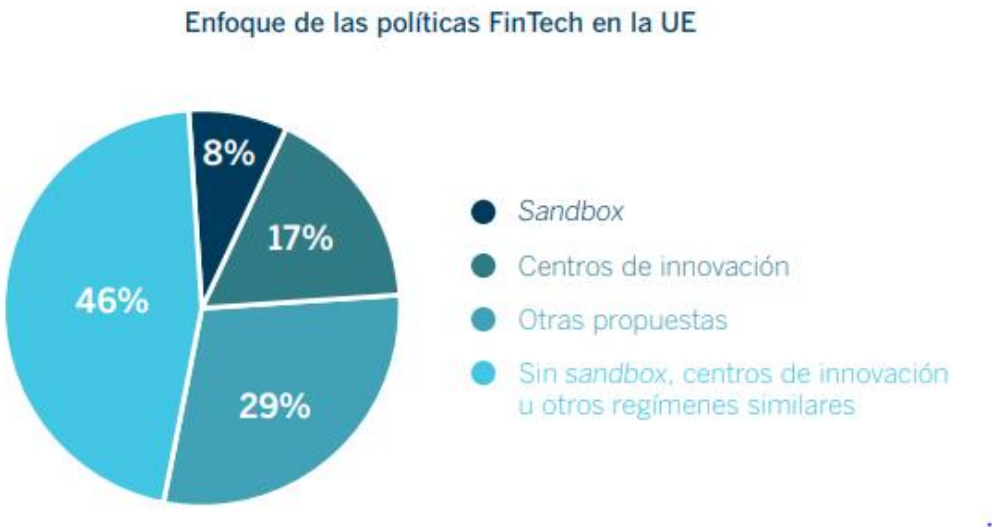
De esta forma nuestro país se uniría a los países que ya están aplicando el *Regulatory Sandbox* como Reino Unido, México, Singapur, Hong Kong, Abu Dabi, Suiza, Australia y EEUU.

En el caso de Reino Unido la FCA (Financial Conduct Authority)[45], en el año 2016 aprobó la implantación de este proyecto en el cual las empresas que fueron seleccionadas[46] se beneficiaban de un marco regulatorio en el cual podrían empezar a trabajar en la implantación de su negocio a modo de pruebas, con el objetivo de una vez pasado dicho periodo, pudieran someterse a la regulación vigente y poder obtener la licencia que se pretendía de forma inicial.

La Autoridad Bancaria Europea (EBA con sus siglas en inglés), publicó en agosto de 2017 un *discussion paper*[47] sobre el número total estimado de regimenes Sandbox y otros intrumentos similares de innovación en la Union Europea (FinReg, 2017).

[45] La Financial Conduct Authority (FCA) es la autoridad reguladora británica en la que se encuentran aquellas empresas financieras no intermediarias de crédito, entre ellas las Fintech, aunque no se limitan a estas últimas.
[46] La FCA lanzó un primer proceso en el que se presentaron 69 empresas, de las cuales fueron aceptadas 18. El éxito de este primer proceso provoco que en un segundo lanzamiento se presentaran 77 empresas, y se aprobaron 24 que están sometidas a este marco legal de pruebas.
[47] European Banking Authority (EBA): Discussion Paper on the EBA's approach to financial technology (FinTech). 4-8-2017 (respuesta a la Comisión Europea).

Ilustración 19 Políticas de las Fintech en la UE



Fuente: FinReg360: Al calor de la regulación

Una vez superada esta fase experimental, se tendría que analizar la fase post-experimental en la que podría darse varias opciones:

1. Una vez superado con éxito el periodo de prueba, salir del marco regulatorio de esta "caja de arena" y operar bajo la normativa general como una compañía más.
2. La prórroga de esta condición dentro del *Sandbox* que permita a la empresa seguir operando bajo la supervisión de los reguladores, en la que estos últimos consideraran que la quedaría poco tiempo para ajustarse a la regulación fuera del *Regulatory Sandbox*.
3. La implantación de esta compañía al sistema económico haya sido tan favorable que haya atraído a nuevas compañías a la realización de procesos y modelos de negocios parecidos y por tanto los reguladores, como proceso de aprendizaje, tengas que regular de forma general, cambiando la regulación o la ley, adaptándose a las nuevas formas de negocio que permitan el impulso de la innovación y el desarrollo económico.
4. Que la idea de negocio fracase, y por tanto se abandone la actividad, o incluso la implantación del *Sandbox* no tena éxito y se deje de aplicar.

PARTE V: Análisis empírico Prototipo: Aplicación práctica

5.1. Introducción del producto

Como parte de esta investigación, se propone un nuevo producto asegurador, en el que se integrarán los elementos que se han estudiado hasta el momento enfocado desde el punto de vista actuarial.

Siguiendo el paradigma Insurtech se analizará las posibilidades de uso que podría desarrollarse mediante la tecnología Blockchain, y que, además, resolvería algunos problemas que existen en la actualidad. Las opciones que se han estudiado han sido las siguientes:

- **Un seguro para alquiler de casas mediante la plataforma Airbnb**: son varios los problemas que supone el alquiler de una propiedad en la plataforma Airbnb, tanto por parte del propietario, como por parte del cliente que alquila la propiedad. Cuando un propietario alquila su propiedad corre el riesgo de que el usuario que ha reservado pueda realizar algún daño dentro de la propiedad, ocasionando desperfectos en la misma, daños a terceros, como puede ser un vecino o la comunidad si se produjese en el bloque, o incluso daños del propio usuario dentro de la propiedad. Dadas estas situaciones, se requerirá de un seguro de hogar, de un seguro a terceros y responsabilidad civil.

  Con el uso de los *Smart Contracts* se podría solucionar algunos de estos problemas. Por ejemplo, el propietario de la vivienda podrá disponer en todo momento de un historial de la persona que acaba de contratarle el producto, dado que todas las operaciones que ha hecho con anterioridad permanecen inalteradas dentro de la red, y en caso de mala reputación, obligar al usuario al pago de un seguro adicional o incluso denegar la operación.

  Por otra parte, cara al usuario, al contratar un seguro para la reserva del alojamiento, podría solucionar el problema de confianza que reserve un alojamiento que no existe, dada la desconfianza de hacer la reserva a una persona desconocida, y en otro lugar, ya sea nacional o internacional. Al contratar el seguro, y en caso de que llegara al domicilio y no existiera, este podría devolver el coste de la reserva más una cantidad en concepto de indemnización.

  Además de todo lo anterior, el uso de este producto asegurador contaría con la gran ventaja de tener los pagos automatizados al ejecutarse mediante contratos inteligentes, y de unos costes de transacción menores.

- **Seguro para entrada de eventos**: son muchas las situaciones en las que una persona ha comprado unas entradas para un concierto, y este, al final, por no ha se ha podido producir debido a cualquier circunstancia que lo haya impedido.

  Con un seguro que cubra la contingencia de que no se produzca el evento, y mediante la implementación de un contrato inteligente, se procedería a la devolución del coste de las entradas, una vez que la red haya validado que efectivamente, el concierto no se ha producido, y por tanto el usuario, dispondrá en su cuenta y de forma inmediata del dinero en su cuenta. Todo ello, sin que sea necesaria una reclamación por parte del asegurado, y ningún trámite por parte de la entidad aseguradora.

  Este producto además podría cubrir la contingencia de que el asegurado, no pueda asistir al mismo, por diferentes razones como pueda ser por motivo de salud.

- **Seguro para personas que no tienen acceso**: un problema que existe en la actualidad es que una gran parte de la población no puede acceder a seguros debido a la baja renta de la que disponen. Con el uso de la tecnología Blockchain, al reducirse en gran parte los costes de gestión y administración, el riesgo de fraude, y demás características que representan un menor coste para la compañía aseguradora, las entidades aseguradoras pueden bajar el precio de la prima y, por tanto, acceder a mercados que hasta ahora no han sido posible.

  Un ejemplo de este caso sería una familia que vive de sus tierras en una zona, imaginemos en el sur de México, Chiapas, y que no tiene seguro por dos motivos, falta de cultura financiera (un gran porcentaje de la población mexicana no tiene cuenta bancaria), y, en segundo lugar, el coste del seguro no es accesible para ellos. Un seguro basado en tecnología Blockchain y *Smart Contract* podría cubrir que, debido a causas meteorológicas, en caso de pérdida parcial o total de la cosecha, se procediera a indemnizar a la familia de forma automática, permitiendo, en muchos casos, poder ayudar a esta familia a cubrir pérdidas que podrían ser devastadoras sin un seguro que les cubra. La forma de comprobar el siniestro sería mediante un oráculo que verifique que efectivamente se ha dado cierto temporal, y cómo ha impactado, y mediante un sistema de dron, se podrían tomar fotografías y videos del lugar, sin la necesidad que un perito tenga que ir al lugar de los hechos.

  Este producto puede cumplir una función social, dando imagen de marca a la compañía, y además puede aumentar su carácter preventivo, dado que, mediante alertas, puede instruir a la familia a que tome ciertas medidas, ante la llegada inminente de un temporal que dañe sus tierras.

- **Seguro para personas que salen a correr**: este producto asegurador para corredores (runners) catalogado como seguro por uso, en el cual, y mediante el ecosistema Blockchain, se activará mediante un contrato inteligente, la póliza de dicho seguro, cuando el corredor inicia la actividad, y, se parará, cuando el mismo finalice dicha actividad. Esto será posible gracias a un smartphone o cualquier wearable[48] que utilice el asegurado, y con el que será posible saber si el asegurado está o no realizando la actividad bajo la cual se engloba el seguro. La contingencia cubierta por este seguro será la de accidente y de muerte súbita.

Este trabajo se centrará en el último caso mencionado, el seguro para corredores, en el que se analizará las propiedades de este, se hará un desarrollo de una aplicación práctica actuarial, se estudiarán las propiedades del mismo, el cálculo de la tarifa bajo el Principio de Prima del Valor Esperado (PPVE), y se examinará las propiedades por separado de cada una de las partes que se utilizan en este producto, y responder a la pregunta de si es necesario o no una Blockchain, y si fuera afirmativa, que valor agrega al seguro.

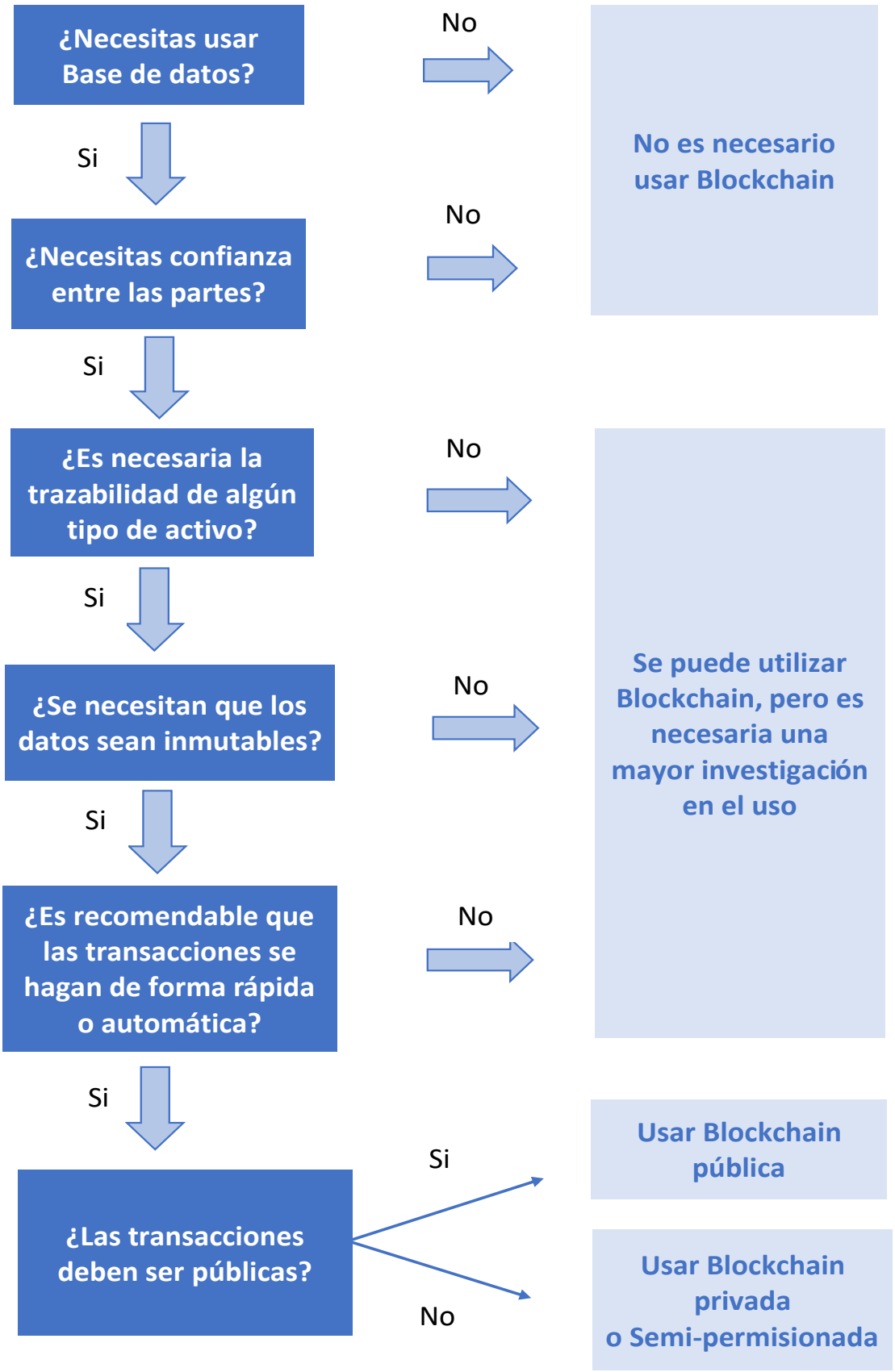
5.2. ¿Hace falta Blockchain en este producto?

Como se ha abordado en este estudio, muchas son las propiedades que tiene la cadena de bloques, pero bien es cierto que no siempre es necesario usar esta tecnología para todo tipo de producto o servicio. Por tanto, se va a estudiar si en este seguro es útil utilizar la cadena de bloques, y en caso afirmativo, qué valor aporta adicional al seguro con la utilización del Blockchain en este.

Hay varias preguntas que son necesarias hacerse para saber si es necesario o no utilizar la cadena de bloques. Según el World Economic Forum, se proponen las siguientes: (WEC, 2018).

[48] Wereable se refiere a la tecnología vestible (traducido al castellano), tecnología corporal, ropa tecnológica, ropa inteligente o tecnología ponible, es decir, aquel dispositivo electrónico que se lleva sobre, debajo o incluido en la ropa. Otras de sus características es que permite la multitarea por lo que no requiere dejar de hacer otra cosa para ser usado y puede actuar como extensión del cuerpo o mente del usuario.

Ilustración 20 ¿Es necesario utilizar Blockchain?



Fuente: Elaboración propia a partir del informe del World Economic Forum

En este caso, como se ha mencionado con anterioridad, es un seguro para corredores, que necesitará estar conectado a un dispositivo electrónico, primero para detectar que se está ejecutando la actividad, y segundo para recalar los datos necesarios. Por tanto, es necesario utilizar una base de datos.

El concepto de confianza es un aspecto clave en este seguro. Bien es cierto, que se podría lanzar al mercado este tipo de seguro, solo es necesario disponer del dispositivo electrónico o *wereable* y la aceptación de las partes para establecer el contrato de seguro. Sin embargo, el hecho de no utilizar la tecnología Blockchain puede romper esta confianza debido a que se esté utilizando este dispositivo de manera fraudulenta o se puedan modificar o hackear los datos, tanto por parte del asegurado como del asegurador. Entonces respondiendo a la segunda pregunta anterior, se establece necesario de tener confianza de las partes dada las características de la cadena de bloques en cuanto a seguridad se refieren.

La siguiente pregunta de si es necesaria la trazabilidad, es clara la respuesta, pues se necesita de tener un historial confiable y consultable en cualquier momento que permita evaluar la siniestralidad y el perfil de riesgo del cliente para el cálculo de la prima.

En cuanto a la inmutabilidad de los datos, tener la seguridad de que ninguna de las partes puede borrar ningún dato y que permanece de forma perenne, dota al producto de una seguridad adicional, algo también necesario en transacciones B2C[49].

Este producto, cuenta con la característica que es ejecutado mediante contratos inteligentes, que detectan la actividad, la posible contingencia, y en caso necesario, de ejecutar el pago de la prima y/o siniestro. Esto supone que se ejecute de forma inmediata y automática todas las transacciones realizadas entre las partes, por tanto y contestando de forma afirmativa todas las preguntas, se considera necesaria la utilización de la cadena de bloques en este seguro. En caso negativo, bastaría con la utilización de una base de datos, tal y como se hace hasta ahora.

Otras ventajas de utilizar Blockchain en el seguro, es el ahorro de costes, al utilizar *Smart Contrats*, se eliminan costes de gestión y administración, por tanto, puede repercutir en un mayor beneficio para la compañía, un menor coste para el cliente y una mayor eficiencia en el producto.

Además, la agilidad de uso de este producto proporcionará satisfacción al asegurado, al no tener que reclamar en caso de que lo necesite, y al pagar solamente por el uso que el cliente le quiera dar. Esta satisfacción, en la mayoría de los casos, se manifestará en una mayor fidelidad del asegurado en la compañía, por lo que la cartera tendrá un menor número de caídas, con respecto del seguro tradicional.

A todo lo anterior, se le suma disminuir el riesgo operacional, que es el riesgo de pérdida derivado de disfunciones o fallos en personal, sistemas, procesos internos, o

[49] B2C se refiere a la actividad comercial entre un negocio y un consumidor individual.

bien producido por circunstancias externas. Esto también genera a la compañía un menor coste.

Y, por último, además de otras características que se han mencionado en este trabajo de la cadena de bloques, la compañía al utilizar Blockchain controlará de una forma mucho más eficiente el riesgo de fraude, y/o actuación de mala fe por parte del asegurado (Art. 19 de la Ley del contrato de Seguros).

5.3. Definición y motivación del seguro para corredores

Considerando lo anterior, se busca crear un producto innovador, que llegue a un colectivo importante y que solucione problemas que hasta ahora no se había podido lograr.

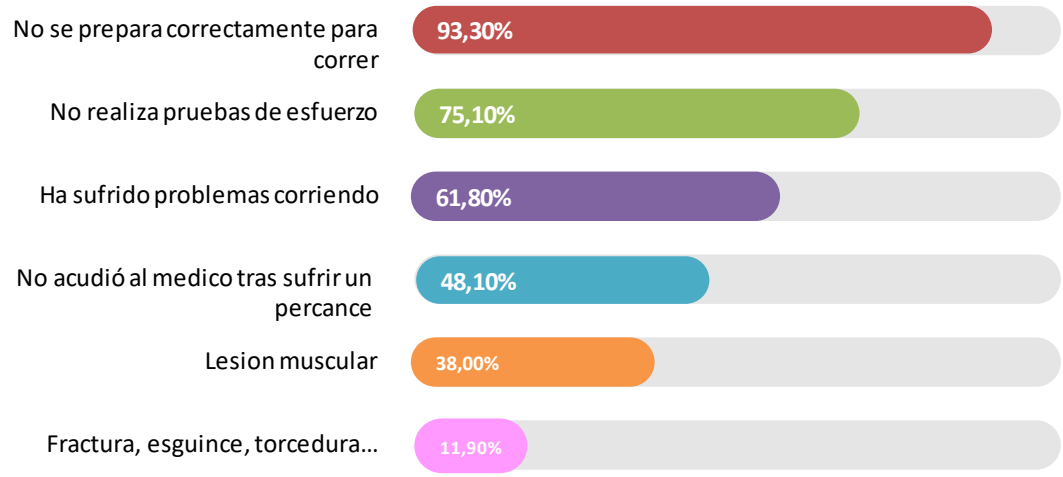
En primer lugar, este seguro cuenta con las siguientes características:

- Seguro paramétrico que cubre las contingencias de accidente, muerte súbita y fallecimiento del corredor durante el desarrollo de la actividad.
- Es un seguro por uso, por tanto, el asegurado solo pagará según la práctica que haga de este deporte.
- Al reducirse la prima, tanto por el ahorro de costes, como al ser un seguro por uso, podrá llegar a un mayor colectivo.
- Un seguro innovador, y que podrá servir de referencia a otros colectivos.

El colectivo objeto del seguro será en este caso, los corredores en España entre los 15 y los 69 años, y que ya sea de manera esporádica o habitual practican *running*. Según datos del Instituto Nacional de Estadística y un estudio de Cinfa Salud, en España hay 33.202.992 habitantes entre estas edades, y de los cuales, 16.521.937 personas, entre hombres y mujeres, que practican este deporte.

Además, el estudio de Cinfa Salud, con el aval de la Sociedad Española de Medicina del Deporte, en España el 93.3% de los corredores no se prepara de una forma correcta, y el 61.8% del total de los corredores, han sufrido problemas corriendo el último año. (CinfaSalud, 2017).

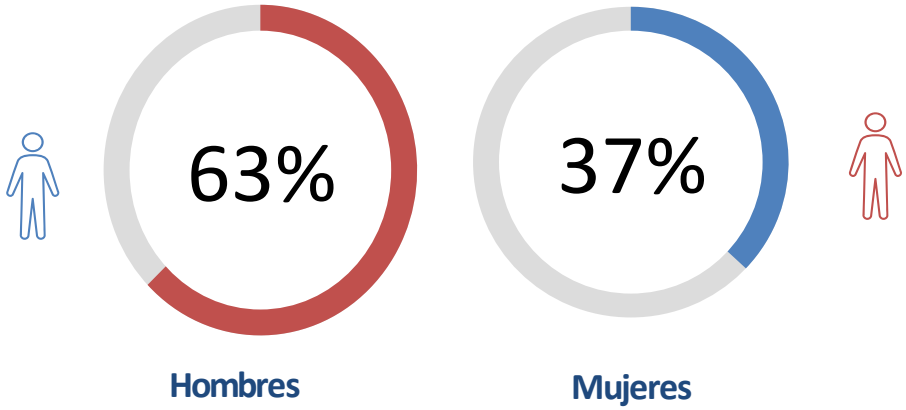
Ilustración 21 Estudio Cinfa Salud sobre lesión en corredores/as



Fuente: Elaboración propia a partir del informe de Cinfa Salud

En este mismo informe, se muestra que el 63% de los corredores son hombres y el 37% mujeres.

Ilustración 22 Porcentaje de corredores según género



Fuente: Elaboración propia a partir del informe de Cinfa Salud

Este seguro, como se ha mencionado con anterioridad, será un seguro por uso, por tanto, tarificado según el corredor/a practique este deporte, que en algunos casos puede ser considerado micro seguros si los corredores salen de forma esporádica, y que cubrirá las contingencias de accidente, y muerte súbita.

5.4. Pruebas de concepto

Durante este estudio se ha hablado y aportado diferentes estudios en los que se establece que la tecnología Blockchain está en una fase introductoria, pero ¿qué significa esto? ¿Qué hacen las compañías en esta fase?...

Las compañías que están invirtiendo en esta tecnología, aparte de investigar y poner su dinero en I+d+i, están desarrollando pruebas de conceptos y proyectos piloto.

Las pruebas de concepto o *proof of concept* (PoC), como generalmente se conocen, significan literalmente evidencia que demuestre que un diseño, concepto, idea de negocio, etc., es factible.

De acuerdo con la definición anterior el objetivo de producir este PoC no debía centrarse demasiado en muchos detalles sobre cualquier seguro existente, sino que, en lugar de ello, proporcionar pruebas a través de un experimento para demostrar cómo la cadena de bloques proporciona una solución elegante a algunos problemas genéricos a los que se enfrenta la industria y tener una visión clara de las ventajas que aporta con respecto a soluciones tradicionales.

5.5. Funcionamiento del seguro

Según se anticipó en páginas anteriores, el funcionamiento de este seguro se ejecutará mediante contratos inteligentes. De esta forma, se podrá detectar cuando el usuario inicia y finaliza la actividad, siempre y cuando esté conectado con un dispositivo electrónico, como puede ser el *Smart Phone*, un reloj o una pulsera inteligente, en caso contrario, no se cubriría al asegurado al no poderse registrar la actividad.

Según el estudio de Cinfa Salud, más de la mitad de los corredores utilizan su teléfono para correr, y un 43% otro dispositivo electrónico. Además, según un estudio del *Institute for Medicine, Informatics & Economics*, de la Heilbronn University, Alemania, un 10% de los corredores utiliza más de un dispositivo para correr (Pobiruchin, Accuracy and Adoption of Wearable Technology Used by Active Citizens:A Marathon Event Field Study, 2017).

Otra característica es que es un seguro paramétrico, cuya definición es: aquella cuya resolución, que dará lugar a la correspondiente indemnización, se resuelve de manera objetiva. En este caso, al tratarse de un contrato inteligente, su resolución está vinculada a un algoritmo registrado en una plataforma Blockchain, por lo que la condición de objetividad se cumple en su totalidad debido al consenso.

5.5.1. Ventajas

Hay varias ventajas que supone este seguro gracias al uso de las tecnologías de la cadena de bloques y el internet de las cosas.

- Se eliminan intermediarios, y se automatiza la contratación del seguro, dotando de eficiencia y rapidez al seguro.
- Al establecer mediante contratos inteligentes, los pagos se ejecutan de forma inmediata, tanto por parte del asegurado con el pago de la prima, como por parte de la compañía, con el pago del siniestro en caso de producirse.
- Adaptado a las necesidades del colectivo.
- Se generan gran cantidad de datos biométricos que servirán para tener un mejor perfil del corredor/a.
- Puede servir como seguro preventivo, dando pequeñas pautas a las personas aseguradas, como pueden ser un estudio de la pisada, hábitos de alimentación y guías que generen una mejor salud del deportista y a un menor número de siniestros.

5.5.2. Desventajas

Existen algunas limitaciones o desventajas que deberían suplirse en este producto. Entre ellas se destaca:

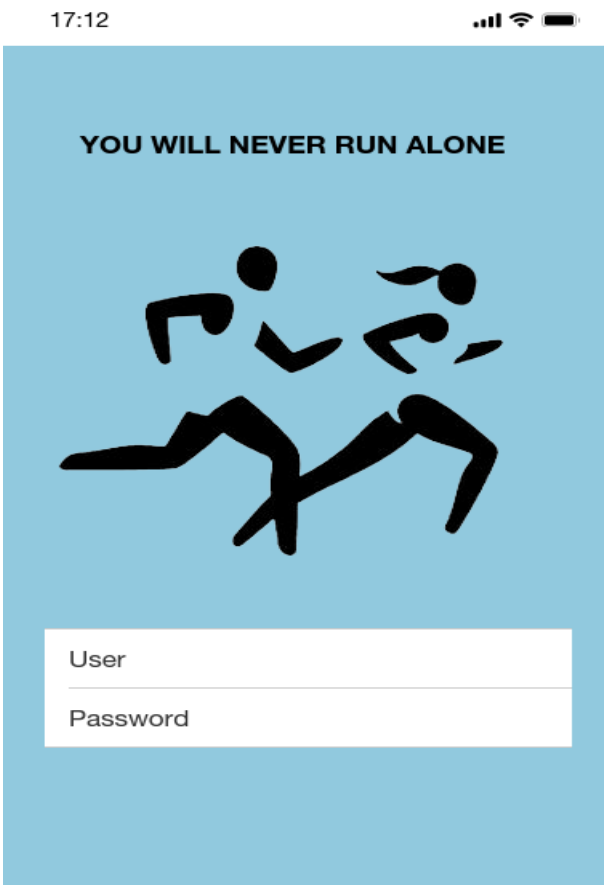
- El corredor/corredora debe practicar la actividad con un dispositivo inteligente que registre la actividad.
- El dispositivo debe estar conectado, por tanto, existe el riesgo de fallo del dispositivo que provoque no estar protegido ante el seguro contratado.
- El coste adicional que supone para el asegurado/a el dispositivo electrónico. Existen diversas compañías aseguradoras, que, para su seguro de vida, la póliza y/o la prima está vinculada a que el asegurado cumpla una serie de objetivos, como son andar 10.000 pasos, y regalan al contratar la póliza el dispositivo electrónico que permita registrar dicha actividad.

5.6. Prototipo App móvil e Internet of Thing

A este producto asegurador se le ha llamado: *You Will Never Run Alone* y se ha diseñado un prototipo para una aplicación móvil y otra para otros dispositivos electrónicos como puede ser un *Smart Watch*, que permitirá ver cómo podría interactuar el asegurado con este seguro y el diseño de la interfaz de usuario.

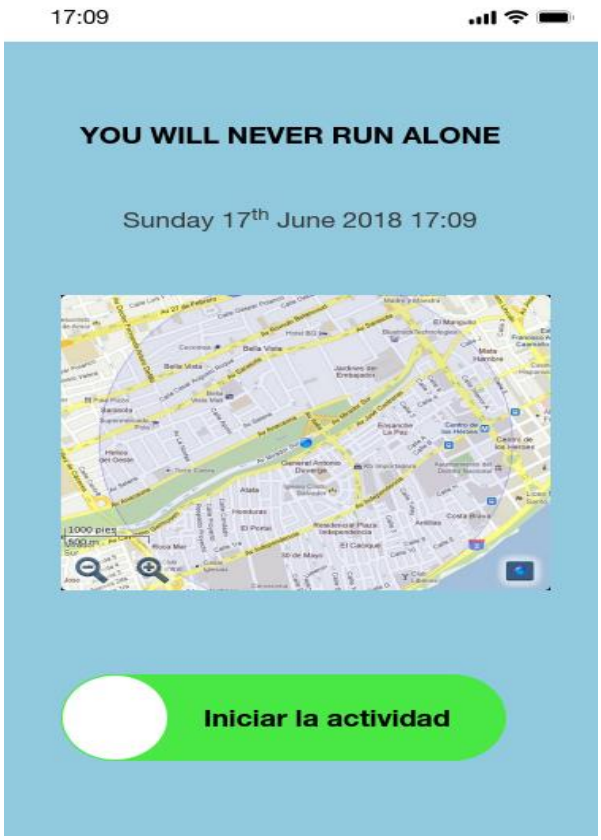
5.6.1. App móvil

La aplicación móvil cuenta en una primera de instancia del registro del corredor antes de iniciar la actividad que le permita identificarse. La representación de esta primera pantalla es:



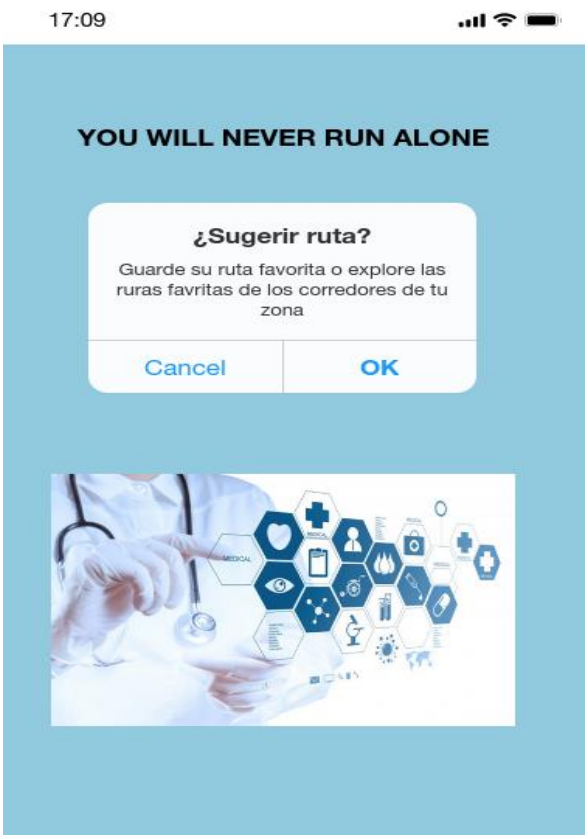
Una vez que el usuario/a se ha registrado, en este caso, al utilizar Blockchain, el usuario/a puede tener un registro único, y utilizarlo para todas las compañías, tal y cómo se explicó en el apartado de *Know your customer* y poner su clave privada para acceder al sistema.

Una vez registrado, la aplicación le mostrará la siguiente pantalla:



En esta pantalla, se le mostrará la ubicación de la persona asegurada y cuando la persona esté preparada para iniciar la actividad, tan solo tendrá que mover la barra, y se activará el contrato.

Una vez realizado esto, la aplicación le podrá recomendar sus rutas favoritas, o rutas favoritas de otros corredores de la zona y se lo mostrará que está siendo asegurado.

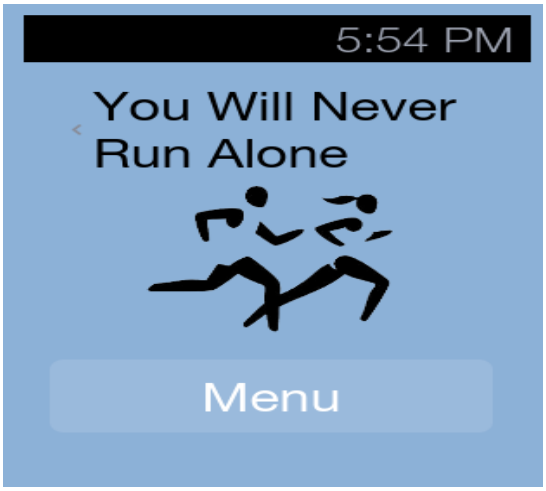


Por último, una vez acabada la actividad, esta quedará registrada y se le mostrará el coste de la póliza de esa actividad. Se ha puesto un importe a modo de ejemplo.

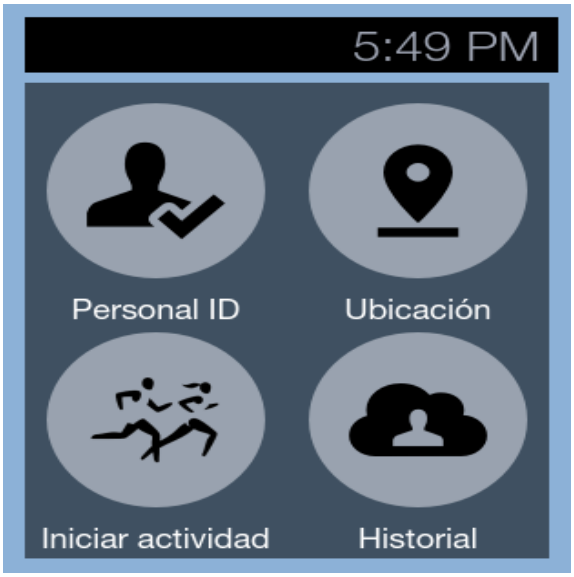
5.6.2. Smart Watch

Al igual que la aplicación móvil, se ha desarrollado un prototipo para mostrar cómo puede interactuar la persona asegurada mediante un *wereable*.

En primer lugar, una vez que el usuario entra en la aplicación de la aseguradora, ésta le muestra su pantalla inicial.

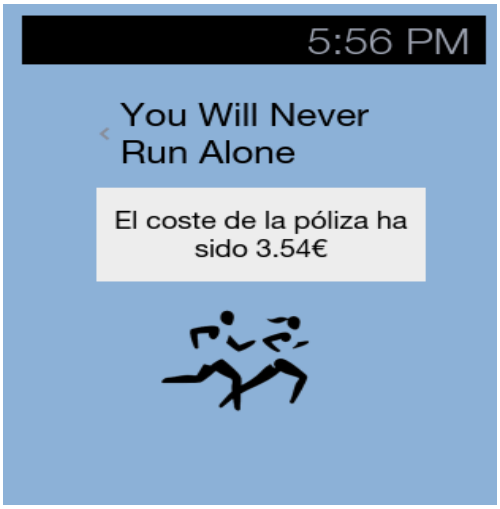


Cuando el usuario entra en el menú, podrá elegir entre una serie de opciones. En primer lugar, tendrá el acceso a su identidad, que al igual que en la aplicación móvil podría hacerse mediante KYC. El menú también le mostrará la ubicación, el historial de sus carreras y pólizas, y podrá iniciar su carrera.



En tercer lugar, y una vez iniciada la actividad, el corredor/a podrá parar la actividad, compartir en sus redes sociales, o incluso solicitar asistencia en caso de necesitarse. El uso de estos *wereables* podría detectar un fallo cardiaco y actuar de forma autónoma para solicitar asistencia, enviando su ubicación a las autoridades sanitarias.

Por último, y de la misma forma que aparecía en la aplicación móvil, se le mostrará el coste de la póliza y quedará registrada la transacción. Al ser ejecutado mediante Contratos Inteligentes y tecnología Blockchain, los pagos se ejecutarán de forma inmediata, y los datos de la transacción podrán ser consultado por ambas partes, de forma que no pueda borrarse dada su condición de inmutabilidad.



5.7. Planteamiento Actuarial

Una vez explicado cómo funciona el seguro, se propone el planteamiento que permita tarificar este seguro. Para el cálculo de la prima se han tenido en cuenta diferentes estudios e hipótesis que, en primer lugar, doten de rigurosidad el cálculo, y por otra parte, permitan simplificarlo.

Como se mencionó con anterioridad, el seguro cubre las contingencias de fallecimiento por muerte súbita y accidentes en los que se requiera asistencia médica, tales como fracturas, esguinces o torceduras.

En el caso de muerte súbita, según el estudio del Centro de Medicina del Deporte, del Consejo Superior de Deportes de Madrid (Boraita, 2011), establece la probabilidad de muerte súbita entre los corredores en un 0.002%. Este porcentaje viene avalado por diversos estudios que coinciden en probabilidad, entre ellos, el estudio de Institut Clínic Cardiovascular de la Universidad de Barcelona, y el estudio de Pedro Manonelle, presidente de la Federación Española de Medicina del Deporte (Sitges & Brugada, 2016).

5.7.1. Tratamiento de los datos

El análisis de este seguro se ha realizado teniendo en cuenta diversos estudios médicos, y población a asegurar. Para ello se ha utilizado los datos facilitados por el Instituto Nacional de estadística (INE), en el cual se extraen los datos de las personas que hay en España en el año 2017 entre las edades de 15 a 69 años y por género, que serán nuestro objetivo de mercado. En total esta población asciende a 33.202.992 personas.

Tabla 1 Población en España 2017 por edad y sexo

Población (españoles/extranjeros) por edad (grupos quinquenales), sexo y año			
	2017	**Hombres**	**Mujeres**
15-19 años	2.215.796	1.087.477	1.128.319
20-24 años	2.293.337	1.125.533	1.167.804
25-29 años	2.567.258	1.259.969	1.307.289
30-34 años	3.012.895	1.478.681	1.534.214
35-39 años	3.754.948	1.842.869	1.912.080
40-44 años	3.973.640	1.950.199	2.023.441
45-49 años	3.740.547	1.835.801	1.904.746
50-54 años	3.517.607	1.726.385	1.791.222
55-59 años	3.142.339	1.542.210	1.600.129
60-64 años	2.625.861	1.288.731	1.337.130
65-69 años	2.358.764	1.157.644	1.201.120
Total habitantes España	**33.202.992**	**16.295.499**	**16.907.494**

Fuente: Elaboración propia

Una vez obtenido esto datos, se ha cruzado con los diversos estudios analizados, en el cual se establece en porcentaje del número de personas por edad y sexo, que salen al menos una vez al año a correr. Los resultados se exponen en la siguiente tabla:

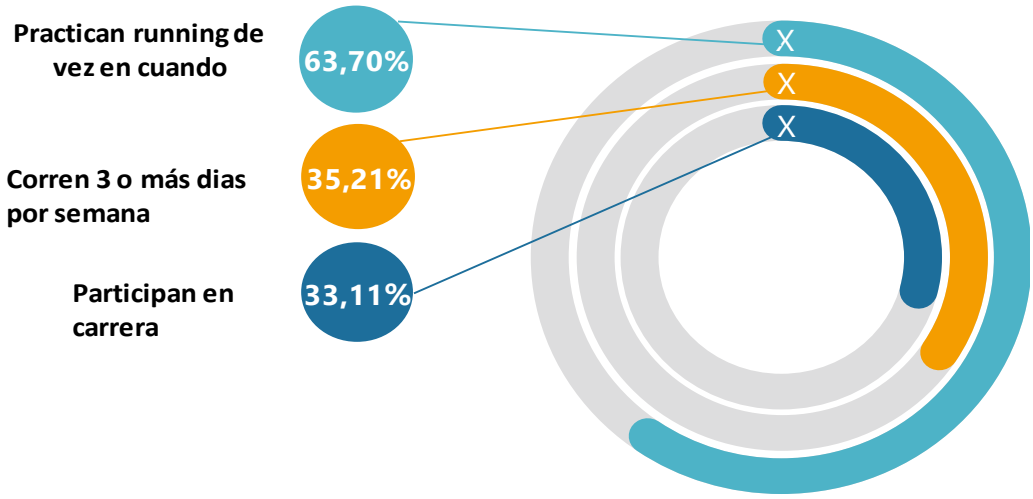
Tabla 2 Número de corredores en España por edad

Número de corredores		
	Hombres	**Mujeres**
15-19 años	685.111	417.478
20-24 años	709.086	432.087
25-29 años	793.781	483.697
30-34 años	931.569	567.659
35-39 años	1.161.007	707.469
40-44 años	1.228.625	748.673
45-49 años	1.156.554	704.756
50-54 años	1.087.623	662.752
55-59 años	971.592	592.048
60-64 años	811.900	494.738
65-69 años	729.316	444.415
Total	**10.266.164**	**6.255.773**

Fuente: Elaboración propia

Además, según el estudio de Nielsen Sport (Bellido & Amich, 2017) la frecuencia en términos esperados de estos corredores es:

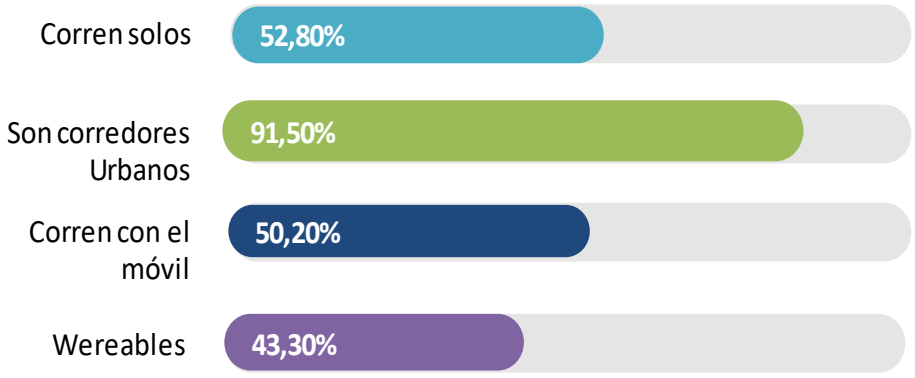
Ilustración 23 Frecuencia de práctica deportiva



Fuente: Elaboración propia a partir del informe de Cinfa Salud

Hay diversos estudios que establecen el porcentaje de personas que salen a correr con en el móvil u otro dispositivo conectado, que se necesita para poder operar con el seguro propuesto. Entre estos estos estudios se encuentran el realizado por Cinfa Salud, la Encuesta de hábitos deportivos o el paper de Monika Pobiruchin (Pobiruchin et al. 2017).

Ilustración 24 Hábitos en la práctica deportiva



Fuente: Elaboración propia a partir del informe de Cinfa Salud

5.7.2. Probabilidad de siniestros

Para el cálculo de la frecuencia se ha considerado una distribución Binomial B(n, p) en el la variable aleatoria X indica las veces que ocurre el evento de fallecimiento por muerte súbita, en la simulación realizada, de forma que:

- 1: indica que ha siniestro
- 0: indica que no se ha producido el siniestro

Se simulan n caminos aleatorios que permitan obtener el número de siniestros que ha habido en una cartera. En el caso de ocurrencia del siniestro (se ha establecido que si el valor simulado es menor que la probabilidad de que ocurra la contingencia por la que se indemniza al asegurado, en este caso, la probabilidad 0.002%, se pone un 1,que indica que hay siniestro, y si no, 0), se instituye el coste que ha tenido que asumir la aseguradora y se va acumulando, de menor a mayor, para el posterior cálculo del *Value at Risk* (Var).

El $Var_{(1-\mu)}(y)$ es el valor en riesgo de y con un nivel confianza 1-μ, que en este caso será $Var_{0.99}$ cuyo resultado refleja el peor caso dentro de los 99% mejores casos, o la mejor situación dentro del 1% de los mejores casos.

El valor en riesgo es una medida de riesgo muy común en la práctica actuarial y financiera debido a los sistemas regulatorios de Solvencia II y Basilea III.

En el caso de la contingencia de accidente, no sigue la misma distribución, dado que, si puedes tener más de un accidente, en el caso anterior ocurría que fallecías o no fallecías, pero en este caso en un año puedes tener dos o más accidentes.

Por tanto, la distribución que se sigue para el cálculo de la tarifa es una distribución de Poisson.

Las propiedades de esta distribución según el estudio de Josef Kupper son:

- La población estudiada es homogénea.
- La ocurrencia de un siniestro posterior no está influenciada por los anteriores siniestros, es decir, no existe contagio.

Su función de probabilidad es:

$$P(N = k) = p_k = \frac{e^{-\lambda} \times \lambda^k}{k!}, \qquad k = 0,1,2 \dots \tag{1}$$

Esta distribución cuenta con la propiedad de que su media y varianza son la misma:

$$E(X) = V(X) = \lambda \tag{2}$$

Los tiempos de espera entre siniestros consecutivos se distribuyen como una Poisson de parámetro λ, estos serán variables aleatorias independientes e idénticamente distribuidas, con una distribución exponencial común con media $\frac{1}{\lambda}$. Además, cuenta con la propiedad de tener ausencia de memoria, donde los siniestros ocurren de forma totalmente aleatorias y son aditivos, que significa que la suma de las variables Poisson independientes también es una Poisson, con parámetro igual a la suma de los parámetros.

Por tanto, suponiendo una cartera de n corredores se tiene:

- Todos tienen la misma λ.
- τ es el tiempo de espera entre siniestros.

Cuya función de densidad es:

$$f_\tau = \lambda \times e^{-\lambda \times \tau} \tag{3}$$

Y la función de distribución es:

$$F_\tau = 1 - e^{-\lambda \times \tau} \tag{4}$$

En el caso de la probabilidad de accidente el cálculo de siniestros esperados sería el siguiente: en España se corre una media de 3 horas 22 minutos, según el estudio de Cinfa Salud, apoyado por la encuesta de hábitos deportivos. Por lo que la media de horas en un año teniendo en cuenta que son 52 semanas es:

$$52 \times \left(3 + \frac{22}{60}\right) = 175{,}066667$$

La tasa de accidente como se ha comentado con anterioridad es 59 lesiones por cada 1000 horas de trote, entonces:

$$\frac{59 \times 175.066667}{1000} = 10{,}32893333$$

Esto significa que en un año habrá 10,32 lesiones, y como solo en 11.90% de estas son fracturas, esguinces o torceduras, se tiene:

$$10{,}32893333 \times 0{,}119 = 1{,}229143067$$

Que será la tasa de accidente que se utilizará para la tarificación de la prima.

5.8. Tarificación

El cálculo de la prima de este tipo de seguros es un reto para los actuarios/as, y para su tarificación se utilizará el Principio de Prima del Valor Esperado (PPVE) cuya expresión es la siguiente: (Balbás, 2018).

$$\pi_{(y)} = (1 + k_1)E_{(y)} + k_2\rho(-y) \qquad (5)$$

Donde Π es el precio de la prima de esta póliza o cartera, y la siniestralidad, k_1 es el recargo de seguridad, k_2 el recargo por riesgo y ρ es una medida de riesgo, en este caso no se tendrá en cuenta el recargo por riesgo, por lo que la expresión anterior queda expresada de la siguiente forma:

$$\pi_y = (1 + k_1)E_y \qquad (6)$$

Por tanto, se aplica un recargo de seguridad que se encarga de cubrir las desviaciones desfavorables de la siniestralidad, que puede derivar a que la compañía incurra en pérdidas, sea incapaz de hacer frente a sus obligaciones y, por tanto, entre en situación de quiebra.

Para hallar el resultado de k_1 que haga que el $Var_{99\%}$ sea igual a 0 se utilizará la siguiente expresión:

$$k_1 = \frac{Var_{0.99} - Coste\ esperado}{Coste\ esperado} \quad (7)$$

En el caso de un capital por accidente de 3000€, se ha realizado una simulación de 10.000 casos en una cartera de 10.000 asegurados, cuyo resultado tras la simulación ha sido:

$$k_1 = \frac{37.677.000 - 36.877.204{,}80}{36.877.204{,}80} = 0.021688 \approx 2{,}17\%$$

Bajo la hipótesis de no tener reservas iniciales y con gastos internos de un 10% (hay que considerar que con Blockchain los gastos de gestión son mínimos), el cálculo de la prima quedaría de la siguiente forma:

Tabla 3 Cálculo de la prima individual por hora

Contingencia	*Capital Asegurado*	$Var_{99\%}$	*Coste Medio de la cartera*	*Recargo seguridad*	*Prima por cada 1000 horas*	*Prima total por persona y hora*
Muerte súbita	60.000€	120.000	12.006	899.50%	120.000	0.012
Lesión	3.000€	36.877.204	37.677.000	2.17%	41.444.700	4.14

Fuente: Elaboración propia

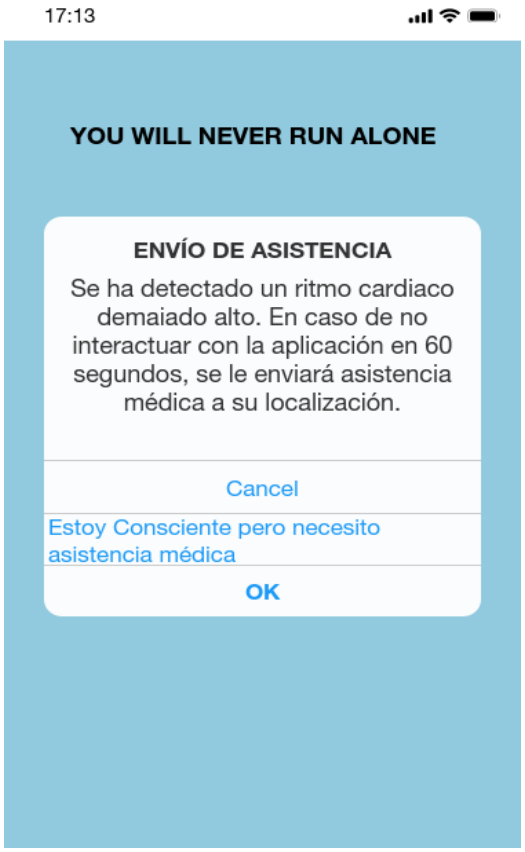
Por tanto, la prima total bajo las hipótesis establecidas sería 4.152€/hora por asegurado. Es lógico que el coste de la prima por lesión sea mayor debido a que las probabilidades de ocurrencia también son mayores.

5.9. Mejoras del Modelo

Lo mejor de una tecnología en fase de iniciación es el enorme potencial que se vislumbra, y las múltiples mejoras que se pueden implementar para ir cubriendo los diferentes obstáculos que se encuentren por el camino y descubriendo nuevos casos de uso y mejoras que cubran las necesidades de los usuarios.

Hay varias mejoras que se pueden incorporar a este producto, y que definimos a continuación:

- No todas las personas tienen las mismas probabilidades de sufrir un siniestro, al tener datos biométricos de cada persona se puede estudiar mejor el perfil de riesgo individual.
- Se puede ajustar la prima según la hora a la que se realice la actividad, es diferente correr de día que de noche…
- También se puede ajustar el riesgo teniendo en cuenta la calzada, y el lugar donde se practique el deporte, si es carretera, campo, camino, en área rural, urbano…
- Con la cantidad de datos y medios electrónicos se puede guiar al corredor de cuándo es mejor para correr debido al tiempo, aglomeración de personas, calzada en mal estado…
- Actuar como prevención en lugar de compensación por siniestro. Cuando el dispositivo electrónico registre alguna anomalía como una frecuencia cardiaca peligrosa (mayor a 220 pulsaciones menos tu edad), envíe un aviso al asegurado, ya sea un aviso en forma de mensaje al usuario, o unas vibraciones durante un determinado tiempo y en caso de no reacción enviar inmediatamente servicios de emergencia a la localización del asegurado para una rápida atención que puedan evitar consecuencias mayores. El ejemplo visual de cómo funcionaría en el prototipo creado sería el siguiente:



- Esta medida de prevención se puede hacer desde el inicio, con un estudio de la pisada para evitar lesiones, estudios de nutrición, pruebas de esfuerzo y asesoramiento deportivo que permitan una mejor práctica deportiva y una menor tasa de siniestralidad.
- Con los datos de uso, biométricos y de riesgo en tiempo real del asegurado, se podrían ofrecer nuevos servicios ajustados a su perfil, como seguro de vida. Un ejemplo de esto último es el producto lanzado este año por El Corte Ingles[50] , que ha lanzado un seguro de vida cuya prima variará en función de los pasos caminados al día.

  Este producto denominado "VidaMovida" está enfocado para personas de entre 18 y 65 años y en el caso de tener menos de 35 años y andar como máximo 10.000 pasos al día, el usuario obtendrá dinero para compras en El Corte Inglés el equivalente al 41% de la prima.

[50] http://www.expansion.com/empresas/banca/2018/04/10/5accd666ca4741fa528b4635.html

PARTE VI Conclusiones

Una vez que se ha abordado el estudio de la tecnología de la cadena de bloques y dando respuesta a los planteamientos marcados en los objetivos de este trabajo, se cierra con las conclusiones teóricas y prácticas que se han llegado en la realización de la presente investigación, estableciendo un vínculo entre la tecnología, el sector asegurador y la ciencia actuarial.

A continuación de estas, se mostrarán las limitaciones encontradas a lo largo de esta investigación, y las futuras líneas de investigación que podrían ser interesantes en el futuro.

6.1. Conclusiones teóricas

Como punto de partida se ha abordado el estudio de la tecnología Blockchain, examinando cada una de las partes que lo integran, revisando la literatura existente hasta el momento y mostrando las diferentes aplicaciones de uso que hace vislumbrar un cambio disruptivo y de pensamiento por parte de usuarios e industrias. De esta forma se abordan los objetivos primarios descritos en el primer epígrafe del presente estudio.

El camino hacia la descentralización, la transparencia, la confianza y los procesos automatizados provocarán un profundo cambio en el sector transformando su operativa tradicional.

Sin embargo, al encontrarse esta tecnología en una fase introductoria y de investigación, hace pensar que en los próximos años se podrán encontrar nuevos casos de uso, y nuevos métodos que mejores las formas de implementación y protocolos conocidos en la actualidad.

El hecho que sea de código abierto permitirá que se vaya ajustando y mejorando su eficiencia en base a los obstáculos encontrados en el camino, por lo que puede provocar que en los próximos años la cadena de bloques resulte de una forma u otra diferente a la conocida en la actualidad. Un caso de ejemplo y situado en la palestra actual es la forma de validar los bloques por los mineros, que se va ajustando de forma casi constante, y, en el que seguramente en los próximos meses o años, estas validaciones de las transacciones se realicen de una forma totalmente diferente y esperemos que aún más eficiente.

Por otra parte, el ritmo de implantación de la tecnología en los modelos de negocio de las compañías aseguradoras y su impacto en el día a día de la profesión actuarial es difícil de predecir, y se espera que se vaya introduciendo de una forma gradual durante los próximos años.

6.2. Conclusiones prácticas

Dando cumplimiento a los objetivos secundarios se ha tratado ver el impacto desde el punto de vista actuarial de lo que el ecosistema Blockchain puede llegar a transformar la profesión, y se ha creado un nuevo producto que permita ver las capacidades de la cadena de bloques, los contratos inteligentes y las demás tecnologías en la nueva era de pensamiento, nuevos modelos de negocio y el cambio de paradigma hacia su enfoque preventivo.

La irrupción de nuevas tecnologías y cambios en los hábitos de vida y consumo provoca que la industria tenga que adaptarse para sobrevivir ante nuevos modelos de negocio. Este hecho también afecta a la industria aseguradora, y ya nadie duda que en los próximos años se transforme en mayor medida que los cambios provocados en los últimos 50 años. En definitiva, se trata de la tecnología más disruptiva para el sector asegurador dentro de todos los ámbitos que engloba Insurtech.

Este nuevo ecosistema liderado por el movimiento Insurtech cambiará la misión y visión de muchas compañías de seguros, en las cuales, existirá un mayor vínculo entre asegurado y aseguradora, donde se podrá ver cómo se activan las pólizas de forma automática, cómo y cuándo se utiliza el coche, se avanzará en el ajuste de las primas en función del uso y del riesgo individual, y surgirán nuevos productos y formas de tarificar, como son los actuales *You pay as you drive*[51] o *You pay as you live*.

También se transformará el sector asegurador desde la función actuarial, donde se camina hacia la prevención en lugar de la predicción. Este cambio de paradigma afectará a todo tipo de seguros, mejorando la fidelidad del cliente, dada su eficiencia, la rápida ejecución de procesos y pagos, y aminorando la tasa de siniestralidad que soportan las compañías.

¿Cómo se consigue esta prevención? dependerá del producto o seguro en cuestión. Un ejemplo podría ser el elaborado recientemente por la compañía aseguradora Línea Directa, en el cual ha diseñado un *Smart Watch* diseñado para personas mayores que detecta las caídas bruscas, y en caso de no interacción envía asistencia. Otras compañías como DKV o ASISA disponen de equipos de profesionales en los cuales los asegurados con seguros de vida tienen a su disposición a médicos, nutricionistas, psicólogos y otros profesionales que ayuden a mejorar su calidad de vida y ayuden a prevenir enfermedades, evolución de embarazos y otras necesidades.

[51] Modalidad de seguro para el automóvil, procedente de Estados Unidos y del Reino Unido, el cual está irrumpiendo en el mercado español en compañías como AXA o Mapfre. En este seguro la prima está ligada en función de la intensidad o frecuencia con la que se utilice el vehículo. Está dirigida a los jóvenes conductores, y con la finalidad de las aseguradoras a la realización de estudios estadísticos de siniestralidad.

Muchos de estos cambios serán posibles gracias a la tecnología Blockchain, dadas sus propiedades y en el que se hace necesaria la confianza entre las partes involucradas, algo que aporta la cadena de bloques.

Este aumento de la confianza entre las partes dará lugar a una mayor reputación de las compañías dada la trasparencia, el aumento de la eficiencia en la gestión de siniestros, procesos de prima y gastos, y la reducción de costes operacionales que impactarán directamente en las primas y la cuenta de resultados.

El importe de la póliza se verá afectado también por el descenso del fraude, por el pago personalizado por uso y riesgo individual, que permitirá llegar a mercados hasta ahora inaccesibles y nuevos productos que se adapten de una forma más dinámica a las necesidades de los usuarios.

6.3. Limitaciones

Una vez desarrollado este trabajo, conviene señalar las limitaciones encontradas durante el desarrollo del presente estudio.

En primer lugar, una de las principales dificultades encontradas a lo largo de la investigación ha sido llevar una exhaustiva revisión de la literatura de una tecnología que apenas se está desarrollando y en la que existen limitadas publicaciones que entren al detalle del funcionamiento de esta.

Si es cierto que actualmente existe interés desde el mundo asegurador por las ventajas del Blockchain, sin embargo, es difícil encontrar publicaciones que entren al detalle de la tecnología, y tenga un fácil acceso a las investigaciones que desde las propias compañías se están desarrollando.

Otra de las limitaciones encontradas en este trabajo ha sido el tratamiento de los datos de corredores que existen actualmente en nuestro país. Se han considerado varios estudios de investigación y diferentes estadísticas que han permitido desarrollar el prototipo descrito en este trabajo, sin embargo, para un producto más maduro y ajustado al perfil de riesgo individual deben considerarse un mayor número de variables, que sin duda dispondrán en un futuro inmediato las compañías aseguradoras.

En cuanto al tratamiento de los datos, ha sido de una elevada complejidad integrar el procesamiento de los datos de los que pueden disponer las compañías y cómo estas pueden tratar con ellos en beneficio del asegurado y aseguradora, y, cumplan los requerimientos legales establecidos. Durante el proceso de trabajo han aparecido nuevas normativas como GDPR o el *Sandbox* que se han explicado de una forma detallada en el epígrafe cuarto de este trabajo.

Una vez abordado estos requerimientos legales, hay que considerar el celo de las personas a ceder sus datos personales y cómo las compañías, pueden luchar contra esto.

Un estudio abordado por la revista TheActuary a través de una encuesta a más de 8000 clientes, más de la mitad de los usuarios estarían dispuestos a compartir sus datos a cambio de reducir sus primas de una forma más personalizada (Institute and Faculty of Actuaries, 2018).

A pesar de las limitaciones encontradas, se puede considerar que la profundidad de la investigación y el prototipo propuesto, han permitido responder de una forma adecuada a los objetivos planteados y sienta las bases para futuras investigaciones.

6.4. Futuras líneas de Investigación

Una vez expuestas las limitaciones encontradas a lo largo del presente trabajo, hay que considerar que, de cada limitación encontrada, debe originarse, al menos, una nueva línea de investigación que supere la limitación hallada.

Hay que tener en cuenta que al estudiar tecnologías innovadoras y en fase de exploración, se debe seguir estudiando con profundidad la revisión teórica de esta tecnología que ayude a comprender de una forma más completa las implicaciones que puede llegar a tener la cadena de bloques, y su impacto en el sector asegurador.

En relación con este último, se está trabajando en la realización de un grupo de actuarios que trabajarán de la mano para la investigación y el desarrollo de la tecnología Blockchain en la ciencia actuarial.

Resulta de interés investigar el comportamiento de los usuarios en relación a los nuevos modelos negocios y cómo la integración de los datos puede llegar a impactar directamente en los modelos de *pricing* realizados por las compañías.

En cuanto a la implementación de los diferentes datos tratados por las compañías resulta todo un reto saber manejar de una forma correcta los mismos en vías de mejoras en las líneas de negocios, procesos, extracción de valor y la versatilidad de las compañías ante la llegada de la era digital.

En definitiva, ha de seguir investigándose una tecnología que promete sin duda un cambio disruptivo del sector pero que aún tiene que dar grandes pasos para su consolidación de una forma generalizada en las aseguradoras y puedan llegar a cumplir todo lo que la tecnología permite, con el fin de un de una mayor desarrollo y crecimiento económico del sector asegurador.

PARTE VII Bibliografía

360, F. (2017). *Sandbox, ¿la solución para que la regulación no sea un obstáculo a la innovación financiera?*

Actuaries, I. a. (2018). How telematics could transform motor insurance. *TheActuary*.

AEFI. (2018). *Propuesta para la implantación de un Sandbox en España.*

Alastria, C. R. (2017). Obtenido de https://alastria.io

Aller, M. G. (2017). *El fin del mundo tal y como lo conocemos* . Editorial Planeta.

Athority, E. B. (2017). *Discussion Paper: on the EBA's approach to financial technology (FinTech).*

B3i, T. B. (2016). Obtenido de https://b3i.tech/home.html

Balbás, A. (2018). Tarificación No vida.

Bellido, P., & Amich, R. (2017). *Conociendo a los Runners: Perfil del Runner en España.* Nielsen Sport.

Binance. (s.f.). Obtenido de https://www.binance.com/: https://info.binance.com/en

Boraita, A. (2011). *La muerte súbita del deportista.* Revista Española de Medicina Legal.

CFO, T. S. (2016). Discussion on Blockchain and Smart Contracts. Singapore Management University.

CinfaSalud. (2017). *VI Estudio CinfaSalud: Percepción y hábitos de los corredores y corredoras españoles.*

Consulting, C. (2017). *Smart Contracts in Financial Services: Getting from Hype to Reality.*

Europea, E. P. (27 de Abril de 2016). *Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo*.

Forum, W. E. (2018). *Blockchain Beyond the Hype: A Practical Framework for Business Leaders.*

Grant Thornton. (2018). Obtenido de www.grantthornton.es: https://www.grantthornton.es/sala-de-prensa/2018/grant-thornton-y-tirea-crearan-la-primera-plataforma-Blockchain-adaptada-al-sector-asegurador/

Hock, D. (2005). *One from many: Visa and the Rise of Chaordic Organization.* San Francisco, California: Berrett-Koehler Publishers, Inc. Obtenido de www.bkconnection.com

Insurtech, A. E. (s.f.). Obtenido de http://asociacionfintech.es/

Kupper, J. (1963). *Some aspects of cumulative risk".* ASTIN Bulletin.

Mainelli, M., & Manson, B. (2016). *How Blockchain tecnology might transform insurance.* PWC.

Marqueta, P. M. (2011). *Muerte súbita del deportista.* Federación Española de Medicina del Deporte.

McKinsey&Company. (2017). *The promise of Blockchain.*

Mercer. (2018). *Cryptocurrencies Fool´s gold or the future?*

Moser, J. (2017). *The Application and Impact of the European General Data Protection Regulation on Blockchains.* R3.

Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System.* Obtenido de www.bitcoin.org

Oliver Wyman. (2017). *Technology-Driven Value Generation in Insuramce.*

Pobiruchin, M. (2017). *Accuracy and Adoption of Wearable Technology Used by Active Citizens:A Marathon Event Field Study.* JMIR Mhealth Uhealth.

Pobiruchin, M., Suleder, J., Zowalla, R., & Wiesner, M. (2017). *Accuracy and Adoption of Wearable Technology Used by Active* . GECKO Institute for Medicine, Informatics & Economics.

Preukschat, A. (2017). *Blockchain: La revolución industrial de internet.* Grupo Planeta.

Preukschat, A., & Molero, I. (2018). *Comunidad Blockchain: El futuro de la criptoeconomía descentralizada y las ICO´s.*

Rafael Illescas; Francisco Uría; Álvaro Requeijo. (2017). INSURTECH: retos y desafíos de cara a la nueva distribución y contratación de seguros. *Revista Española de Seguros*(169), 16-19.

Reuters. (2016). *Allianz apuesta por Blockchain para el comercio de bonos catastróficos*. Obtenido de https://www.reuters.com/article/allianz-Blockchain/allianz-bets-on-Blockchain-for-catastrophe-bond-trading-idUSL8N1961VY

Rey, J. F. (2018). Smart Contracts: Concepto, ecosistema y principales cuestiones de Derecho privado. *La Ley Mercantil* (47).

Saramago, J. (2005). *Las intermitencias de la muerte.* Harcourt.

seguro, A. d. (2016). Obtenido de https://www.adndelseguro.com/es/actualidad/companias/allianz-risk-transfer-y-nephila-prueban-con-el-Blockchain-en-contratos-swap-de

Sitges, M., & Brugada, J. (2016). *Sudden death in the athlete.* Barcelona: Institut Clínic Cardiovascular.

PARTE VIII Anexos

Código para el cálculo de la prima por muerte súbita a través de una distribución Binomial elaborado en Visual Basic.

```
1. Sub Siniestralidad_Binomial()
2.
3. Dim i As Long, j As Long, n As Long
4. Dim
   Tamano As Long, Simulaciones As Long, Probabilidad As Double, u
   As Double
5. Tamano = Cells(2, 2): Probabilidad = Cells(3, 2): Simulaciones =
    Cells(4, 2)
6.
7. For i = 1 To Simulaciones
8.     n = 0
9.     For j = 1 To Tamano
10.             u = Rnd
11.             If u < Probabilidad Then n = n + 1
12.         Next j
13.         Cells(i + 6, 1) = n
14.         Cells(i + 6, 2) = n * Cells(5, 2)
15.     Next i
16.
17.
18.     'Se suma las veces que se ha pagado en cada cartera (por
   lo que el bucle va hasta el número de simulaciones realizadas)
19.     'y se divide por el número de simulaciones para obtener el
   n° de siniestros esperados
20.     Dim h As Long
21.     Dim suma As Double
22.     suma = 0
23.     For h = 1 To Simulaciones
24.         suma = suma + Cells(6 + h, 1)
25.     Next h
26.
27.     Cells(7, 3) = suma / Simulaciones
28.
29.     'Se suma el coste de cada cartera a la vez que se crea el
   vector de costes para ordenar los costes de menor a mayor
30.
31.     Dim costeordenado() As Single
32.     ReDim costeordenado(1 To Simulaciones)
33.
34.     Dim k As Long
35.     Dim suma3 As Double
36.     suma3 = 0
37.     For k = 1 To Simulaciones
38.     suma3 = suma3 + Cells(6 + k, 2)
39.     costeordenado(k) = Cells(6 + k, 2)
40.     Next k
41.
42.     'Se divide la suma de los costes de cada cartera entre el
   número de simulaciones para obtener el coste medio de una
   cartera
43.     Cells(7, 4) = suma3 / Simulaciones
```

```
44.
45.       'Se llama a la subrutina ordenarray
46.       ordenarray costeordenado, LBound(costeordenado),
   UBound(costeordenado)
47.
48.       'Se vuelcan los costes ordenados de menor a mayor
49.       Dim m As Long
50.       For m = 1 To Simulaciones
51.       Cells(6 + m, 5) = costeordenado(m)
52.       Next m
53.
54.       'Se calcula el VaR al 99%
55.
56.       Dim var99 As Single
57.
58.       var99 = 0.99 * Simulaciones
59.       Cells(7, 6) = Cells(1 + var99, 5)
60.
61.
62.       End Sub
63.
64.
65.       'SUBRUTINA PARA ORDENAR LOS ARRAYS DE MENOR A MAYOR
66.       Sub ordenarray(ByRef ordenada As Variant, ByVal
   inferior As Long, superior As Long)
67.       'Esta subrutina es conocida como QUICKSORT, el cuál es un
   algoritmo basado en la técnica de divide y venceras que permite
   ordenar n elementos en un tiempo proporcional a n log n
68.       'Llamamos ordenada() a la matriz que tenemos que ordenar
69.       'Llamamos inferior al límite inferior de la matriz
70.       'Llamamos superior al límite superior de la matriz
71.
72.       Dim comienzo As Long 'Límite inferior de la matriz
73.       Dim fin As Long 'Límite superior de la matriz
74.       Dim x As Variant
75.       Dim y As Variant
76.
77.       comienzo = inferior
78.       fin = superior
79.
80.       x = ordenada((inferior + superior) / 2)
81.
82.       While comienzo <= fin
83.           While (ordenada(comienzo) < x) And comienzo < superior
84.               comienzo = comienzo + 1
85.           Wend
86.
87.           While (x < ordenada(fin)) And (fin > inferior)
88.               fin = fin - 1
89.           Wend
90.
91.           If comienzo <= fin Then
92.               y = ordenada(comienzo)
93.               ordenada(comienzo) = ordenada(fin)
94.               ordenada(fin) = y
95.               comienzo = comienzo + 1
96.               fin = fin - 1
97.           End If
98.
99.       Wend
100.
```

```
101.      If inferior < fin Then ordenarray ordenada, inferior, fin
102.      If comienzo < superior Then ordenarray
   ordenada, comienzo, superior
103.
104.
105.
106.      End Sub
```

Código para el cálculo de la prima por lesión a través de una distribución Poisson elaborado en Visual Basic.

```
1. Sub Siniestralidad_Poisson()
2.
3. Dim i As Long, j As Long, n As Long, y As Double, m As Long
4. Dim
   Tamano As Long, Simulaciones As Long, Esperanza As Double, u As
   Double, z As Double
5. Tamano = Hoja2.Cells(2, 2): Esperanza = Hoja2.Cells(3, 2): Simul
   aciones = Hoja2.Cells(4, 2)
6. Esperanza = 1 / Esperanza
7.
8. For i = 1 To Simulaciones
9.     n = 0
10.          For j = 1 To Tamano
11.              m = 0: z = 0
12.              Do While z < 1
13.                  u = Rnd: y = -Esperanza * (Log(1 -
    u)): z = z + y
14.                  If z < 1 Then m = m + 1
15.              Loop
16.              n = n + m
17.          Next j
18.          Hoja2.Cells(i + 6, 1) = n
19.          Hoja2.Cells(i + 6, 2) = n * Hoja2.Cells(5, 2)
20.      Next i
21.
22.      'Se suma las veces que se ha pagado en cada cartera (por
   lo que el bucle va hasta el número de simulaciones realizadas)
23.      'y se divide por el número de simulaciones para obtener el
   nº de siniestros esperados
24.      Dim h As Long
25.      Dim suma As Double
26.      suma = 0
27.      For h = 1 To Simulaciones
28.          suma = suma + Hoja2.Cells(6 + h, 1)
29.      Next h
30.
31.      Hoja2.Cells(7, 3) = suma / Simulaciones
32.
33.      'Se suma el coste de cada cartera a la vez que se crea el
   vector de costes para ordenar los costes de menor a mayor
34.
35.      Dim costeordenado() As Single
36.      ReDim costeordenado(1 To Simulaciones)
37.
38.      Dim k As Long
39.      Dim suma3 As Double
40.      suma3 = 0
41.      For k = 1 To Simulaciones
42.      suma3 = suma3 + Hoja2.Cells(6 + k, 2)
43.      costeordenado(k) = Hoja2.Cells(6 + k, 2)
44.      Next k
45.
46.      'Se divide la suma de los costes de cada cartera entre el
   número de simulaciones para obtener el coste medio de una
   cartera
47.      Hoja2.Cells(7, 4) = suma3 / Simulaciones
```

```
48.
49.       'Se llama a la subrutina ordenarray
50.       ordenarray costeordenado, LBound(costeordenado),
   UBound(costeordenado)
51.
52.       'Se vuelcan los costes ordenados de menor a mayor
53.       Dim w As Long
54.       For w = 1 To Simulaciones
55.       Hoja2.Cells(6 + w, 5) = costeordenado(w)
56.       Next w
57.
58.       'Se calcula el VaR al 99%
59.
60.       Dim var99 As Single
61.
62.       var99 = 0.99 * Simulaciones
63.       Hoja2.Cells(7, 6) = Hoja2.Cells(1 + var99, 5)
64.
65.
66.       End Sub
67.
68.
69.       'SUBRUTINA PARA ORDENAR LOS ARRAYS DE MENOR A MAYOR
70.       Sub ordenarray(ByRef ordenada As Variant, ByVal
   inferior As Long, superior As Long)
71.       'Esta subrutina es conocida como QUICKSORT, el cuál es un
   algoritmo basado en la técnica de divide y venceras que permite
   ordenar n elementos en un tiempo proporcional a n log n
72.       'Llamamos ordenada() a la matriz que tenemos que ordenar
73.       'Llamamos inferior al límite inferior de la matriz
74.       'Llamamos superior al límite superior de la matriz
75.
76.       Dim comienzo As Long 'Límite inferior de la matriz
77.       Dim fin As Long 'Límite superior de la matriz
78.       Dim x As Variant
79.       Dim y As Variant
80.
81.       comienzo = inferior
82.       fin = superior
83.
84.       x = ordenada((inferior + superior) / 2)
85.
86.       While comienzo <= fin
87.           While (ordenada(comienzo) < x) And comienzo < superior
88.               comienzo = comienzo + 1
89.           Wend
90.
91.           While (x < ordenada(fin)) And (fin > inferior)
92.               fin = fin - 1
93.           Wend
94.
95.           If comienzo <= fin Then
96.               y = ordenada(comienzo)
97.               ordenada(comienzo) = ordenada(fin)
98.               ordenada(fin) = y
99.               comienzo = comienzo + 1
100.              fin = fin - 1
101.          End If
102.
103.      Wend
104.
```

```
105.      If inferior < fin Then ordenarray ordenada, inferior, fin
106.      If comienzo < superior Then ordenarray
   ordenada, comienzo, superior
107.
108.
109.
110.      End Sub
```